TOC

Cove Data Protection (Cove) Getting Started guide **36**

Getting Started with Management Console 37

Requirements 37

Management Console 37

Install and Enable Backup Manager 38

Cove Data Protection (Cove) Management Console **39**

What's inside: 39

End User License Agreement (EULA) 39

System requirements for Management Console 40

Hardware requirements 40

Software requirements 40

Supported web browsers 40

Install Cove Data Protection (Cove) 41

User interface of Management Console 42

Information panel 42

Help Search 43

Account Information 43

Help & Resources 44

App Switcher 45

Dashboard view selection 46

Customer selection 47

Vertical menu 48

Widgets 49

Toolbar 51

Search 52

Filter 53

Devices List 55

Action menu 55

Views for Dashboards in Management Console 56

Changing the view 56
Adding new views 58
Columns to display 59
Deleting custom views 62
Download tools in Management Console 62
Custom columns in Management Console 63
Permissions required 63
Columns to display 64
Adding custom columns 67
Adding data to custom columns 68
Managing custom columns 68
Filtering Devices in Management Console 69
Widgets 70
Filter Panel 71
Clear Filters 74
Searching in Management Console 75
Basic search 75
Advanced search 76
Expressions for advanced filter in Management Console 76
Statistic field types 77
Expressions for column titles 77
Expressions for active data sources 87
Expressions for advanced filter in Management Console (Legacy) 89
Syntax for advanced filter in Management Console 100
Device management in Management Console 103
Device definition 103
Access permissions 103
Adding devices 104
Moving Devices 104
Editing devices 105

Viewing statistics for devices 106
Regular Backup 107
Microsoft 365 Backup 108
Session Flags 109
Deleting device(s) 109
Launching devices Backup Client remotely 111
Adding Devices for Quick installation in Management Console 112
Adding Devices for Legacy Installation in Management Console 114
Adding Devices for Documents in Management Console 118
Sending remote commands to devices in Management Console 122
Instructions 122
Syntax for parameters 123
Primary commands 123
Secondary Commands 124
Advanced commands 124
Parameters for remote commands 125
Backup now 125
Set Backup Manager password 125
Check Consistency 126
Clear backup selections 126
Recheck backup selections 127
Restore 128
Set backup archiving 129
Set backup bandwidth 131
Set backup filter 132
Set backup scheduling 133
Set backup selection 134
Set backup settings 135
Set logging level 140
Advanced commands 141

Force Update Backup Register 141
Upload logs 141
Backup Profiles in Management Console 142
Limitations 142
LocalSpeedVault settings in backup Profiles 142
Managing Profiles 143
Edit Existing Profiles 143
Find a Profile ID and Version 144
Removing and Deleting Profiles 145
Remove a Profile 145
Delete a Profile 145
Create Custom Backup Profiles 146
Add a Profile 146
Configure the Profile 148
Assign the profile to devices on the Management Console 151
Backup Filters and Exclusions 151
Benefits 151
Predefined filters 152
File Type Examples 153
Suggested Additional Filters 153
Product management in Management Console 154
Creating custom products 154
Custom product options 156
Assign Product 158
From Device Properties 159
From the Assign option on the Toolbar 159
Edit Product 160
Rename product 160
Remove product 161
Continuity In Management Console 161

Benefit 162
Requirements 162
Operating System 162
One-Time Restores 162
What's inside: 162
One-Time Restore to Hyper-V 163
Recovery status 178
Recovery Session Statistics 179
One-Time Restore to Azure 182
Recovery status 199
Recovery Session Statistics 200
Standby Image 203
What's inside: 204
Standby Image to Hyper-V 204
Top bar menu 217
Location context menu 218
Right-hand menu 220
Searching 225
Filtering 225
Recovery status 226
Recovery data sources 227
Recovery session statistics 227
Widgets 228
Device recovery status 228
VDR checks time frame 228
Device restore time frame 229
Exporting 229
Manage Table Columns 230
For single devices 232
For single or multiple devices 233

Settings Tab 233
General 233
Backup 234
Recovery 234
Standby Image Verification Tab 236
From Device Properties 236
From Standby Image Overview 236
Standby Image to Azure 238
Searching 256
Filtering 256
Recovery status 257
Recovery data sources 258
Recovery session statistics 258
Widgets 259
Device recovery status 259
VDR checks time frame 259
Device restore time frame 260
Exporting 260
Manage Table Columns 261
For single devices 263
For single or multiple devices 264
Settings Tab 264
General 264
Backup 265
Recovery 265
Standby Image Verification Tab 267
From Device Properties 267
From Standby Image Overview 267
Standby Image to ESXi 269
Top bar menu 279

Location context menu 280
Right-hand menu 282
Searching 287
Filtering 287
Recovery status 288
Recovery data sources 289
Recovery session statistics 289
Widgets 290
Device recovery status 290
VDR checks time frame 290
Device restore time frame 291
Exporting 291
Manage Table Columns 292
For single devices 294
For single or multiple devices 295
Settings Tab 295
General 295
Backup 296
Recovery 296
Standby Image Verification Tab 298
From Device Properties 298
From Standby Image Overview 298
Standby Image Use in Case of Disaster 300
Recovery Testing 302
Limitations 302
Enable Recovery Testing 302
Monitor Recovery Testing Devices 311
Device recovery status 316
VDR checks time frame 316
Device restore time frame 317

From Device Properties 321
From Recovery Testing Overview 321
Recovery Locations 324
Minimum Requirements 326
Recommendations for Maximum Performance 328
Add Recovery Locations 329
Add Storage Location and Server Connections 333
Top bar menu 338
Location context menu 339
Right-hand menu 341
Configure N-able Recovery Service on Azure Recovery Locations 343
Processes 358
Folders 359
Configure N-able Recovery Service on ESXi Host Server 360
Configure N-able Recovery Service on Hyper-V Server 2019 373
Manage Recovery Locations 387
Disabling Recovery Services 396
Customer management in Management Console 397
Types of customer 399
What's Next? 400
Add Customers 400
Manage Customers 410
Editing customers 411
Delete customers 416
Enable Automatic Deployment in Management Console 416
Customer UID 418
Find the Customer UID 419
Change the Customer UID 420
User management in Management Console 422
User roles 422

Adding users 426
Editing users 428
Removing users 428
Managing security officers 428
Single Sign-On 429
N-Able Single Sign-On (SSO) in Management Console 429
Single Sign-On 429
Console Update 430
Email Address Credentials 430
Single Sign-On URL Access https://sso.navigatorlogin.com 431
Duplicate Email Addresses 431
Existing Single Sign-On users 432
Two-Factor / Multi-Factor Authentication 432
Software Only Partners 434
Historical charts in Management Console 434
Scheduled Reports in Management Console 435
Requirements 435
How it works 436
Add a schedule 436
Variables for the "Subject" field 441
Manage Existing Schedules 441
Edit 441
Disable/Enable 442
Delete 442
Unsubscribe 442
Example Report 443
User Actions Log 443
Export 444
Searching and Filtering 445
Search 445

Filter 446
Data export in Management Console 448
How to Export 448
Configure Aggregated Device Statistics report 449
Configuring Maximum Value reports 451
Glossary of Cove Data Protection (Cove) terms 452
Microsoft 365 protection 453
Requirements 453
Benefits 453
Limitations 453
Microsoft 365 Benefits 453
Teams 453
Exchange 454
OneDrive 454
SharePoint 455
Microsoft 365 Limitations 455
Teams 456
Exchange 456
OneDrive 457
SharePoint 457
Custom Document Library 457
Enable Microsoft 365 Backups 458
Requirements 458
Teams, Exchange, OneDrive and SharePoint 458
Microsoft 365 Teams: What Is/Is Not Included 466
What's included 466
What's not included 466
Manage Microsoft 365 domains 467
Searching and Filtering 467
Widgets 467

Searching 468
Filtering 468
Export Protected Users 469
Manage backup selection 470
View backup and restore job queue 474
Actions for domains 474
Microsoft 365 Domain Properties 477
Restore Microsoft 365 Data 486
Requirements 486
Instructions 486
Cancel Restore 522
Microsoft 365 SharePoint Permissions 523
Restore Permissions Processes 523
Permissions restore is turned off 523
Permissions restore is turned on 523
Permissions restore is turned on (overwrite) 524
Glossary of Cove Data Protection (Cove) terms 525
Documents guide 526
How it works 526
Requirements 527
Limitations 527
Upgrading options 527
Features supported by Documents 530
Installation 531
Backup-related features 531
Recovery-related features 532
General features 533
Upgrading options 534
File types supported by Documents 534
Text files 535

Microsoft Word (Office 97-2003) 535
Microsoft Word Open XML (introduced in Office 2007) 535
Other types of text files 535
Data files 536
Page layout files 536
Presentation files 536
Microsoft PowerPoint (Office 97-2003) 536
Microsoft PowerPoint Open XML (introduced in Office 2007) 536
Other types of presentation files 537
Spreadsheet files 537
Microsoft Excel (Office 97-2003) 537
Microsoft Excel Open XML (introduced in Office 2007) 538
Misc. Excel formats 538
Other types of spreadsheets 538
Database files 539
Microsoft Access 539
Other types of database files 539
Vector Image files 539
Microsoft Office Visio 539
Other types of vector image files 540
Compressed files 540
Backup files 540
Web files 540
Exclusions for Documents 540
System data 540
Temporary files of no value 541
Other filters 541
Documents installation instructions 541
Restoring data in Documents 545
Instructions 545

Glossary of Cove Data Protection (Cove) terms 546
Glossary of Cove Data Protection (Cove) terms 547
Backup Manager 548
What's inside: 548
Backup Manager installation guide 548
Windows and macOS installers 548
GNU/Linux installers 548
System requirements for Backup Manager 549
Hardware requirements 549
Software requirements 549
Quick Installation of the Backup Manager 552
Quick Installation vs. Silent installation vs. Manual installation 552
Requirements 553
Instructions 553
Windows Only 556
Re-installing automatically deployed devices 558
Getting passphrases for automatically installed devices 559
Convert devices to passphrase-based encryption 560
Windows devices 561
Linux devices 561
MacOS devices 562
Backup Manager Installation on GNU/Linux 563
Manual Installation on GNU/Linux 563
Alternative installation on GNU/Linux 569
Installation parameters on GNU/Linux 574
Installation Verification on GNU/Linux 575
Manual installation on Windows and macOS 576
Step 1: Add device 577
Step 2: Language settings 580
Step 3: Personal access 581

Step 4: Security code (Encryption key or Passphrase) 581
Step 5: Schedule your backup (optional) 581
Step 6: Report via email (optional) 581
Step 7: Automatic selection for backup (Windows workstations only) 581
macOS Full Disk Access 582
Silent installation of Backup Manager 583
Quick Installation vs. Silent installation vs. Manual installation 583
Instructions 584
Silent installation of Backup Manager - macOS 586
Instructions 586
Update Backup Manager 587
Precursor checks 587
Instructions 588
Re-installation 591
Replaced end-user device 592
Reinstall old device for recovery only 592
Backup Manager Restore-Only Mode 594
Preconditions 594
Enabling the restore-only mode 594
Disabling the restore-only mode 596
Backup Manager Restore-Only Mode - Linux 597
Restore-only installation steps 597
Uninstalling Backup Manager 601
Uninstalling Backup Manager - Windows 601
Silent uninstallation of Backup Manager (Windows Only) 602
Uninstalling Backup Manager - macOS 604
Uninstalling Backup Manager (GNU/Linux) 605
Launch the Backup Manager 606
In-Agent Authentication 606
Add users to the "N-able Backup Users" Group (Windows Only) 607

Launch Backup Manager on Windows 609
From Start 609
From Command-Line interface 609
Launch Backup Manager on macOS 610
Launch Backup Manager on Linux 610
Backup Manager guide 610
What's inside: 611
Backup Manager Interface 611
Overview 613
Backup 616
Restore 616
Preferences 617
Preferences for Backup Manager 627
Available settings for scripts 632
Reasons to enable Bandwidth Limiting 635
Feature availability 635
Reasons to enable the LocalSpeedVault 637
How it works 637
Feature availability 637
What can be used as the LocalSpeedVault 637
Size Requirements 637
For Local Drives 638
For Network Resources 638
Windows 639
macOS & Linux 640
Synchronization statuses 641
Synchronized 642
Synchronizing 642
Failed 642
Email alerts on LocalSpeedVault synchronization statuses 643

Synchronizations errors 644
Access is denied 645
Path is invalid 645
Not enough space 645
Edit Archive tasks 647
Delete Archive tasks 649
Windows temp locations 653
Chrome/Edge/Firefox browser cache and update files 653
N-central cache directories 653
AV Defender cache files 653
EDR/SentinelOne 653
Source machine requirements 656
Temporary storage medium requirements 656
Host machine requirements 656
Supported features 657
Operating systems for backup and recovery 657
Data sources for backup and recovery 658
Backup-related features 659
Recovery-related features 660
Common features 660
Data processing technologies 661
8dot3 661
Data sources 661
Files and folders 664
More about "Files On-Demand" 665
System state 667
Virtual Disaster Recovery and Bare Metal Recovery 669
Network shares 669
Start a one-time backup 678
Configure schedule-based backups 678

Configure frequency-based backups 680
MS SQL 680
Start a one-time backup 685
Configure schedule-based backups 685
Configure frequency-based backups 687
Recovery to the Original Location 687
Recovery to an Intermediate Location 688
VMware 688
Transport Mode Values 690
Start a one-time backup 695
Configure schedule-based backups 695
Configure frequency-based backups 697
Hyper-V Overview 697
Backup 698
Restore 698
Backup 698
Restore 698
Start a one-time backup 705
Configure schedule-based backups 705
Configure frequency-based backups 707
Individual File and Folder Recovery 707
Requirements 708
Limitations 708
Instructions 708
Oracle 708
tnsnames.ora 710
sqlnet.ora 711
Option A: Map the network drive for the LocalSystem account 711
Option B: Map the network drive for an administrative user account 712
Oracle server access 712

Backup folder access 712
Retention control settings 713
Start a one-time backup 716
Configure schedule-based backups 716
Configure frequency-based backups 718
MS Exchange 718
Preparation 722
Step 1: Configure Retention 722
Step 2: Enable Single Item Restore 722
Step 3: Create User 723
Instructions to Restore 723
Recovery using the Deleted Item folder 723
Recovery using the "Recover deleted items" tool 723
Single Item Recovery (SIR) using the Recoverable Folder structure (Dumpster) 723
Restore recoverable items using a temporary PST file 724
Alternative solutions 726
Restore to a local drive 727
Requirements and recommendations 727
Instructions/example 727
In-place restore 729
Requirements 729
Important 730
Instructions 730
Pre-recovery instructions 730
Step 1: Confirm Requirements and Install the Virtual Drive 730
Step 2: Check the status of the mailbox database 730
Step 3: Check the state of log files (if applicable) 731
Step 4: Put the database into the clean shutdown state (if applicable) 731
Recovery instructions 732
MS Exchange 2007 recovery 732

MS Exchange 2010 recovery 733
Post-recovery instructions 734
MS Exchange 2007 734
MS Exchange 2010 734
MS SharePoint 734
Availability 734
Supported versions 734
Host system 734
Free space 734
VSS writers 735
Start a one-time backup 738
Configure schedule-based backups 738
Configure frequency-based backups 740
MySQL 742
Operating Systems and MySQL versions: 743
Enabling schedule-based backups 743
Configure backup selection 744
Create backup schedule 745
Start a one-time backup 747
How in-place restores work 748
Starting the MySQL service on Security-Enhanced Linux after recovery 749
Important 750
Backup technology 750
Backup session structure 750
Sequence of backup sessions 752
Practical implications 752
Enabling backups in Backup Manager 753
Requirements 753
Configure backup selection 753
Starting a Backup 756

Backup options 758
Automatic file selection in Backup Manager 758
Backup Accelerator for faster backups in Backup Manager 762
Recovering data in Backup Manager 763
Additional requirements and settings by data source 764
Instructions 764
Settings 769
Linux System Recovery 771
Additional types of recovery in Backup Manager 772
Virtual disaster recovery guide 772
Supported Windows versions 773
Backup selection requirements 773
Optional settings (for better restore speed) 773
Supported Windows versions 773
Device passphrases 774
Additional Required Software 774
Device passphrases 781
Device passphrases 788
Additional Hyper-V Optional Settings 796
Required settings 801
Optional settings 801
Device passphrases 802
Recovery Console instructions 802
Continuous restore in Backup Manager 804
Seed restore in Backup Manager 809
Required parameters 811
Optional parameters 811
Preferences for Backup Manager 812
What's inside: 812
General 812

Schedule 813
Scripts in Backup Manager 815
Proxy 819
Performance 820
LocalSpeedVault (a local storage directory in Backup Manager) 822
Synchronized 827
Synchronizing 827
Failed 827
Access is denied 830
Path is invalid 830
Not enough space 830
Archiving backup sessions in Backup Manager 830
Backup Filters in Backup Manager 835
Advanced 838
Seed backup in Backup Manager 840
Step 1. Set seeding path 842
Step 2. Enable seeding 843
Step 3. Transfer seeding folder to storage 844
Additional advanced options for Backup Manager 845
Command-line interface for Backup Manager 845
Name 851
Active 851
Data Sources 851
Day of the Week 851
Day of the Month 851
Months 852
Time 852
Weeks 852
Delimiter 853
No Header 853

ID 854
Active 854
Data Sources 854
Day of the Week 854
Day of the Month 854
Months 855
Name 855
Time 855
Weeks 855
ID 856
Name 857
Password 857
MySQL Server Port 857
User 857
Delimiter 858
No Header 858
Name 859
MySQL Server Port 859
New Port 859
Password 859
User 859
MySQL Server Port 860
Domain 861
Path to Network Share 861
User 861
Password 861
Delimiter 862
No Header 862
Path to Network Share 863
Domain 863

New Path 863
Password 863
User 863
Path to Network Share 864
Local Backup Directory 865
Name 865
Password 865
User 865
Delimiter 866
No Header 866
Name 867
Rename 867
Local Backup Directory 867
Password 867
User 867
Name 868
Name 869
Active 869
Data Sources 869
Days 869
Post-Backup Script 869
Pre-Backup Script 869
Time 870
Delimiter 870
No Header 870
ID 871
Active 871
Data Sources 871
Days 871
Name 871

Post-Backup Script 871
Pre-Backup Script 872
Time 872
ID 872
Content File path 873
Name 873
Password 873
User 873
Fail Session on Error 873
Timeout 873
Delimiter 874
No Header 874
ID 875
Password 875
User 875
Content File path 875
Fail Session on Error 875
Name 875
Timeout 875
ID 876
Data Sources 876
Data Sources 877
Delimiter 877
No Header 877
Data Sources 878
Exclude 878
Include 878
Priority 878
Data Sources 879
Delimiter 879

No Header 879
Limit 879
Date & Time 879
Data Sources 880
Delimiter 880
No Header 880
Domain 881
Format 881
Output Field 881
Date & Time 881
Domain 882
Delimiter 882
No Header 882
Limit 882
Offset 882
Removed Nodes 883
Date & Time 883
Delimiter 884
No Header 884
Plugin 884
Setting Name 884
Name 885
Value 885
Path to Configuration File 886
Path to Configuration File 886
Data Sources 886
Add 887
Remove 887
Path to Configuration File 887
Data Sources 888

Add Suffix ... 889
Existing Files Restore Policy ... 889
Outdated Files Restore Policy ... 889
Restore To ... 889
Selection ... 889
Session Search Policy ... 889
Date & Time ... 889
Host ... 890
Password ... 890
Port ... 890
Timeout ... 890
Username ... 890
Virtual Drive: for quick access to backups ... 891
Installation Wizard ... 897
Command-Line Installation ... 899
Parameters ... 899
Example ... 903
Configuration File ... 904
Config.ini location ... 904
Logging ... 906
Versions of the application log ... 906
Application log structure ... 906
Application log settings ... 907
View application log ... 907
Filter application logs ... 907
Enable debug logs ... 909
Enable protocol logs ... 911
Restarting the internal backup processes and service ... 911
Windows instructions ... 911
Linux instructions ... 912

macOS instructions 912
FAQs 912
General 912
Installation & Setup 913
Backup 915
Restore 921
Glossary of Cove Data Protection (Cove) terms 923
Recovery 924
What's inside: 924
Continuity In Management Console 924
Benefit 924
Requirements 924
Operating System 925
One-Time Restores 925
What's inside: 925
One-Time Restore to Hyper-V 925
Recovery status 941
Recovery Session Statistics 942
One-Time Restore to Azure 945
Recovery status 962
Recovery Session Statistics 963
Standby Image 966
What's inside: 967
Standby Image to Hyper-V 967
Top bar menu 980
Location context menu 981
Right-hand menu 983
Searching 988
Filtering 988
Recovery status 989

Recovery data sources 990
Recovery session statistics 990
Widgets 991
Device recovery status 991
VDR checks time frame 991
Device restore time frame 992
Exporting 992
Manage Table Columns 993
For single devices 995
For single or multiple devices 996
Settings Tab 996
General 996
Backup 997
Recovery 997
Standby Image Verification Tab 999
From Device Properties 999
From Standby Image Overview 999
Standby Image to Azure 1001
Searching 1019
Filtering 1019
Recovery status 1020
Recovery data sources 1021
Recovery session statistics 1021
Widgets 1022
Device recovery status 1022
VDR checks time frame 1022
Device restore time frame 1023
Exporting 1023
Manage Table Columns 1024
For single devices 1026

For single or multiple devices 1027
Settings Tab 1027
General 1027
Backup 1028
Recovery 1028
Standby Image Verification Tab 1030
From Device Properties 1030
From Standby Image Overview 1030
Standby Image to ESXi 1032
Top bar menu 1042
Location context menu 1043
Right-hand menu 1045
Searching 1050
Filtering 1050
Recovery status 1051
Recovery data sources 1052
Recovery session statistics 1052
Widgets 1053
Device recovery status 1053
VDR checks time frame 1053
Device restore time frame 1054
Exporting 1054
Manage Table Columns 1055
For single devices 1057
For single or multiple devices 1058
Settings Tab 1058
General 1058
Backup 1059
Recovery 1059
Standby Image Verification Tab 1061

From Device Properties 1061
From Standby Image Overview 1061
Standby Image Use in Case of Disaster 1063
Recovery Testing 1065
Limitations 1065
Enable Recovery Testing 1065
Monitor Recovery Testing Devices 1074
Device recovery status 1079
VDR checks time frame 1079
Device restore time frame 1080
From Device Properties 1084
From Recovery Testing Overview 1084
Recovery Locations 1087
Minimum Requirements 1089
Recommendations for Maximum Performance 1091
Add Recovery Locations 1092
Add Storage Location and Server Connections 1096
Top bar menu 1101
Location context menu 1102
Right-hand menu 1104
Configure N-able Recovery Service on Azure Recovery Locations 1106
Processes 1121
Folders 1122
Configure N-able Recovery Service on ESXi Host Server 1123
Configure N-able Recovery Service on Hyper-V Server 2019 1136
Manage Recovery Locations 1150
Disabling Recovery Services 1159
Recovery Console Guide 1160
Recovery Console installation 1161
Requirements 1161

Exclusions 1161
Instructions 1162
Starting and quitting Recovery Console 1162
How to Quit 1162
Recovery Console interface 1163
Enabling recovery in Recovery Console 1164
Restore from date/time session 1168
Continuous Restore in Recovery Console 1170
Requirements 1170
Enabling the Continuous Restore mode 1170
Using virtual machines in-between restore sessions 1171
Advanced settings in Recovery Console 1172
Editing configuration file 1172
Required settings for Recovery configuration file 1172
Enable debug logging 1174
Bare metal recovery guide 1174
Alternative solutions 1175
Bare metal recovery requirements and limitations 1175
Source system requirements 1175
Host system requirements 1176
Target computer requirements 1176
USB drive requirements 1179
USB drive limitations 1179
Bare metal recovery instructions 1179
Step 1: Download recovery software 1179
Step 2. Create a bootable media 1179
Step 3. Boot the target machine 1180
Step 4: Recover the source system 1183
Step 5. Recover other data (if applicable) 1185
Virtual disaster recovery guide 1185

Virtual Disaster Recovery Requirements 1185
Hyper-V & Local VHD 1187
VMWare VMDK & VMWare ESXi 1187
Virtual Disaster Recovery Instructions 1188
Virtual disaster Recovery for Linux 1208
Virtual Disaster Recovery Settings 1208
Hyper-V, Local VHD, VMWare VMDK 1208
VMWare ESXi 1211
Continuous Restore for Virtual Disaster Recovery 1215
Requirements 1215
Enabling the Continuous Restore mode 1215
Using virtual machines in-between restore sessions 1216
Hyper-V Post Virtual Disaster Recovery 1217
VMWare VMDK Post Virtual Disaster Recovery 1217
Glossary of Cove Data Protection (Cove) terms 1217
Additional Services 1218
What's inside: 1218
Storage management guide 1218
Cloud structure 1218
Functions of a node 1219
States of a node 1219
Requirements and recommendations 1219
Supported operating systems 1219
Supported file system types 1220
Storage Node Installer version 1220
Recommended number of storage nodes 1220
Hardware recommendations 1220
Storage virtualization recommendations 1221
Clusters 1221
Custom SSL Certificates 1221

Storage node installation instructions 1222
Install storage node on Linux 1223
Install storage node on Windows 1226
Updating and reconfiguring a storage node 1231
Preparatory steps for versions prior to 16.2 1231
Linux instructions 1232
FreeBSD instructions 1232
Windows instructions 1232
Update and reconfigure a storage node 1233
Relocating a storage node to new hardware 1238
Requirements 1238
Instructions 1239
Relocate storage node on GNU/Linux 1239
Relocate storage node on Windows 1241
Managing private storage 1243
Selecting partnership model for customers 1243
Selecting storage pool for device 1245
Storage Reporting 1247
Monitoring private storage 1248
Storage node service 1249
Stop the storage node service 1249
Making sure the service has been stopped (optional) 1250
JSON-RPC API guide for Cove Data Protection (Cove) 1250
Data format 1250
Making changes 1251
Date and time format 1251
Size format 1251
Requirements for HTTP requests 1252
What's Inside 1252
How to use the Backup Manager JSON-RPC API schema 1252

Recommendations 1252
Schema sections 1253
Construct A JSON-RPC API Call 1255
Authorization in JSON-RPC API 1258
Required parameters 1260
Sample request 1260
Sample response 1260
Device management methods in JSON-RPC API 1261
Adding backup devices in JSON-RPC API 1261
StorageNodeCommonInfo child parameters 1264
StorageNodeStateInfo child parameters 1265
StorageNodeModeInfo child parameters 1266
Getting device info by name in JSON-RPC API 1267
StorageNodeCommonInfo child parameters 1268
StorageNodeStateInfo child parameters 1269
StorageNodeModeInfo child parameters 1269
Getting device info by ID in JSON-RPC API 1271
StorageNodeCommonInfo child parameters 1272
StorageNodeStateInfo child parameters 1273
StorageNodeModeInfo child parameters 1274
Getting device info by Token in JSON-RPC API 1276
Getting device ID in JSON-RPC API 1278
Enumerating Devices in JSON-RPC API 1278
Enumerating Device Statistics in JSON-RPC API 1280
Changing device properties in JSON-RPC API 1283
Removing devices in JSON-RPC API 1286
Customer management methods in JSON-RPC API 1287
Adding customers in JSON-RPC API 1288
PartnerCompanyInfo Child Parameters 1290
AdvancedPartnerPropertiesInfo Child Parameters 1291

Enumerating customers in JSON-RPC API 1292
Enumerating customer properties in JSON-RPC API 1295
Enumerating child customers in JSON-RPC API 1298
Getting Customer Information By Name in JSON-RPC API 1301
Getting Customer Information By ID in JSON-RPC API 1302
Getting Customer Information by UID in JSON-RPC API 1304
Getting Customer Information History in JSON-RPC API 1306
Getting Customer State in JSON-RPC API 1308
Getting Customer Tree in JSON-RPC API 1309
Regenerate a Customer UID on JSON-RPC API 1311
Changing customer properties in JSON-RPC API 1312
PartnerCompanyInfo Child Parameters 1314
AdvancedPartnerPropertiesInfo Child Parameters 1316
Removing Customers in JSON-RPC API 1317
Storage management methods in JSON-RPC API 1318
Getting storage information in JSON-RPC API 1318
Getting storage node information in JSON-RPC API 1319
Getting a list of storage nodes in JSON-RPC API 1321
Getting a list of storage nodes (by account ID) in JSON-RPC API 1322
Getting a list of storage statistics in JSON-RPC API 1324
Getting a list of storages in JSON-RPC API 1325
User management methods in JSON-RPC API 1326
Adding users in JSON-RPC API 1327
Enumerating users in JSON-RPC API 1329
Getting user information in JSON-RPC API 1331
Getting user information by user ID in JSON-RPC API 1332
Changing user properties in JSON-RPC API 1333
Removing users in JSON-RPC API 1336
Miscellaneous methods in JSON-RPC API 1337
Get Dashboard View settings in JSON-RPC API 1337

Enumerating User Dashboard View settings in JSON-RPC API 1338
Enumerating Regions in JSON-RPC API 1340
Enumerating Storage Locations in JSON-RPC API 1341
Enumerating Device's Profiles in JSON-RPC API 1346
Management Console column codes for API 1352
Expressions for active data sources 1353
Column Codes 1354
Management Console column codes for API (Legacy) 1360
User Guide for Cloud Management Console (legacy) 1370
Legacy - Getting started with Cloud Management Console 1370
Installation 1371
User authorization 1372
One-time email notifications in Cloud Management Console 1373
Instructions 1373
Formatting rules 1374
Templates for one-time notifications in Cloud Management Console 1377
Variables supported by templates 1378
Variables related to customers in Cloud Management Console 1378
Variables related to devices in Cloud Management Console 1381
Common settings for notification templates in Cloud Management Console 1385
ConnectWise Billing integration with Cloud Management Console 1386
Autotask integration with Cloud Management Console 1386
PDF version of Documentation 1386
Glossary of Cove Data Protection (Cove) terms 1387

Cove Data Protection (Cove) Getting Started guide

To help you install Backup Manager and get your backups running quickly and easily, this **Getting Started guide** is designed to help you get up and running with the basic functionality of Cove Data Protection (Cove).

Since Cove Data Protection (Cove) is a cloud-first data protection platform, it does require the very first backup to be a full backup. This will take longer than future daily backups, where only a fraction of protected data is sent to the cloud. It is recommended to do this in advance whenever possible.

You can use this product to protect physical and virtual servers, workstations, and Microsoft 365 instances.

For information on geographical backup locations, please see Data Center Backup.

This is not an all inclusive guide to the Cove Data Protection (Cove) product and so does not cover some additional features. For full information on the product, please see the full backup documentation.

Please see the pages below to complete the initial setup of Cove Data Protection (Cove). Ensuring these steps are completed in this given order which will stop any conflicts.

Getting Started with Management Console

Requirements

System Requirements for Management Console

Check the System requirements for Management Console to be sure you meet the relevant hardware and software requirements.
Complete

Backup Manager installation system requirements

Check the Backup Manager installation system requirements to confirm the intended backup devices meet the relevant hardware and software requirements.
Complete

Management Console

Accept the End User License Agreement

Accept the End User License Agreement (EULA) in order to proceed using Backup Manager
Complete

Add Users (Optional)

Add Users. Users (Or User Accounts) are required for access to the Management Console and other services. Take a look at the User Management page to check which user roles best fit, then follow the instructions to add users.
Complete Skipped

Add Customers/Partners

Add Customers to the Management Console as a way to organize backup devices by your clients, or groups or departments within your own company.
Complete

Create Profiles (Optional)

Create Profiles, which allow you to configure backup settings for multiple devices as one.
Complete Skipped

Install and Enable Backup Manager

Backup Manager Supported Features

Check the supported features for the Backup Manager to ensure we support the Operating System versions, Data Sources and additional features you require before installing.
Complete

Install Backup Manager

Install Backup Manager on devices where a backup is required.
Complete

Launch Backup Manager

Launch the Backup Manager client on the device.
Complete

Enable Backups

Configure the backup selection and schedule, then enable backups on the device. Alternately you may Start a one-time backup.
Complete

Cove Data Protection (Cove) Management Console

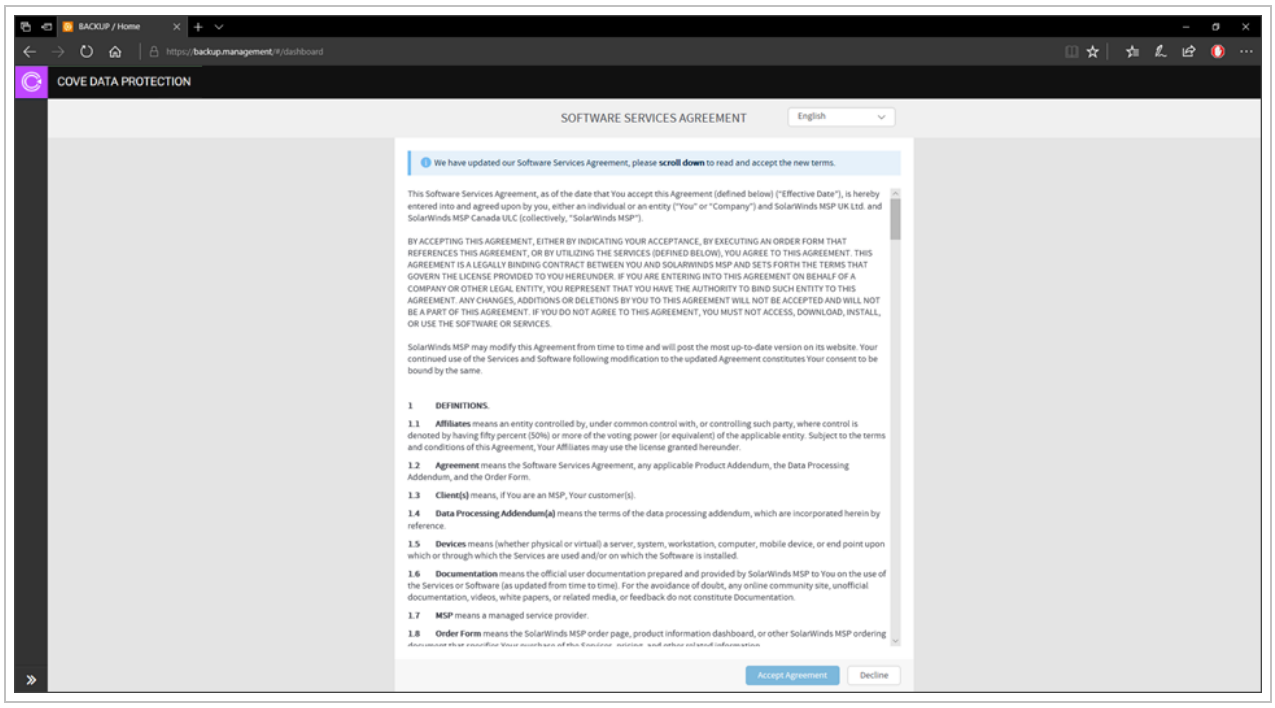
The Management Console is an all-in-one platform for backup service providers and system administrators. Using the Console, a company can manage its user and reseller network, customize access to the service, manage storage and backup/recovery processes and more.

What's inside:

End User License Agreement (EULA)

When you create a customer at Distributor, Sub-distributor or Reseller levels, they must accept our End User License Agreement (EULA) in order to proceed with using our software.

Once a customer has been created and they log in for the first time, they will be given the Software Services Agreement to read.



If the customer wishes to proceed and accept the agreement, they must click **Accept Agreement**, fill in their details and tick **I have the authority to accept this agreement on behalf of my organization 'Organization Name'** and click **Confirm**.

Once this has been done, the customer will be taken to the Management Console's dashboard to add devices, users or customers of their own.

If the customer does not agree to the terms of use, they should click **Decline**, fill in the relevant details and click **Confirm**.

> The customer must accept the EULA to continue using the Backup software.

System requirements for Management Console

Hardware requirements

- 1 GB of computer memory (RAM)
- Screen resolution of 1366 x 768 pixels or higher
- High-speed Internet connection

Software requirements

You can use the Console on any workstation or server that has a required web browser installed.

Mobile devices are not supported. You can launch the Console on a phone at your own responsibility but we cannot guarantee that all elements will be displayed correctly.

Supported web browsers

Most web browsers that have **JavaScript** on are supported. We **recommended** the following browsers:

- Google Chrome
- Mozilla Firefox

- Safari for macOS (limitation[1])
- Microsoft Edge

> You must have **JavaScript** enabled in your browser; the application will not be able to load properly without it.

Install Cove Data Protection (Cove)

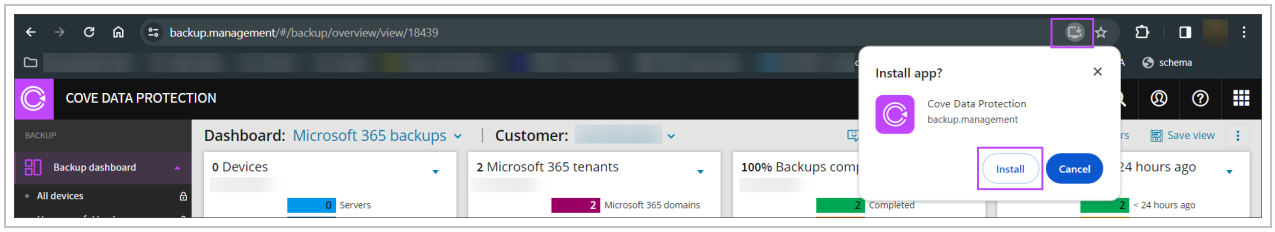
The Cove Data Protection (Cove) console (backup.management) can be installed as an app on your device on Windows, macOS and Linux devices.

> The Cove Data Protection app functions in exactly the same manner as the web page in a browser, you do **not** need any additional permissions, or a specific user level.

> Your browser **must** be up to date to the latest version.

To download and install:

1. Log in to the Management Console
2. In the search bar of your browser, click the install button:

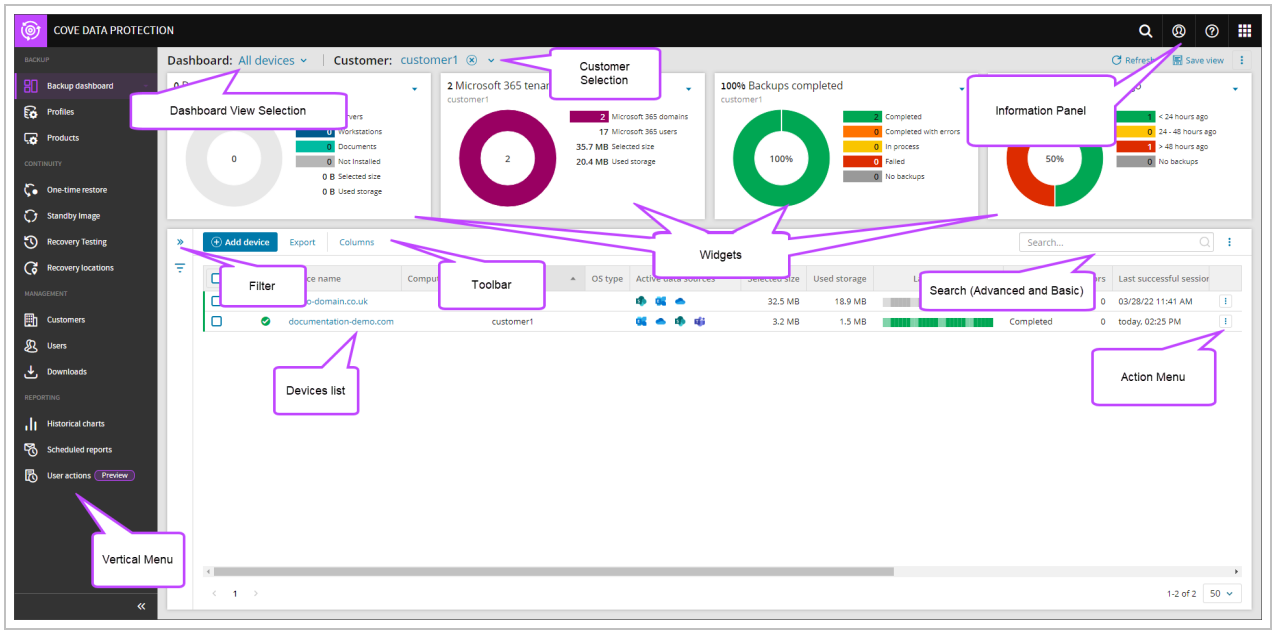


3. Select **Install**

The **Cove Data Protection** app will open independently of the browser and will be pinned to the task bar with the following icon:

[1]If the name of a directory contains a letter with the "umlaut" symbol (ä, ü, ö), it may not be possible to view the contents of the directory in the restore selection. If you experience the issue, please open the Backup Manager in another browser, for example Google Chrome.

User interface of Management Console



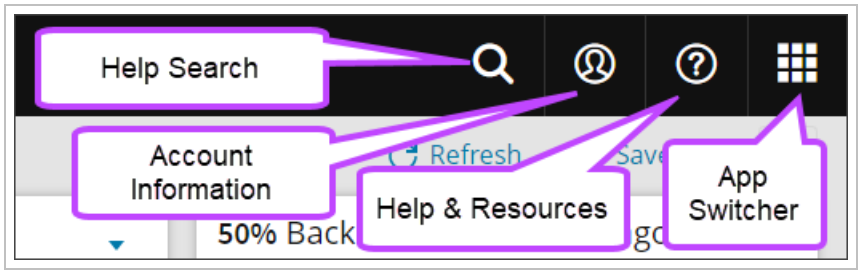
The Dashboard is broken down into several primary elements:

- Information panel
  - Help Search
  - Account Information
  - Help & Resources
  - App Switcher
- Dashboard view selection
- Customer selection
- Vertical menu
- Widgets
- Toolbar
- Search
- Filter
- Devices List
- Action menu

Information panel

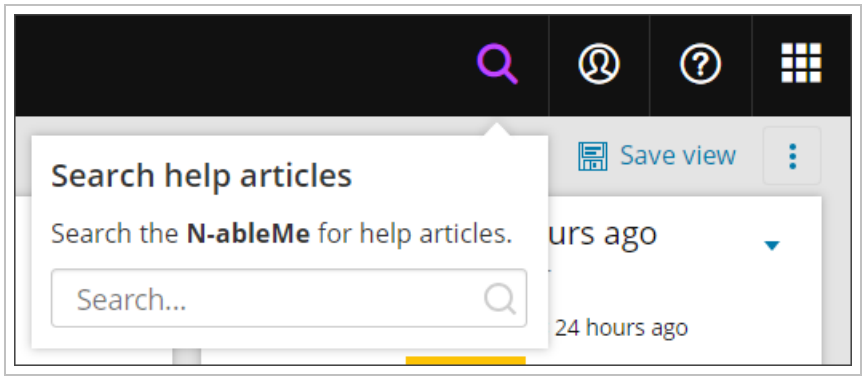
The information panel is broken into three distinct areas:

- Help Search
- Account Information
- Help & Resources
- App Switcher



Help Search

This search function allows you to search in the N-AbleMe for Knowledge Base/Troubleshooting articles to help resolve issues.



Account Information

The email address used for login to the Management Console can be found in the upper-right corner of the screen. Clicking on this opens the **Account information** box, which gives access to some more options:

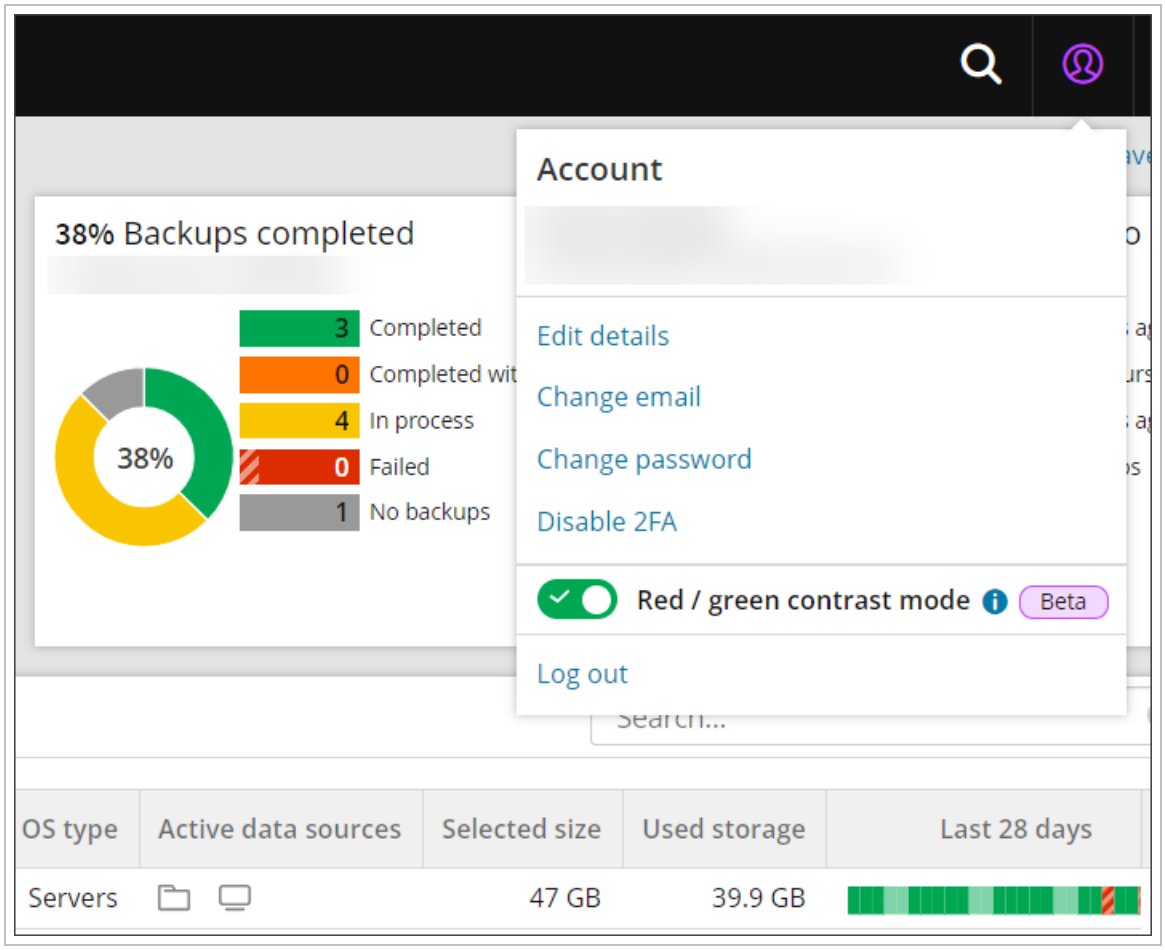
- The name and email address of the user logged on
- Edit details
- Change email
- Change password
- Setup or Disable 2FA

  This will differ depending on whether 2FA is enabled for the user or not

- Enable/Disable red / green contrast mode

  This will be applied to the key status colours for charts and the last 28 days color bar **only**

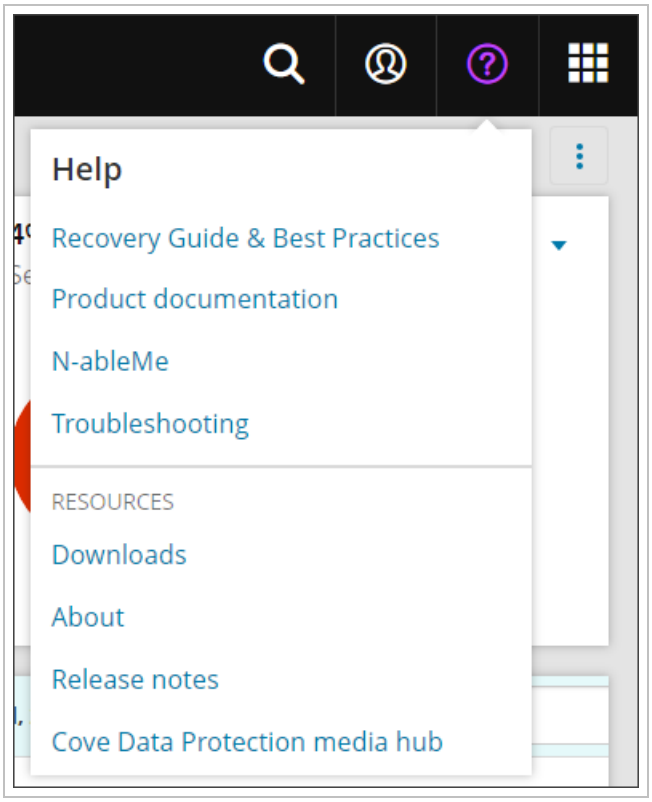
- Logout



Help & Resources

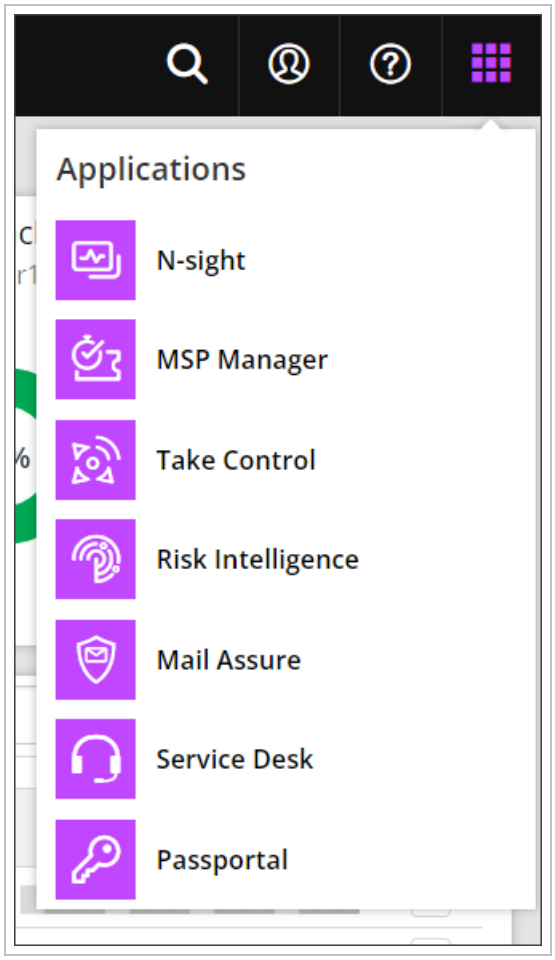
The help and resources box provides several links to resources we hope you will find useful, including to:

- Help:
  - Recovery Guide & Best Practices
  - Product Documentation
  - N-AbleMe
  - Troubleshooting
- Resources
  - Downloads
  - About
  - Release Notes
  - Cove Data Protection Media Hub



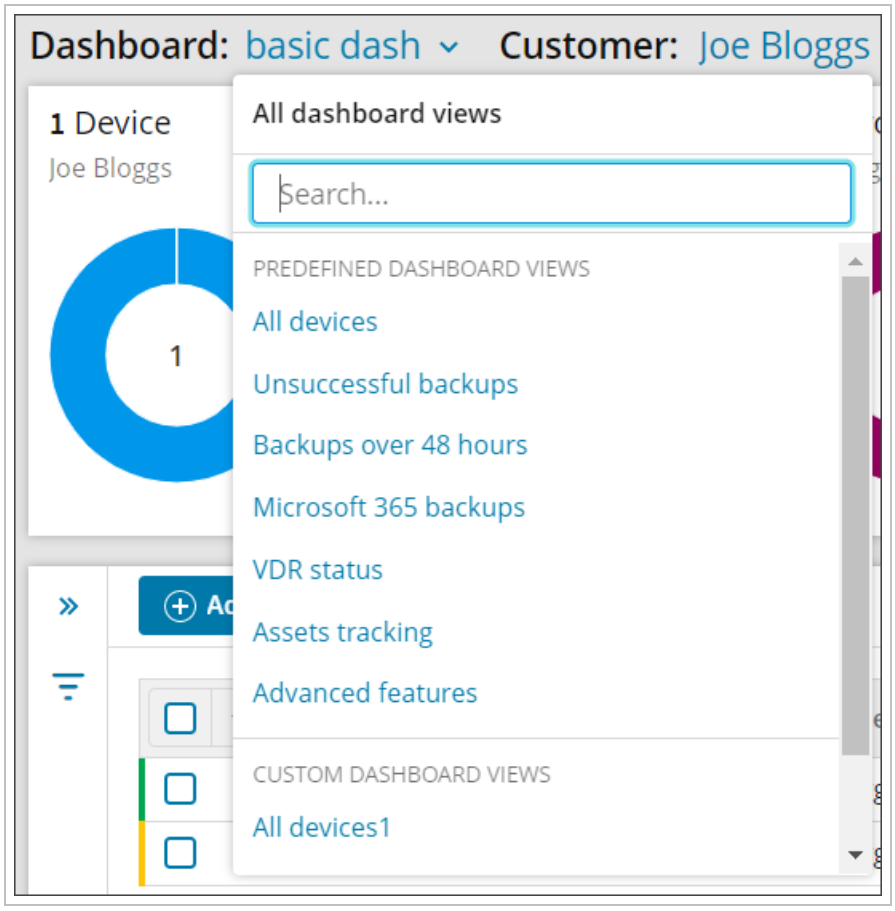
App Switcher

Using the App Switcher, it is possible to move between the suite of N-Able products that you have purchased that use N-Able Single Sign-On (SSO).



Dashboard view selection

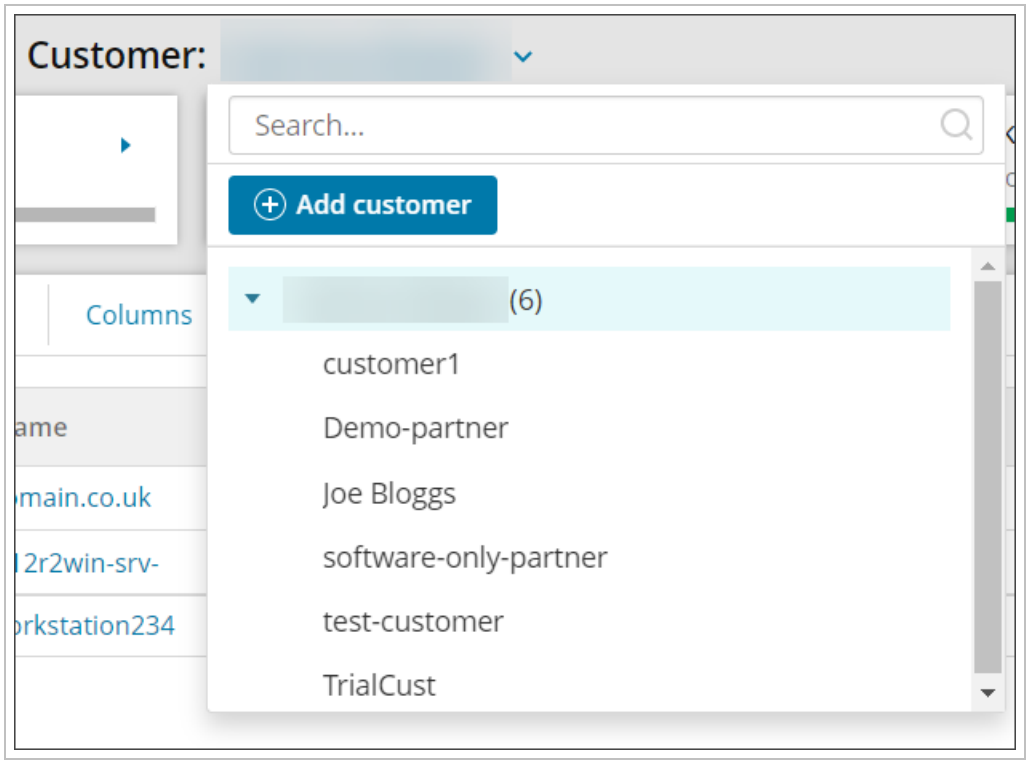
The Dashboard view selection allows you to apply different views (predefined and custom) to the dashboard using the dropdown at the top of the page.



For full details on Dashboard views, see Views for Dashboards in Management Console.

Customer selection

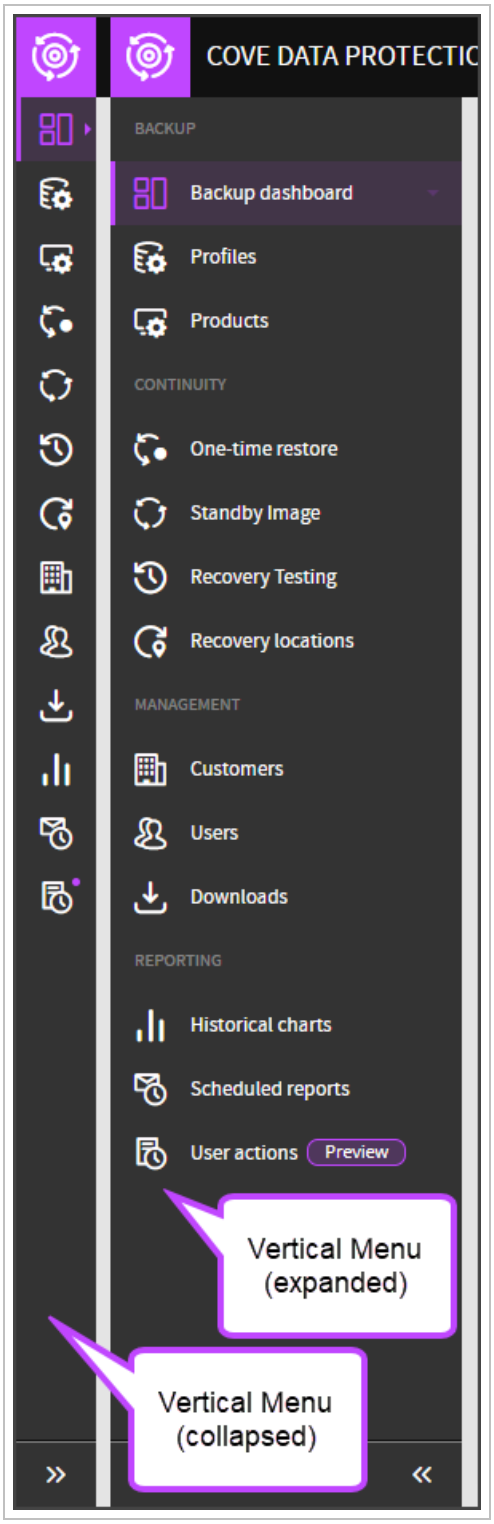
The Customer selection allows you to view the backup devices specific to the selected customer using the dropdown at the top of the page.



For full details on Customers, see Customer management in Management Console.

Vertical menu

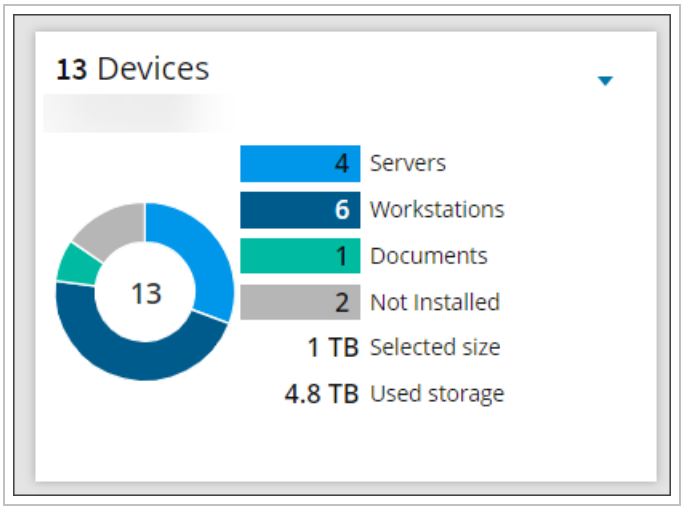
A vertical menu on the left side of the screen lets you navigate from **Backup > Dashboard** to other modules and back. The menu can be collapsed or expanded using the << or >> arrows as required.



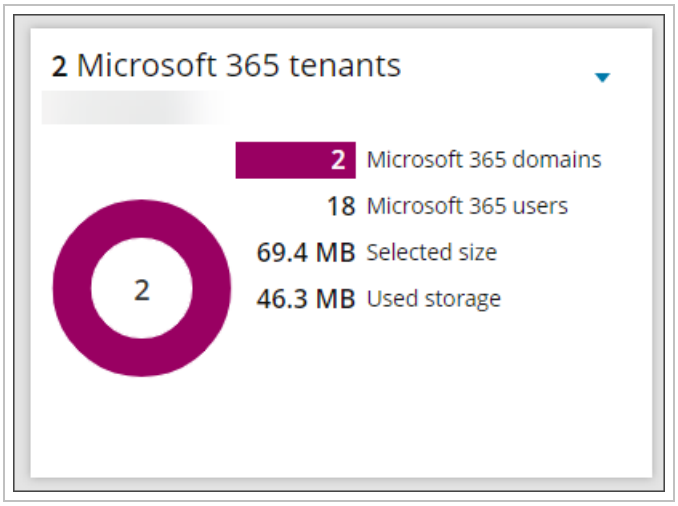
Widgets

In the Management Console's Backup Dashboard, you will see 4 graphic widgets in the form of doughnut charts.

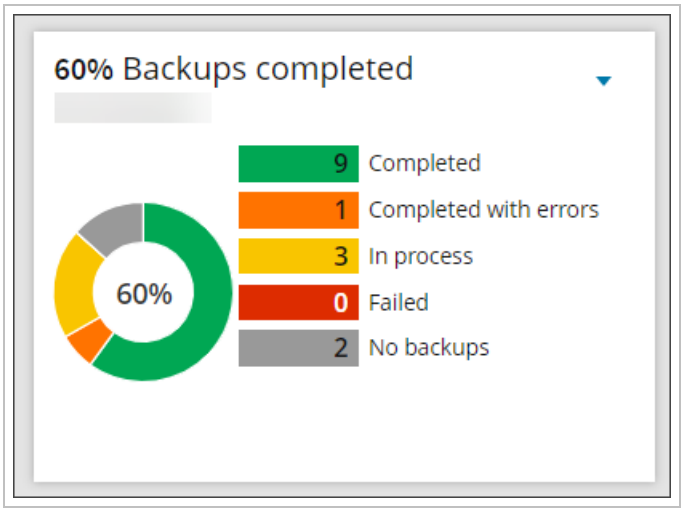
- The **Devices** widget illustrates the distribution of devices by the type with a choice of **Server, Workstation, Documents** and **Not Installed**. The selected size and used storage for these devices is displayed below



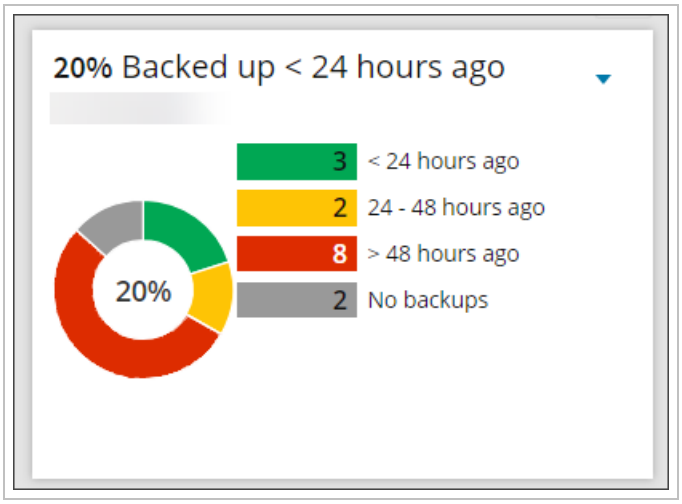
- The **Microsoft 365** widget gives a break down of the number of Microsoft 365 domains and users. The selected size and used storage are displayed below



- The **Backup Statuses** widget offers a breakdown of the statuses of the latest backup sessions for your devices



- The **Last Backup** widget shows a the timing of the latest backup sessions for your devices

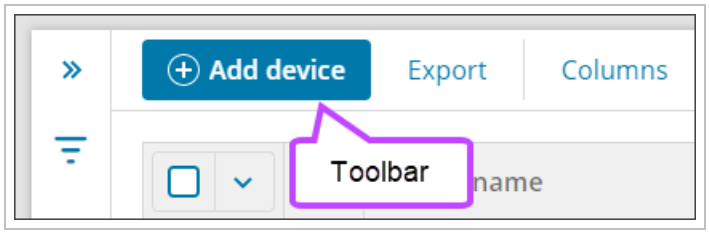


What you can do with these widgets:

- **Expand/minimize** a widget using the arrow icon in the top right corner
- **Select data on a widget and reset the filter** - By default, the widgets summarize statistics for the devices listed below (see the **Devices** widget). If you click on a value, the list of devices on the dashboard is immediately updated to match the selection

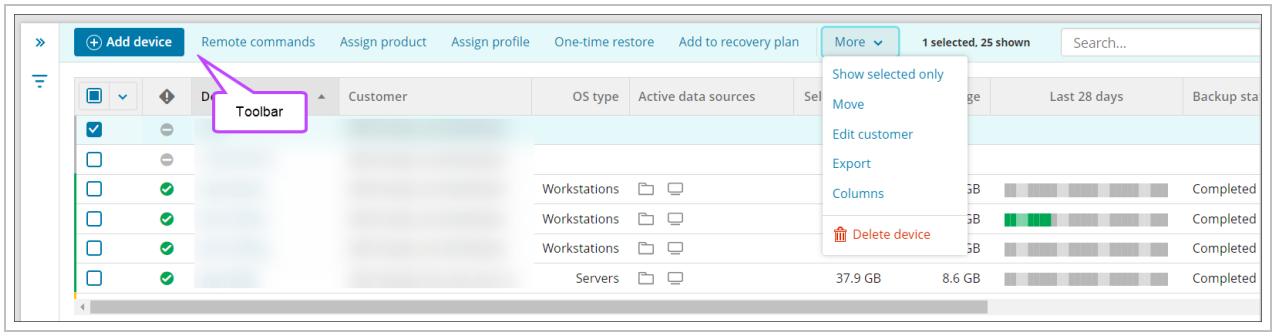
Toolbar

The toolbar gives access to the most important functions in the Backup Dashboard. When no device is selected, the toolbar has the following options:



- Add new devices
- Export monthly device statistics
- Set the columns to be displayed

When any number of devices have been selected, the toolbar provides additional key features:



- Add new devices
- Move a device to a different customer
- Assign a product
- Assign a profile
- Assign a recovery testing plan
- More:
  - Show selected device(s) only
  - Send remote commands to the selected device(s)
  - Export monthly device statistics
  - Set the columns to be displayed
  - Delete the device/domain(s)

The toolbar will also display the number of device/domain(s) selected out of the total shown.

Search

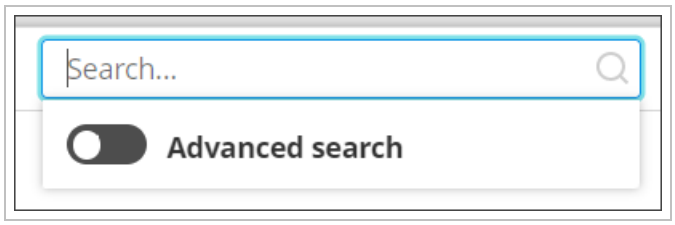
The Search box has two modes:

- **Basic search** - allows you to enter a text value for such columns as Device Name, Customer and Product

  For example, type `.co.uk` to find all Microsoft 365 domains using a .co.uk suffix.

- **Advanced search** - allows the use of advanced filter expressions to search column data

  For example, type `us > 10.giga()` to find all devices with a Used Storage of more than 10 GB, or `I78 =~ 'D01D02'` to list all devices which backup the Files and Folders and System State data sources



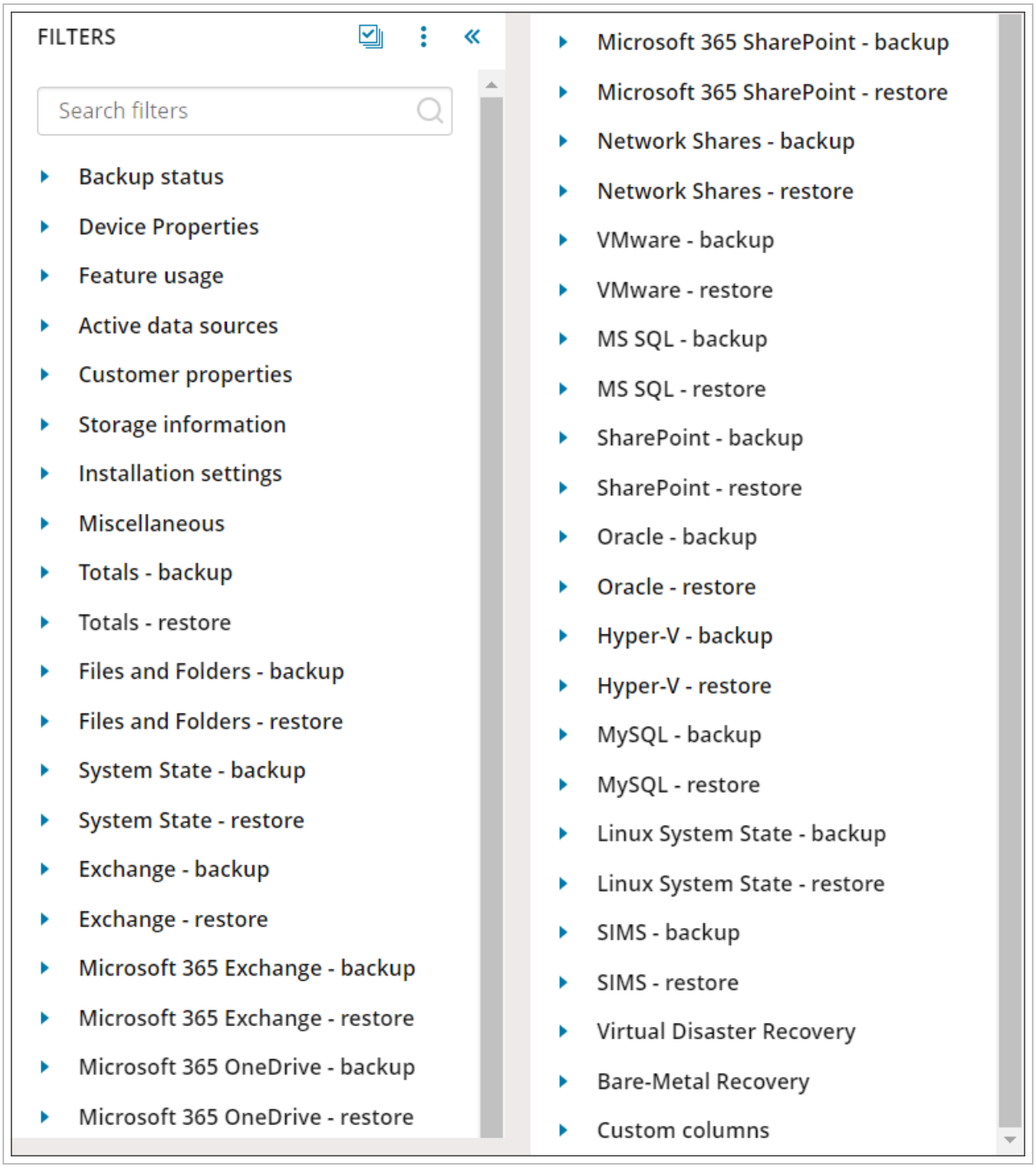
> You can clear the search by clicking the **X** on the search bar.

See the following pages for full details:

- Searching in Management Console
- Expressions for advanced filter in Management Console
- Expressions for advanced filter in Management Console (Legacy)

Filter

Filtering devices can be done by using the predefined criteria in one of the graphic Widgets or by using the filter panel on the left of the devices list to narrow down the devices displayed.



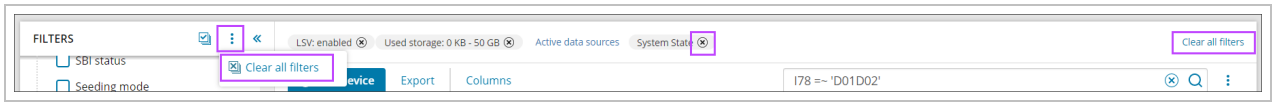
Using the Filters list, you can find devices that meet any multitude of criteria.

For example, if you would like to know which devices back up the System State data source, use a LocalSpeedVault and have a used storage of under 50GB, you can use the following filters:

- **Active data sources** - System State
- **Feature Usage** - LSV, select enabled

- **Storage Information** - Used storage, use the slider bar to move the top marker down to 50GB

You can clear individual filters by clicking the **x** beside each one from the banner above the toolbar, or clear all filters by clicking the **Clear all filters** button, or selecting it from the action menu by clicking the three vertical dots in the filter menu.



For full details on filtering, see Filtering Devices in Management Console.

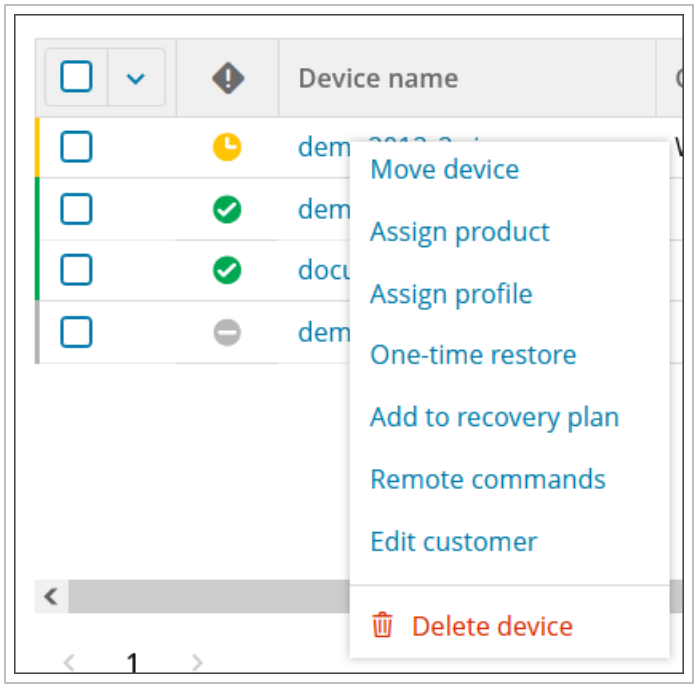
Devices List

The devices list will display a list of all devices meeting the currently set filter, search and customer conditions. If no filters or searches are applied, the list will display all devices for the selected customer, or if viewing from the Root customer, all devices for all customers.

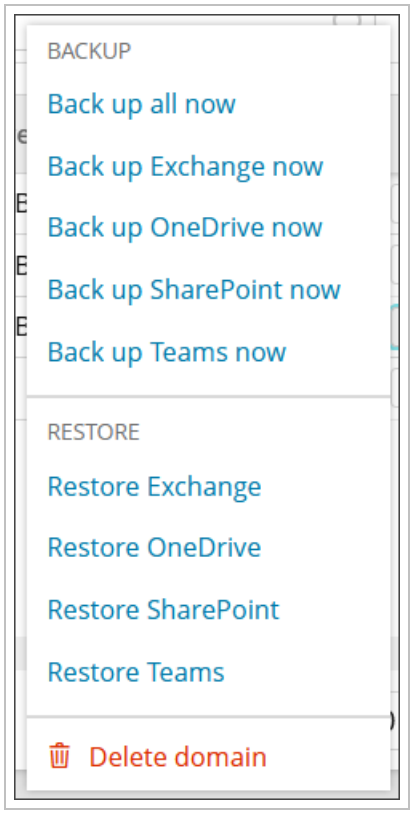
Action menu

The full selection of device management options is available through an action menu. It opens when you click the three vertical dots to the far right of the device, or when right clicking the device name. The view of the Action Menu changes depending on whether you are looking at a regular device or an Microsoft 365 device.

Regular backup device:



Microsoft 365 domain:



> For Microsoft 365 devices, only the services configured will be displayed in the Action Menu. For example, if your domain only has SharePoint configured, you will not see an option for Backup Exchange Now, Backup OneDrive Now, Restore Exchange or Restore OneDrive.

Views for Dashboards in Management Console

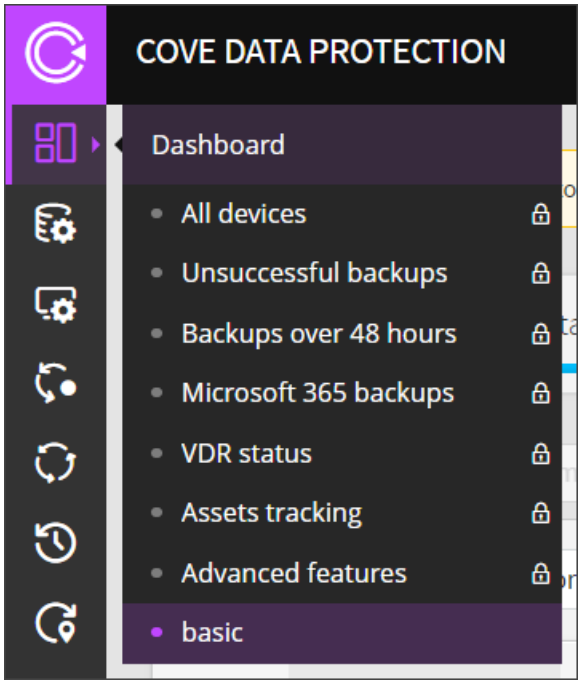
Manage statistics for backup devices with the help of views. You can change between **predefined views** and add new views and create email reports based on a certain view.

View management settings are **user-specific**. You cannot access views created by other users. The set of predefined views is identical for all.

Changing the view

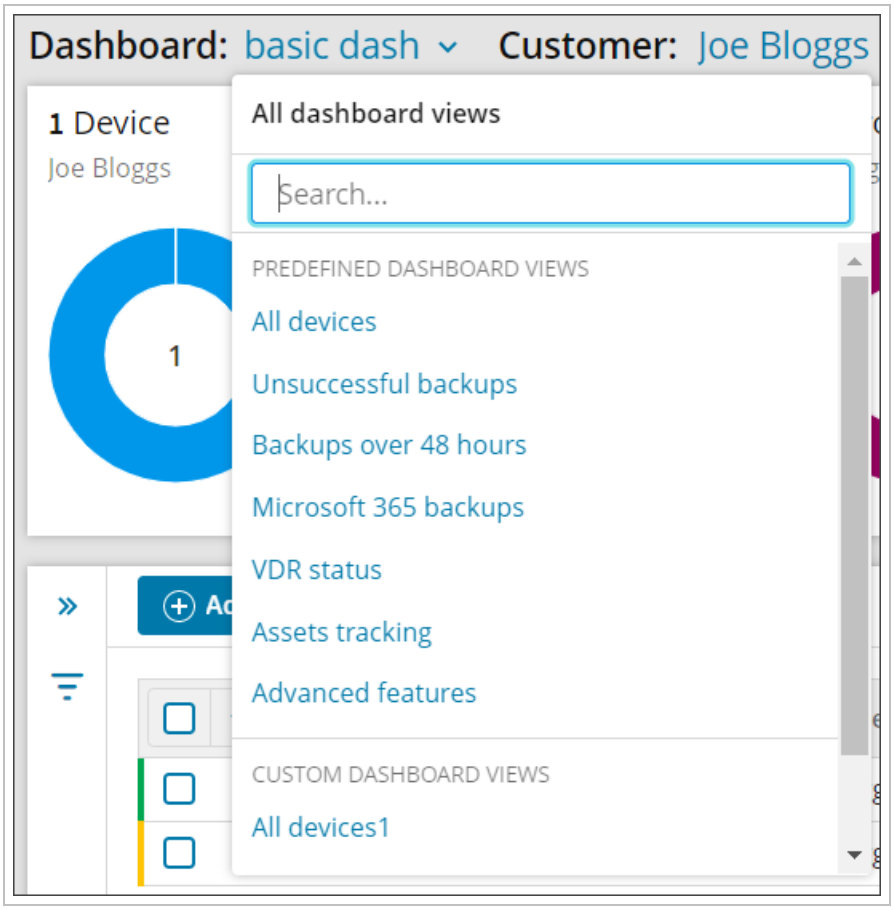
To change the current view to one previously saved, this can be done one of two ways:

1. Hover the cursor over **Backup** in the vertical menu and click on the view you want to apply



Or

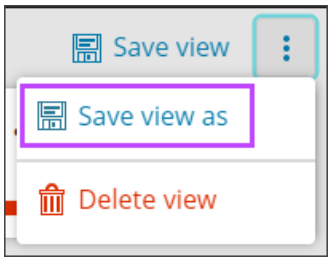
2. Click into the **Dashboard** dropdown at the top of the page, search for and select the view you want to apply



Adding new views

Create new views by basing these on existing views:

1. Apply any view to the dashboard
2. From the top of the page, select the three vertical dots to open the view action menu



3. Select **Save view as**
4. Specify the name for the view
5. Customize the view as needed
6. Click **Save view** once complete

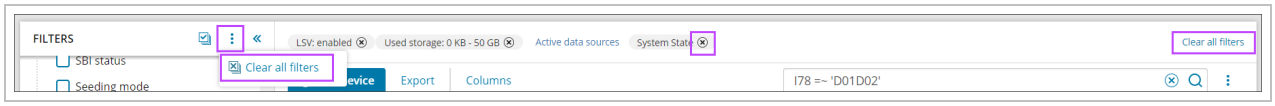
Please be aware, column codes have now changed to a new notation. Existing views that were built using old notation will still function, but we would recommend all new views are built using the new advanced filter expressions, found here.

Customizing Views

You can customize the view by using:

- Filters
- Widgets
- Basic or Advanced searches
- Selecting or deselecting columns to display
- Re-arranging the columns
  - This can be done by dragging and dropping columns into a different order
- Changing the width of columns
- Changing the sorting method (for example, by Customer in alphabetical order A-Z)

You can clear individual filters by clicking the **x** beside each one from the banner above the toolbar or clear all filters by clicking the **Clear all filters** button, or selecting it from the action menu by clicking the three vertical dots in the filter menu.



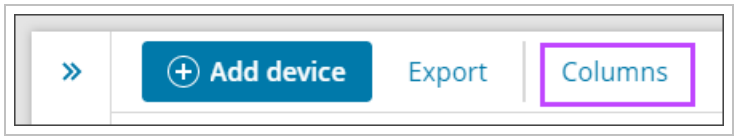
If changes have been made to a view that need to be undone, this can be done by using the Reset View option.

This can only be done if the view has **not** been saved since the changes were made.

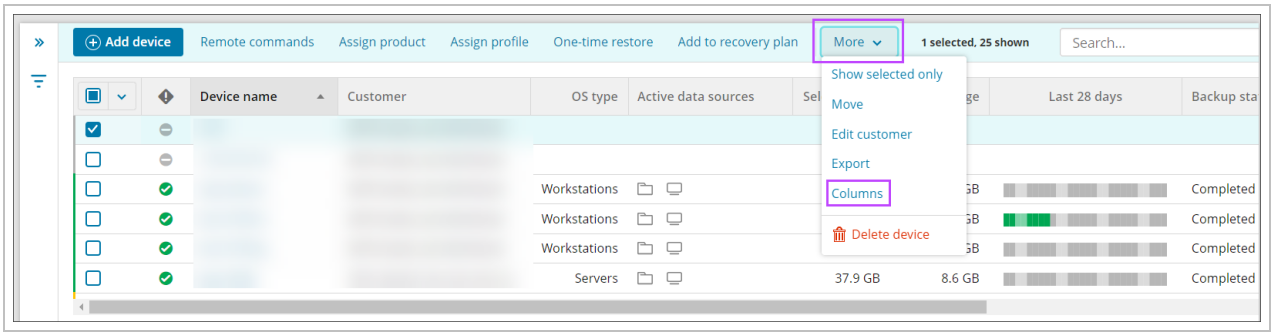
Columns to display

To add columns to the view, use the Columns option on the toolbar.

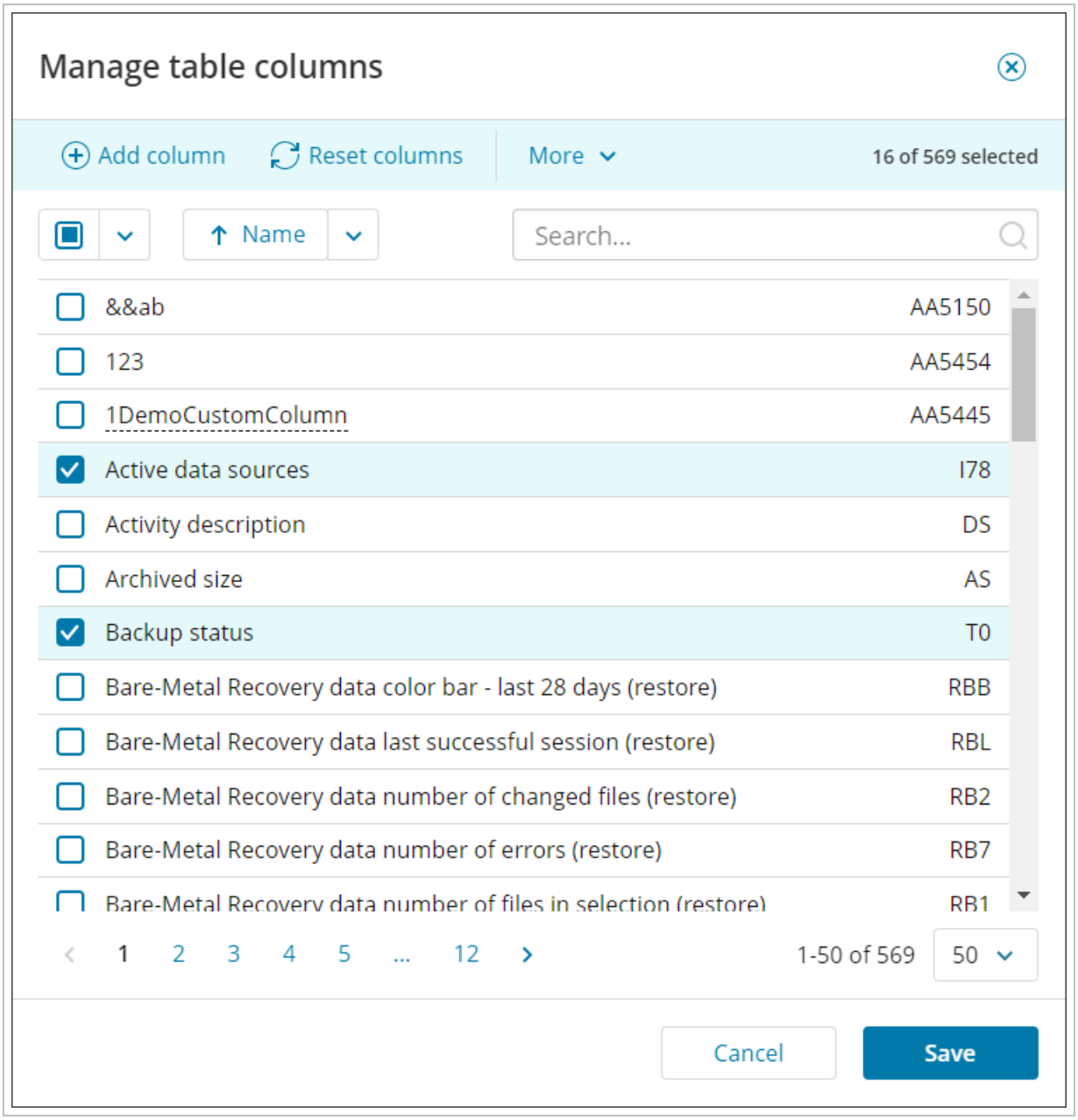
When no device or domain is selected, the Columns option is found on the toolbar.



However, when a device or domain is selected, the Columns option can be found in the More dropdown.


Add device
Remote commands
Assign product
Assign profile
One-time restore
Add to recovery plan
More
1 selected, 25 shown
Search...
Show selected only
Move
Edit customer
Export
Columns
Delete device
Device name
Customer
OS type
Active data sources
Last 28 days
Backup sta
Workstations
Workstations
Workstations
Servers
37.9 GB
8.6 GB
Completed
Completed
Completed
Completed

1. Once clicked, the **Manage table columns** window is shown



2. Select or deselect the columns required

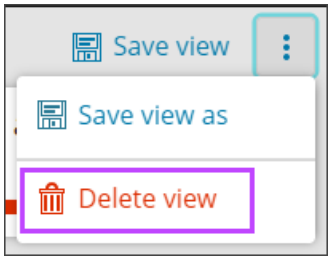
> There is no limit to the number of columns that can be added, you can see the number of columns selected at the top of the window

3. **Save** the changes made

In this window, you can also Add a custom column, reset columns, reset the column width and filter to show only the columns currently selected. You can also change the sorting method from column name to shortcode. For full details on column codes, see Expressions for advanced filter in Management Console.

Deleting custom views

To delete a custom view, first apply this view to your dashboard. Then open the view management menu from the top right-hand corner of the page by clicking the three vertical dots, and select **Delete view**.

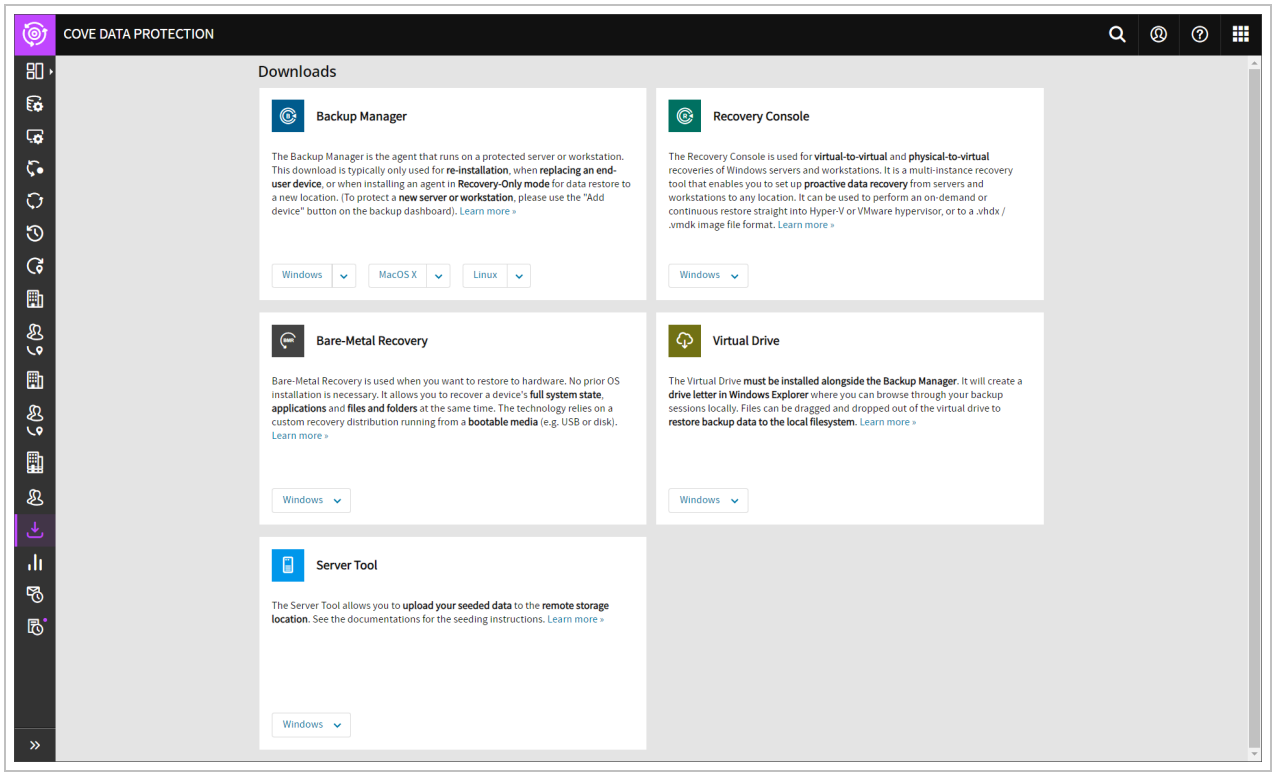


> The predefined views cannot be deleted (you will find the view management menu does not show the Delete option for these views).

Download tools in Management Console

From the Management Console, you can download tools related to Backup Manager from the **Downloads** page.

You can access this page by selecting **Downloads** from the Vertical menu to the right-hand side of the page.



> When installing Backup Manager, a download of the product will process as part of this, so you should not have to come in here to download Backup Manager.

Custom columns in Management Console

You can add custom columns to the **Devices** table. Custom columns with their values are visible to all users.

> Custom columns support **text values** only (no date or numeric functions are available for filtering). We strongly discourage storing sensitive information like encryption keys or passwords in custom columns.

Permissions required

- Actions related to custom columns require SuperUser permissions (adding, renaming and removing columns as well as adding data to them)
- Only custom columns created by users from your company can be renamed or removed (you will not have permission to edit columns created by other companies)
- Custom columns can only be added to views if these are internal (created by users from your company or a parent company)

Key

The following icons indicate availability:

Key	Status	Description
✅	Available	Is available for *all*
⚠	Available if additional criteria met	Is available for all, so long as an additional criteria is met (see * for additional information)
⛔	Not Available	Is **not** available

For distributor

Action	Columns created internally	Columns created by resellers and end-customers
View	✅	✅
Rename & remove	✅	⛔
Add to view	✅	⛔
Add data	✅	⛔

For reseller

Action	Columns created internally	Columns created by distributor	Columns created by end-customers
View	✅	✅	✅
Rename & remove	✅	⛔	⛔
Add to view	✅	✅	⛔
Add data	✅	✅	⛔

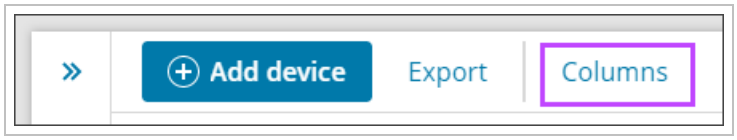
For end-customer

Action	Columns created internally	Columns created by distributor and reseller
View	✅	✅
Rename & remove	✅	⛔
Add to view	✅	✅
Add data	✅	✅

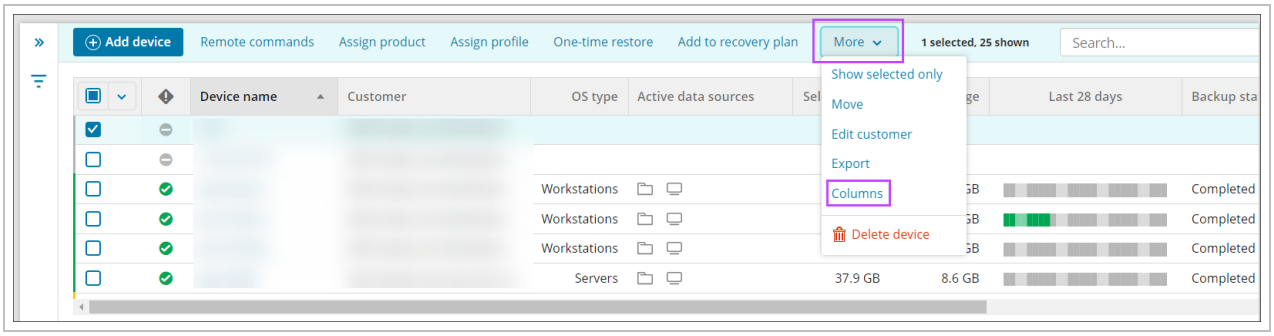
Columns to display

To add columns to the view, use the Columns option on the toolbar.

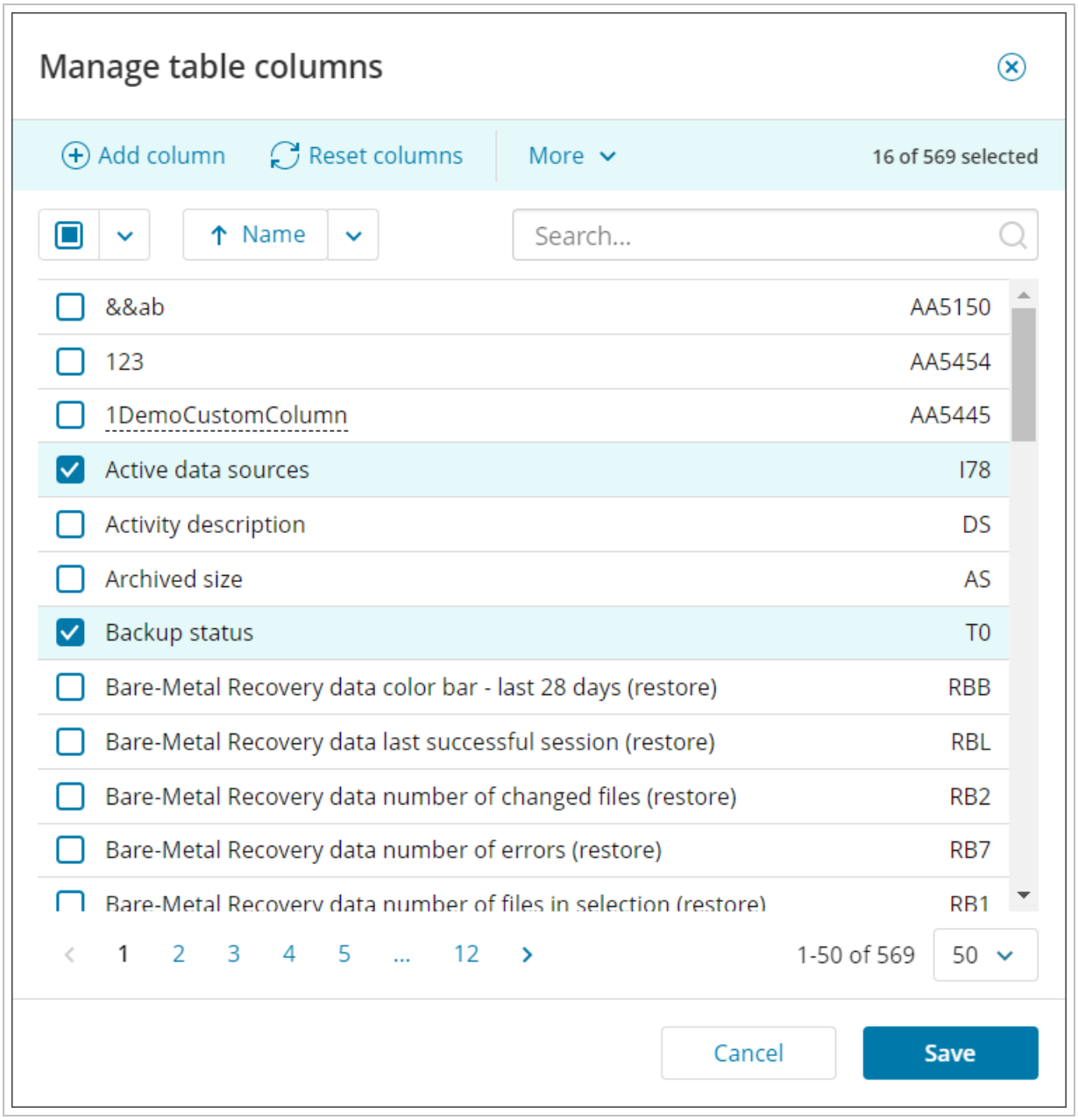
When no device or domain is selected, the Columns option is found on the toolbar.



However, when a device or domain is selected, the Columns option can be found in the More dropdown.


Add device
Remote commands
Assign product
Assign profile
One-time restore
Add to recovery plan
More
1 selected, 25 shown
Search...
Show selected only
Move
Edit customer
Export
Columns
Delete device
Device name
Customer
OS type
Active data sources
Last 28 days
Backup sta
Workstations
Workstations
Workstations
Servers
37.9 GB
8.6 GB
Completed
Completed
Completed
Completed

1. Once clicked, the **Manage table columns** window is shown



2. Select or deselect the columns required

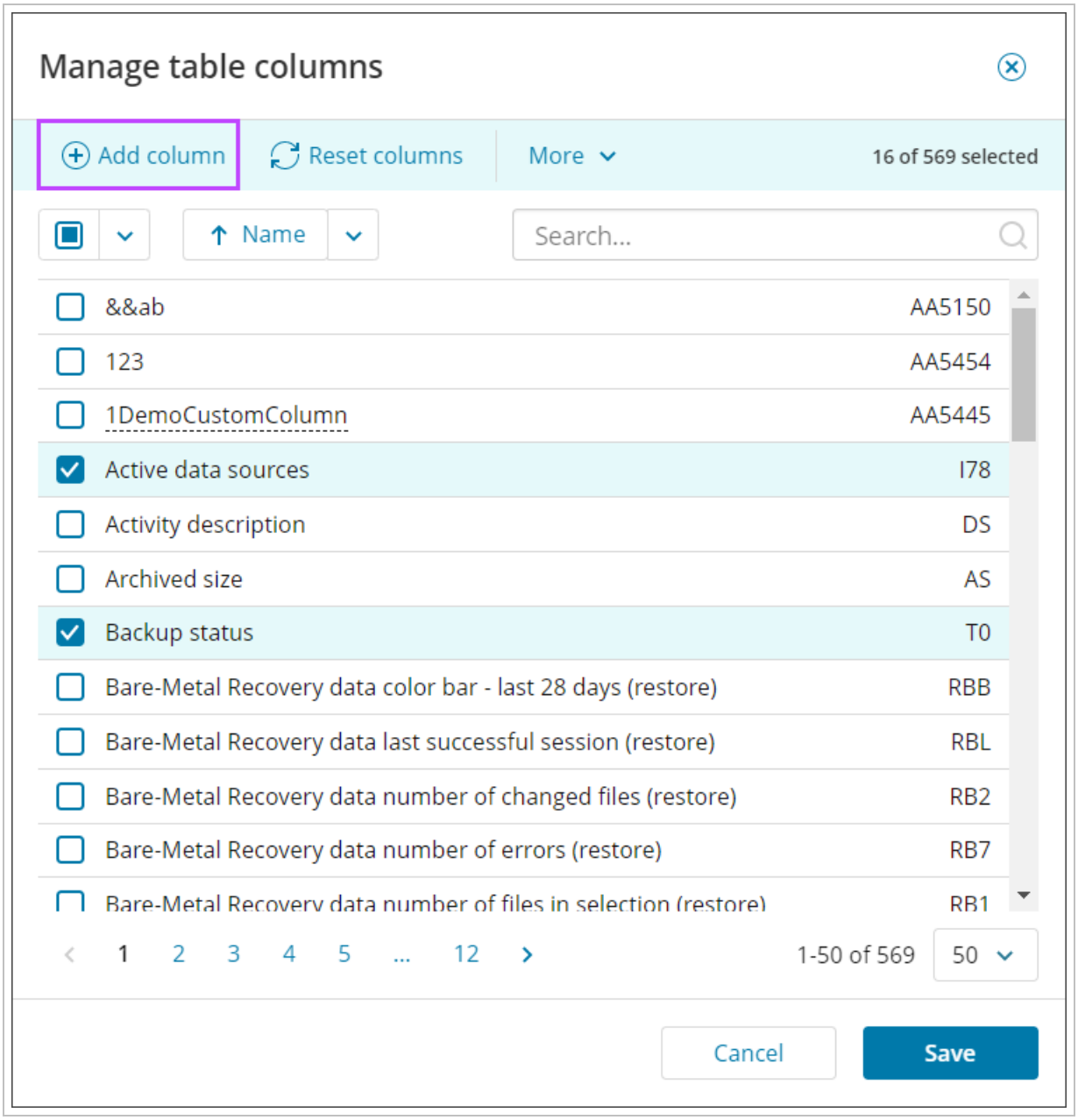
> There is no limit to the number of columns that can be added, you can see the number of columns selected at the top of the window

3. **Save** the changes made

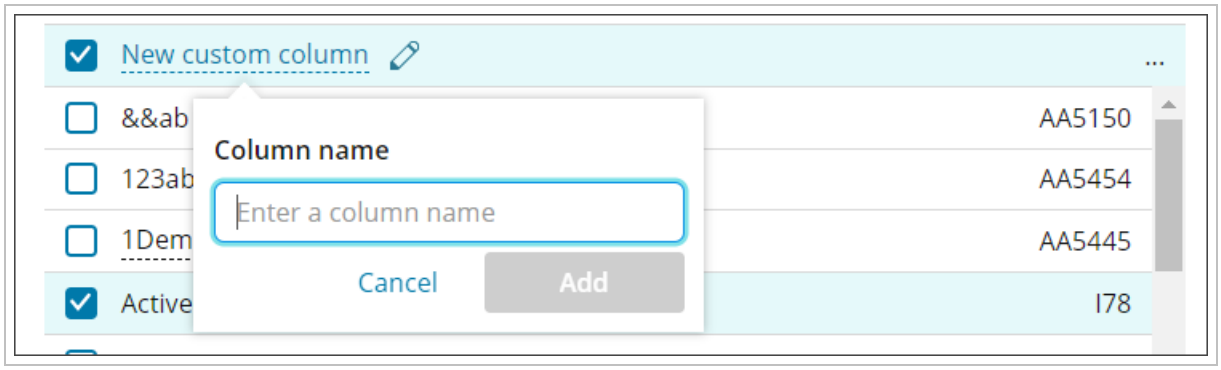
In this window, you can also Add a custom column, reset columns, reset the column width and filter to show only the columns currently selected. You can also change the sorting method from column name to shortcode. For full details on column codes, see Expressions for advanced filter in Management Console.

Adding custom columns

1. Log in to the Console under a SuperUser account
2. Click **Columns > Add column**



3. Enter a unique name to the column



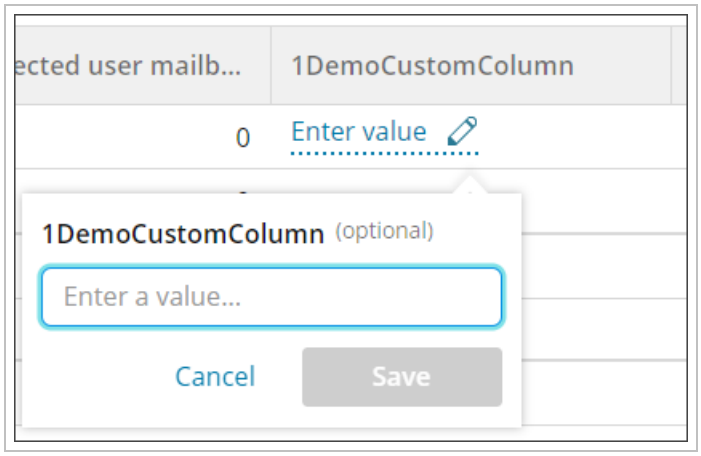
4. Click **Add**

> Each custom column acquires its unique **shortcode**, so you can easily identify it in the future.

Adding data to custom columns

> You can add data to columns created by users from your company and parent companies/groups (if applicable).

1. Add the column to your view following these steps
2. Point the cursor to the cell you want to update and click **Enter Value**

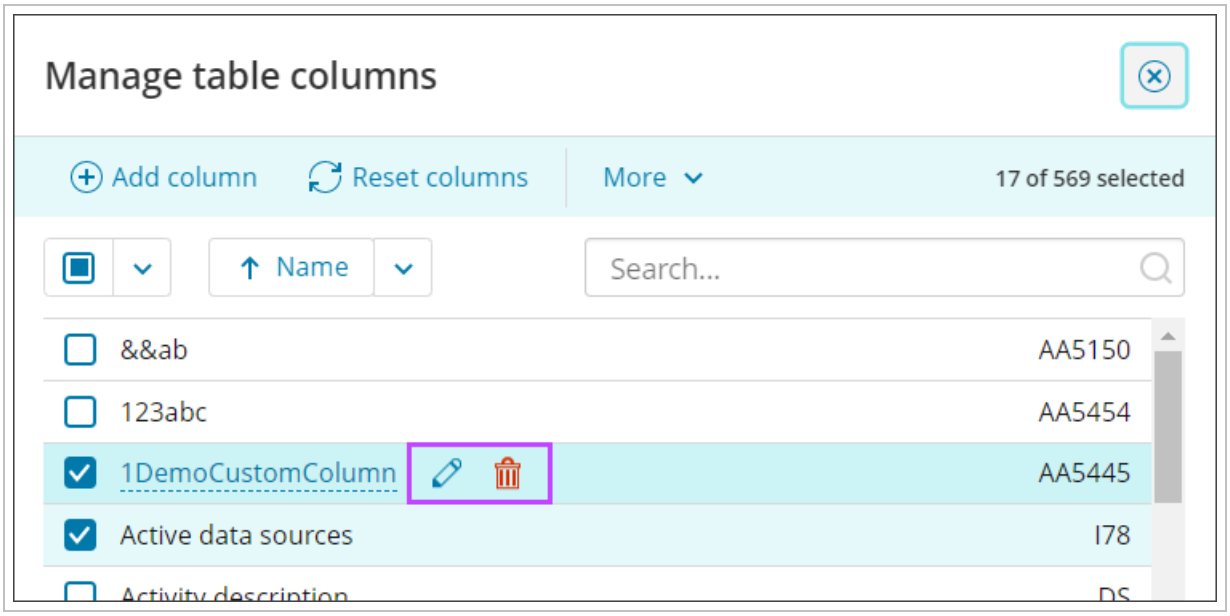


3. Enter your text
4. **Save** the changes

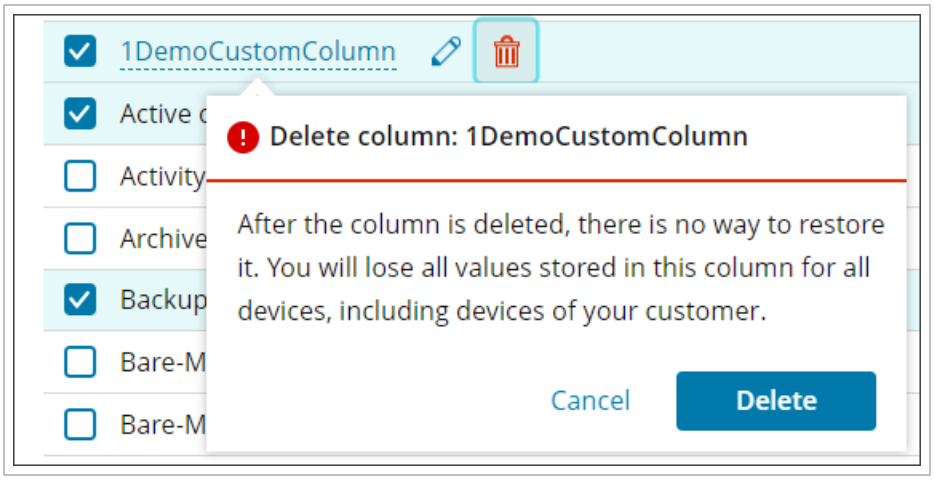
Managing custom columns

1. Log in to the Console under a SuperUser account
2. Open the **Columns** window and find custom column by scrolling or using the search function

3. Click the **Edit** or **Remove** icons next to the column you want to change



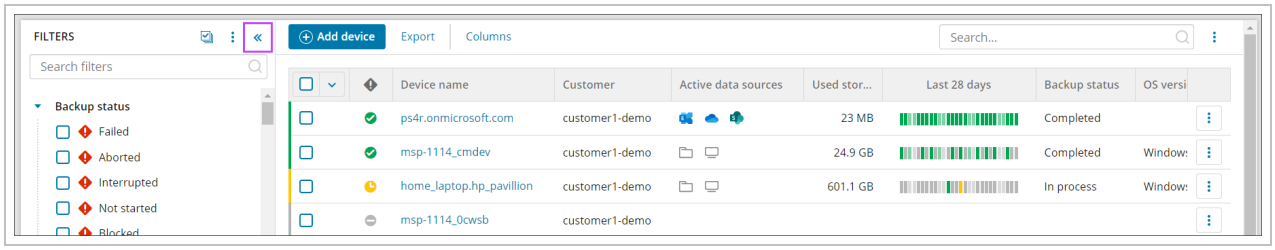
4. Editing allows you to change the custom column Name only. If deleting, you must confirm deletion:



> Columns created at a parent level to where you are logged in will not be editable or deletable. The **Edit** and **Remove** icons will be replaced by a padlock.

Filtering Devices in Management Console

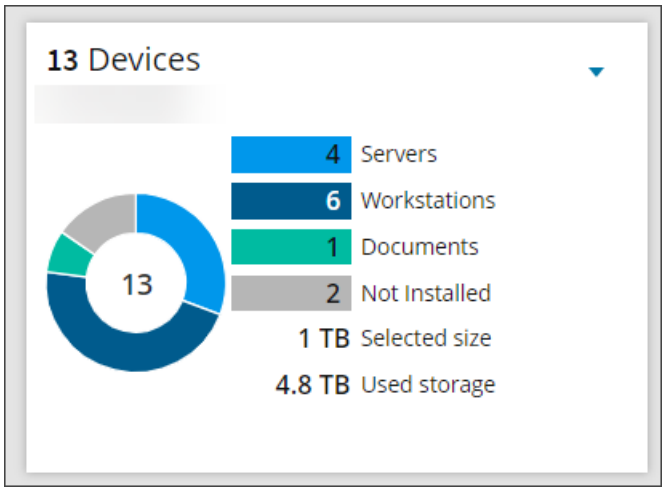
Users of all roles can filter devices and domains in the Management Console. Filtering devices can be done by using the predefined criteria in one of the graphic Widgets or by using the Filter Panel on the left of the devices list to narrow down the devices displayed.



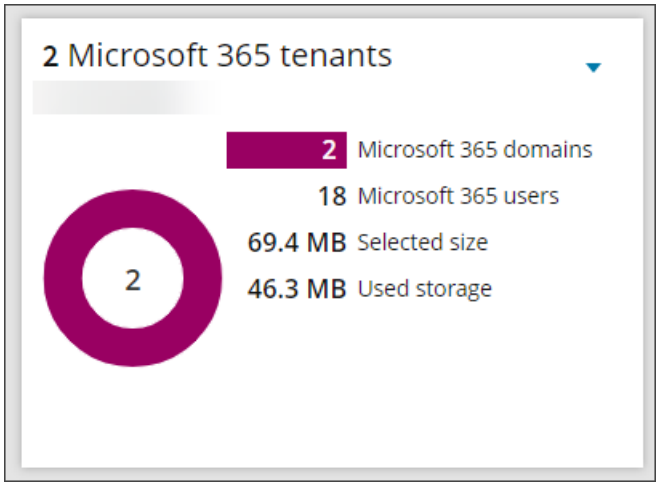
Widgets

In the Console, you will see 4 graphic widgets on the Backup Dashboard in the form of doughnut charts.

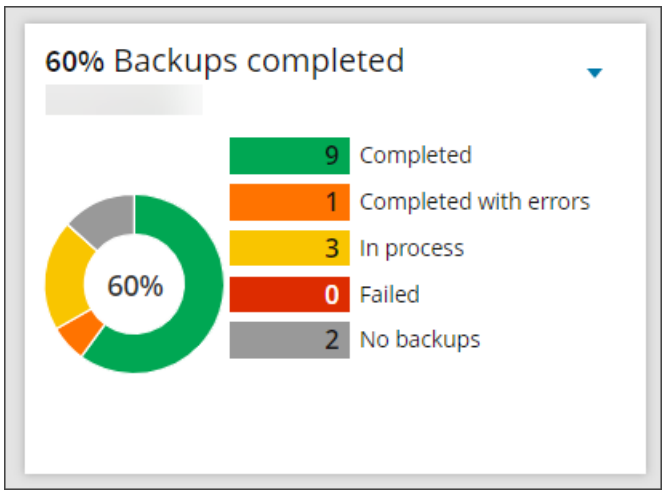
- The **Devices** widget illustrates the distribution of devices by the type with a choice of **Server, Workstation, Documents**and **Not Installed**. The selected size and used storage for these devices is displayed below



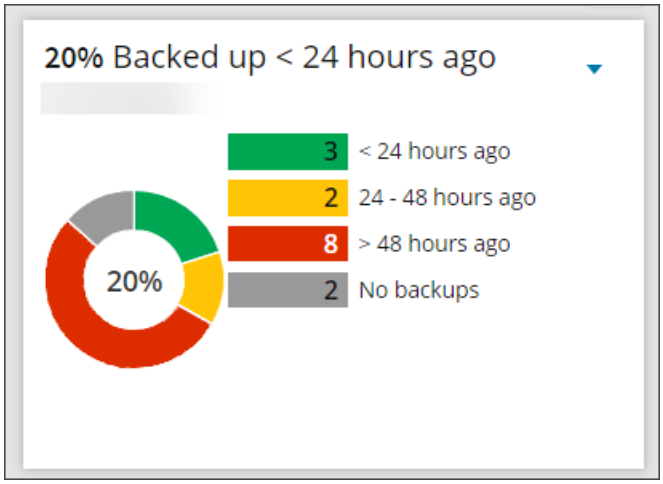
- The **Microsoft 365** widget gives a break down of the number of Microsoft 365 domains and users. The selected size and used storage are displayed below



- The **Backup Statuses** widget offers a breakdown of the statuses of the latest backup sessions for your devices



- The **Last Backup** widget shows a the timing of the latest backup sessions for your devices



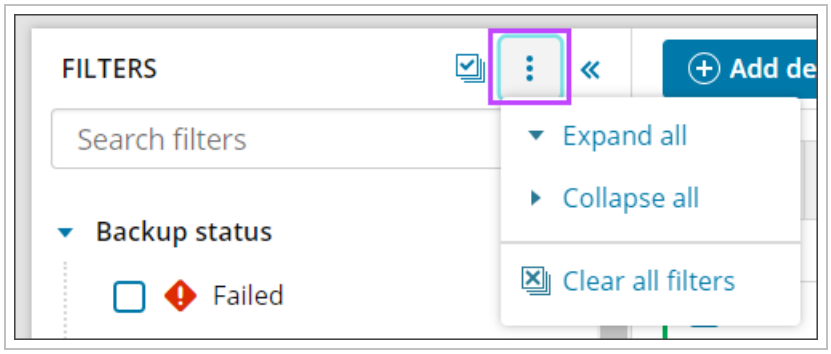
What you can do with these widgets:

- **Expand/minimize** a widget using the arrow icon in the top right corner
- **Select data on a widget and reset the filter** - By default, the widgets summarize statistics for the devices listed below (see the **Devices** widget). If you click on a value, the list of devices on the dashboard is immediately updated to match the selection

Filter Panel

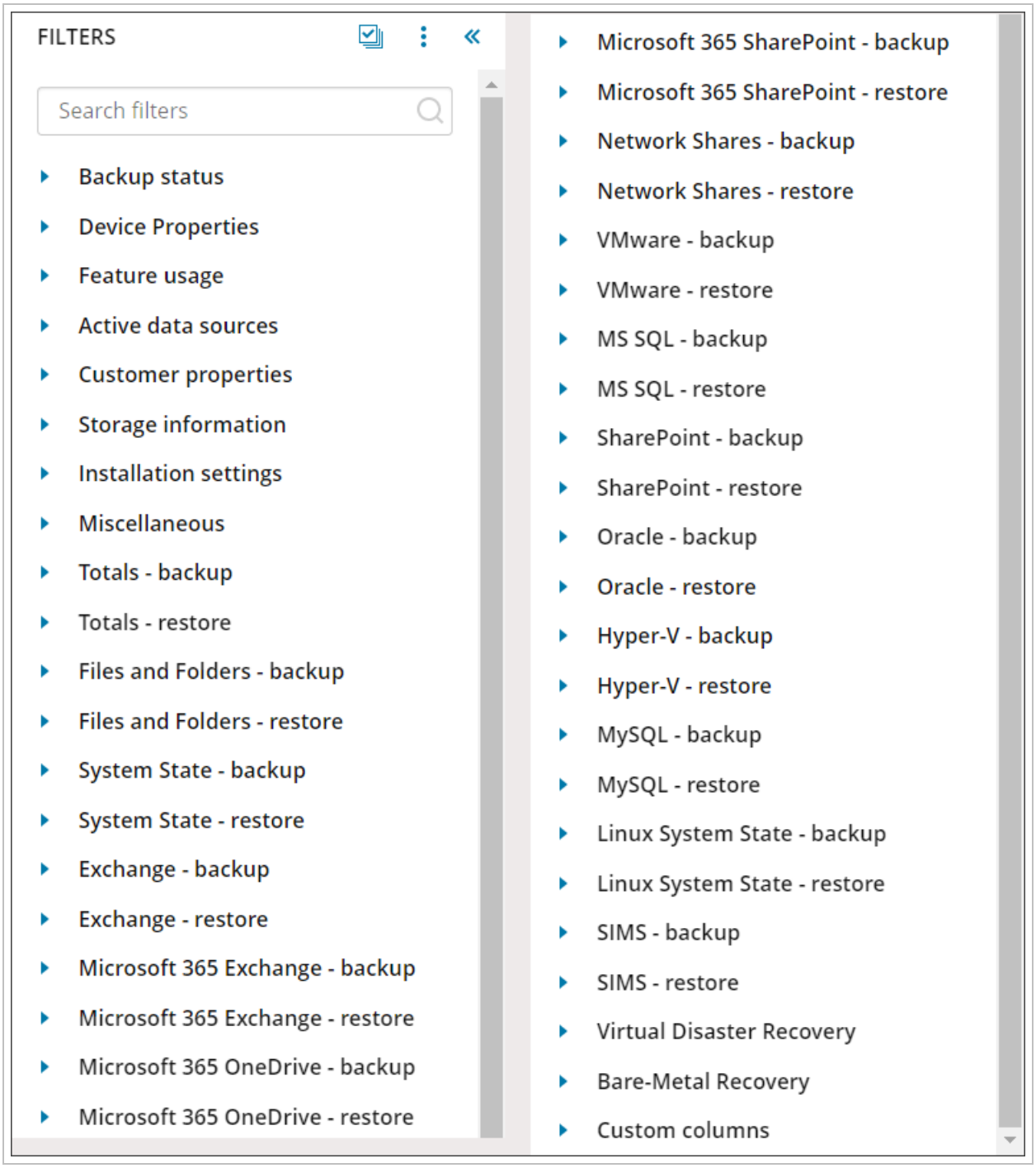
The filter panel can be accessed by clicking the two right-hand arrows (>>) on the toolbar.

It is possible to expand and collapse all of the filter sections by clicking the three vertical dots in the toolbar:



By default, the top 5 most commonly used filter sections will be expanded:

- **Backup Status** - Select from a list of the backup statuses including (but not limited to) Failed, Completed and In Process
- **Device Properties** - Several aspects of the device including (but not limited to) Device name, Product, Profile and Creation date
- **Feature Usage** - Select from a list of Cove features including (but not limited to) LocalSpeedVault, Seeding or a Recovery Plan
- **Active Data Sources** - Select from a list of data sources being backed up on the device including (but not limited to) Files and Folders, Microsoft 365 OneDrive and Network Shares
- **Customer Properties** - Which customer does the device belong to, search by customer name or a Partner reference



Using the Filters list, you can find devices that meet any multitude of criteria.

For example, if you would like to know which devices back up the System State data source, use a LocalSpeedVault and have a used storage of under 50GB, you can use the following filters:

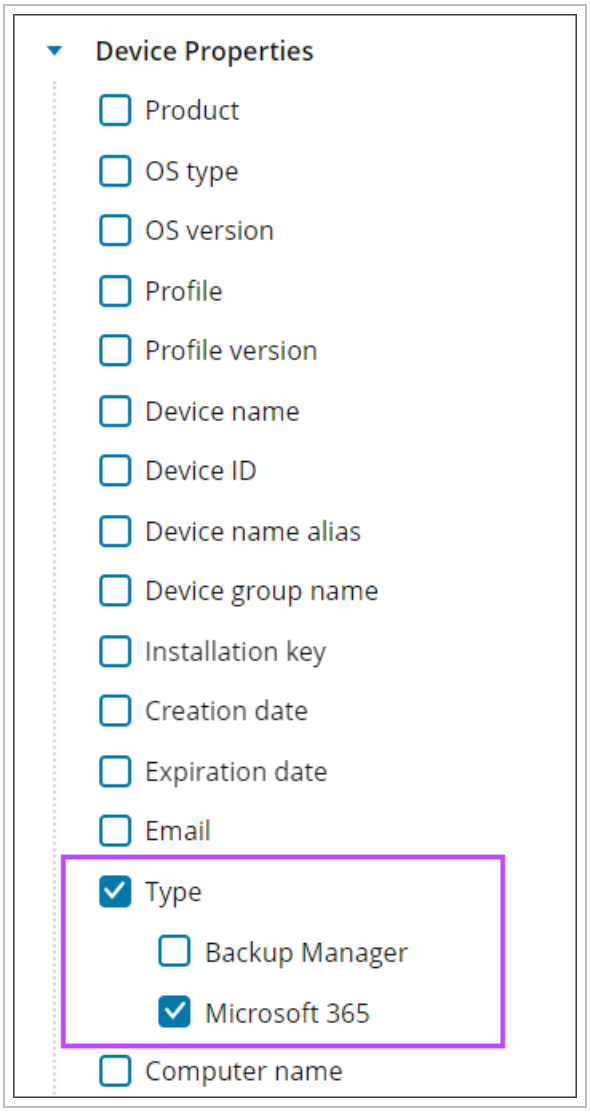
- **Active data sources** - System State
- **Feature Usage** - LSV, select enabled

- **Storage Information** - Used storage, use the slider bar to move the top marker down to 50GB

Filter for Microsoft 365 domains

To filter for Microsoft 365 domains only:

1. Use the **Filter** panel to the left of the devices list, this can be expanded or collapsed by clicking the two arrows (>> or <<)
2. Under the Device Properties filter heading, select the **type** filter
3. Tick **Microsoft 365**

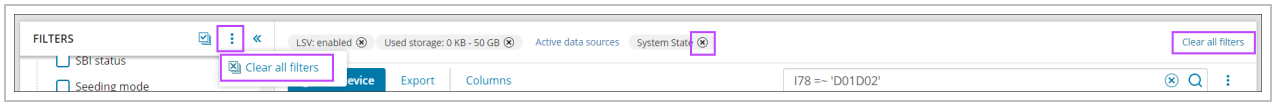


4. The devices list will automatically update to display the list of devices meeting this criteria
5. Click on a domain name to view the Domain's property tabs

Clear Filters

You can clear individual filters by clicking the **x** beside each one from the banner above the toolbar.

You can also clear all filters by clicking the **Clear all filters** button to the right-hand side of the toolbar or above the widgets, or by selecting it from the action menu by clicking the three vertical dots in the filter menu.

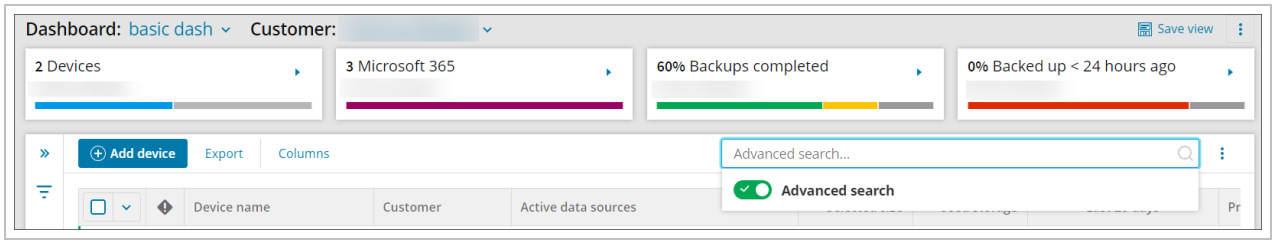


Searching in Management Console

The Search function in the Management Console, Backup Dashboard has two modes:

- Basic Search
- Advanced Search

Searching within the dashboard is done by clicking into the search box on the right-hand side of the Toolbar. You can switch between basic and advanced searching by using the toggle below the text box. By default, the search will open in the basic search mode.

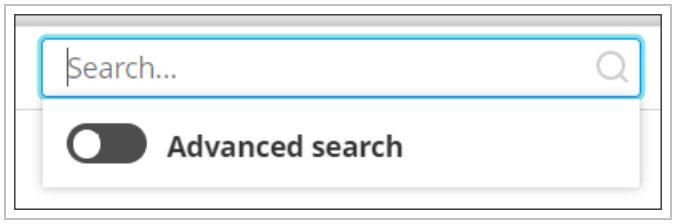


If using Filtering, the search box will automatically populate the appropriate search to find the same information, if enabling Advanced searching.

E.g. Filtering only for devices that have a Backup Status of **No backups** or **In Process**, when Advanced filtering is then enabled, the search box will pre-populate with `(T0 == 0 OR T0 == 1)`

> If using this feature, be aware that removing a filter will not automatically update the search text unless switching to basic then back to advanced searching.

Basic search



Basic searching can be used for solving basic tasks where the search criteria is a text-only value. It can be used for such columns as Device Name, Customer and Product.

For example:

```
.co.uk
```

To find all devices or domains using a .co.uk suffix

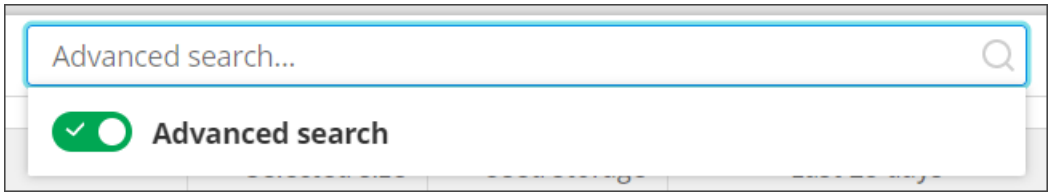
or

```
Server
```

To find all devices which are recognized as a Server Operating System Type, or that have 'server' in the device name

You can clear the search by clicking the **X** on the search bar.

Advanced search



Advanced searching can be used for non-text string values. It allows the use of advanced filter expressions to search column data for more complex or combined searches.

For example:

```
us > 10.giga()
```

To find all devices with a Used Storage of more than 10 GB

or

```
I78 =~ 'D01D02'
```

To list all devices which backup the Files and Folders and System State data sources

or

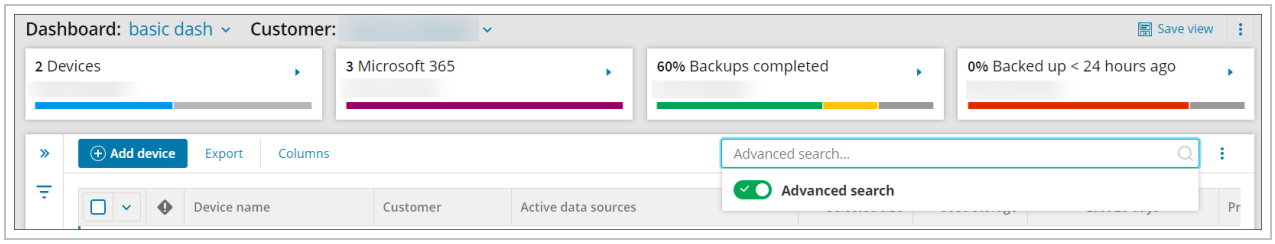
```
us > 10.giga () AND I78 =~ 'D01D02'
```

To list all devices with a Used Storage of more than 10 GB and which backup the Files and Folders and System State data sources

You can clear the search by clicking the **X** on the search bar.

Expressions for advanced filter in Management Console

You can find devices in the dashboard matching certain conditions using the advanced filter. To access it, click the arrow next to the filter field and select the **Advanced search** option.



Please note, the old legacy notations (found here) will still work for the time being, but we would strongly recommend you change to use the below notations as soon as possible.

Statistic field types

In this notation, there are three types of statistic fields:

- Common - All begin with the letter "I" (upper i) and be followed by a number

  Example: `I24` is used to request Time Zone
- Backup Plugin Statistic - This is a 'per-datasource' field

  Example: `D01F03` is used to request the selected size for the last backup session for the Files and Folders data source
- Restore Plugin Statistic - This is a 'per-datasource' field

  Example: `D01F03R` is used to request the selected size for the last restore session for the Files and Folders data source

When making requests for multiple data sources or fields per data source, these must be either line or comma separated. E.g. `D01F03, D02F03, D03F05`

Expressions for column titles

Primary device properties

Column title	Short name	Type of data
Device name	AN	String
Installation key	QW	String
Device ID	AU	String
Device group name	AG	String
Device name alias	AL	String
Customer	AR	String
Creation date	CD	Time
Expiration date	ED	Time

Column title	Short name	Type of data
Product	PN	String
Retention units	RU	String
Email	EM	String

Installation details

Column title	Short name	Type of data
Client version	VN	String
Computer name	MN	String
Computer manufacturer	MF	String
Computer model	MO	String
OS version ?[1]	OS	String
OS type ?[2]	OT	▪ 1 - workstation ▪ 2 - server ▪ 0 - undefined
MAC address	MA	String
Internal IPs	IP	String
Time offset	TZ	Number

Storage info

Column title	Short name	Type of data
Storage location ?[3]	LN	String
Used storage	US	Size
Storage status	YS	▪ -2 - Offline ▪ -1 - Failed ▪ 0 - Undefined

---

[1]Name and version of Operating System
[2]Operating System type
[3]Location of the home node

Column title	Short name	Type of data
		▪ 50 - Running ▪ 100 - Synchronized

Feature usage

Column title	Short name	Type of data
Active data sources	AP	String
LSV ?[1]	VE	▪ 0 - Disabled ▪ 1 - Enabled
LSV status	YV	▪ -2 - Offline ▪ -1 - Failed ▪ 0 - Undefined ▪ 50 - Running ▪ 100 - Synchronized
SBI ?[2]	IE	▪ 0 - Disabled ▪ 1 - Enabled
SBI status	IT	▪ 1 - In process ▪ 2 - Failed ▪ 3 - Aborted ▪ 5 - Completed ▪ 6 - Interrupted ▪ 7 - NotStarted ▪ 8 - CompletedWithErrors ▪ 9 - InProgressWithFaults ▪ 10 - OverQuota ▪ 11 - NoSelection ▪ 12 - Restarted
Seeding mode	IS	▪ 0 - Undefined ▪ 1 - Normal

---

[1] LocalSpeedVault enabled
[2] Standby Image enabled

Column title	Short name	Type of data
		▪ 2 - Seeding ▪ 3 - PreSeeding ▪ 4 - PostSeeding

Miscellaneous

Column title	Short name	Type of data
Archived size	AS	String
Account type	AT	String
Dashboard frequency	DF	Bitmask
Dashboard language	DL	String
Activity description	DS	String
External IPs	EI	String
Number of ESX virtual machines	EN	String
Encryption status	ES	String
Number of Hyper-V virtual machines	HN	String
SKU	KU	String
Profile	OP	String
Own user name	OU	String
Profile version	OV	String
Customer reference	PF	String
SKU of the previous month	PU	String
Restore email	REM	String
Restore dashboard frequency	RDF	Bitmask
Restore dashboards language	RDL	String
Timestamp	TS	Unix time
Proxy type	PT	String

Backup statistics per data source (continued)

Column title	System State	Files and Folders	MySQL	Network Shares	VSS MS SQL	Exchange Stores
Status	S0	F0	L0	N0	Z0	X0
Number of files in selection	S1	F1	L1	N1	Z1	X1
Number of changed files	S2	F2	L2	N2	Z2	X2
Selected size	S3	F3	L3	N3	Z3	X3
Processed size	S4	F4	L4	N4	Z4	X4
Sent size	S5	F5	L5	N5	Z5	X5
Protected size	S6	F6	L6	N6	Z6	X6
Number of errors	S7	F7	L7	N7	Z7	X7
Session duration	SA	FA	LA	NA	ZA	XA
Last successful session	SL	FL	LL	NL	ZL	XL
Status of the last successful session	SQ	FQ	LQ	NQ	ZQ	XQ
Status of the last completed session	SJ	FJ	LJ	NJ	ZJ	XJ
Timestamp of the last completed session	SO	FO	LO	NO	ZO	XO
Retention	SR	FR	LR	NR	ZR	XR
Color bar - last 28 days	SB	FB	LB	NB	ZB	XB
Session verification details	SK	FK	LK	NK	ZK	XK
License items count	-	-	-	NI	-	-

Backup statistics per data source (continued)

Column title	Total backup	SharePoint data	Oracle	VMware virtual machines	Hyper-V data
Status	T0	P0	Y0	W0	H0
Selected count	T1	P1	Y1	W1	H1

Column title	Total backup	SharePoint data	Oracle	VMware virtual machines	Hyper-V data
Number of files in selection	T	P2	Y2	W2	H2
Changed count	T2	P3	Y3	W3	H3
Number of changed files	-	P4	Y4	W4	H4
Selected size	T3	P5	Y5	W5	H5
Processed size	T4	P6	Y6	W6	H6
Sent size	T5	P7	Y7	W7	H7
Protected size	T6	PA	YA	WA	HA
Errors	T7	PL	YL	WL	HL
Number of errors	-	PQ	YQ	WQ	HQ
Session Duration	-	PJ	YJ	WJ	HJ
Last successful session	TL	PO	YO	WO	HO
Last successful session status	-	PR	YR	WR	HR
Status of the last successful session	TQ	PB	YB	WB	HB
Last session status	TJ	PK	YK	WK	HK
Status of the last completed session	-	-	-	WI	HI
Timestamp of the last completed session	TO	-	-	-	-
Session verification details	TK	-	-	-	-
Protected user mailboxes	TM	-	-	-	-

Backup Statistics per Microsoft 365 Service

Column title	Microsoft 365 Exchange	Microsoft 365 SharePoint	Microsoft 365 OneDrive	Microsoft Teams
Status	G0	D5F0	J0	D23F0
Number of files in selection	G1	D5F1	J1	D23F1
Number of changed files	G2	D5F2	J2	D23F2

Column title	Microsoft 365 Exchange	Microsoft 365 SharePoint	Microsoft 365 OneDrive	Microsoft Teams
Selected size	G3	D5F3	J3	D23F3
Processed size	G4	D5F4	J4	D23F4
Sent size	G5	D5F5	J5	D23F5
Protected size	G6	D5F7	J6	D23F7
Number of errors	G7	D5F6	J7	D23F6
Session Duration	GA	D5F12	JA	D23F12
Color bar - last 28 days	GB	D5F8	JB	D23F8
Status of the last completed session	GJ	D5F17	JJ	D23F17
Session verification details	GK	D5F19	JK	D23F19
Last successful session	GL	D5F9	JL	D23F9
Protected user mailboxes	GM	D5F20	JM	-
Timestamp of the last completed session	GO	D5F18	JO	D23F18
Status of the last successful session	GQ	D5F16	JQ	D23F16
Retention	GR	D5F14	JR	D23F14
Protected shared mailboxes	G@	-	-	-
Protected sites	-	D5F22	-	-
Protected owners	-	-	-	D23F20
Protected teams	-	-	-	D23F23
Protected channels	-	-	-	D23F24
Protected messages	-	-	-	D23F25
Auto add new entities	D19F26	D5F26	D20F26	D23F26

Status outputs are displayed as one of the following numeric values:

Value	Meaning
`[1]`	InProcess

Value	Meaning
[2]	Failed
[3]	Aborted
[5]	Completed
[6]	Interrupted
[7]	NotStarted
[8]	CompletedWithErrors
[9]	InProgressWithFaults
[10]	OverQuota
[11]	NoSelection
[12]	Restarted

Restore statistics per data source

Column title	System State	Files and Folders	Bare Metal Recovery data	Virtual Disaster Recovery data	MySQL	Network Shares	VSS MS SQL	Exchange stores
Status (restore)	RS0	RF0	RB0	RV0	RL0	RN0	RZ0	RX0
Number of files in selection (restore)	RS1	RF1	RB1	RV1	RL1	RN1	RZ1	RX1
Number of changed files (restore)	RS2	RF2	RB2	RV2	RL2	RN2	RZ2	RX2
Selected size (restore)	RS3	RF3	RB3	RV3	RL3	RN3	RZ3	RX3
Processed size (restore)	RS4	RF4	RB4	RV4	RL4	RN4	RZ4	RX4

Column title	System State	Files and Folders	Bare Metal Recovery data	Virtual Disaster Recovery data	MySQL	Network Shares	VSS MS SQL	Exchange stores
Sent size (restore)	RS5	RF5	RB5	RV5	RL5	RN5	RZ5	RX5
Number of errors (restore)	RS7	RF7	RB7	RV7	RL7	RN7	RZ7	RX7
Session duration (restore)	RSA	RFA	RBA	RVA	RLA	RNA	RZA	RXA
Last successful session (restore)	RSL	RFL	RBL	RVL	RLL	RNL	RZL	RXL
Status of the last successful session (restore)	RSQ	RFQ	RBQ	RVQ	RLQ	RNQ	RZQ	RXQ
Status of the last completed session (restore)	RSJ	RFJ	-	RVJ	RLJ	RNJ	RZJ	RXJ
Timestamp of the last completed session (restore)	RSO	RFO	RBO	RVO	RLO	RNO	RZO	RXO
Color bar - last 28 days (restore)	RSB	RFB	RBB	RVB	RLB	RNB	RZB	RXB
Session verification details (restore)	RSK	RFK	RBK	RVK	RLK	RNK	RZK	RXK

Restore statistics per data source (continued)

Column title	Total	SharePoint data	Oracle	VMware virtual machines	Hyper-V data
Status (restore)	RT0	RP0	RY0	RW0	RH0
Number of files in selection (restore)	RT1	RP1	RY1	RW1	RH1
Number of changed files (restore)	RT2	RP2	RY2	RW2	RH2
Selected size (restore)	RT3	RP3	RY3	RW3	RH3
Processed size (restore)	RT4	RP4	RY4	RW4	RH4
Sent size (restore)	RT5	RP5	RY5	RW5	RH5
Number of errors (restore)	RT7	RP7	RY7	RW7	RH7
Session duration (restore)	-	RPA	RYA	RWA	RHA
Last successful session (restore)	RTL	RPL	RYL	RWL	RHL
Status of the last successful session (restore)	RTQ	RPQ	RYQ	RWQ	RHQ
Status of the last completed session (restore)	RTJ	RPJ	RYJ	RWJ	RHJ
Timestamp of the last completed session (restore)	RTO	RPO	RYO	RWO	RHO
Color bar - last 28 days (restore)	RTB	RPB	RYB	RWB	RHB
Session verification details (restore)	RTK	RPK	RYK	RWK	RHK
Protected user mailboxes (restore)	RTM	-	-	-	-

Restore Statistics per Microsoft 365 Service

Column title	Microsoft 365 Exchange	Microsoft 365 SharePoint	Microsoft 365 OneDrive	Microsoft Teams
Status (restore)	RG0	D5F0R	RJ0	D23F0R
Number of files in selection (restore)	RG1	D5F1R	RJ1	D23F1R
Number of changed files (restore)	RG2	D5F2R	RJ2	D23F2R
Selected size (restore)	RG3	D5F3R	RJ3	D23F3R

Column title	Microsoft 365 Exchange	Microsoft 365 SharePoint	Microsoft 365 OneDrive	Microsoft Teams
Processed size (restore)	RG4	D5F4R	RJ4	D23F4R
Sent size (restore)	RG5	D5F5R	RJ5	D23F5R
Number of errors (restore)	RG7	D5F6R	RJ7	D23F6R
Session duration (restore)	RGA	D5F12R	RJA	D23F12R
Color bar - last 28 days (restore)	RGB	D5F8R	RJB	D23F8R
Status of the last completed session (restore)	RGJ	D5F17R	RJJ	D23F17R
Session verification details (restore)	RGK	D5F19R	RJK	D23F19R
Protected user mailboxes (restore)	RGM	D5F20R	RJM	-
Timestamp of the last completed session (restore)	RGO	D5F18R	RJO	D23F18R
Status of the last successful session (restore)	RGQ	D5F16R	RJQ	D23F16R
Last successful session (restore)	RGL	D5F9R	RJL	D23F9R
Protected shared mailboxes (restore)	RG@	-	-	-
Protected sites (restore)	-	D5F22R	-	-
Protected teams	-	-	-	D23F23R
Protected channels	-	-	-	D23F24R
Protected messages	-	-	-	D23F25R
Auto add new entities (restore)	D19F26R	D5F26R	D20F26R	D23F26R

Expressions for active data sources

See the list of Backup data sources here, with the legacy shortnames detailed for ease:

Full Name	New ID	Legacy Shortname
Files and Folders	D1	F
System State	D2	S

Full Name	New ID	Legacy Shortname
MsSql	D3	Q
VssExchange	D4	X
Microsoft 365 SharePoint	D5	--
NetworkShares	D6	N
VssSystemState	D7	S
VMware Virtual Machines	D8	W
Total	D9	T
VssMsSql	D10	Z
VssSharePoint	D11	P
Oracle	D12	Y
Hyper-V	D14	H
MySql	D15	L
Virtual Disaster Recovery	D16	V
Bare Metal Restore	D17	B
Microsoft 365 Exchange	D19	G
Microsoft 365 OneDrive	D20	J
Microsoft Teams	D23	--
Removable Media	--	R

Example

For example, if you want to find the devices that back up "Files and Folders" and "System State" only, the advanced filter expression looks as follows:

```
I78 =~ 'D01D02'
```

Breakdown

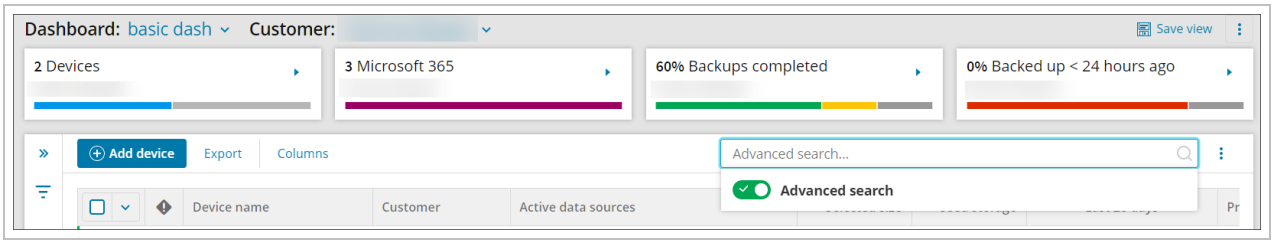
- `I78`: this is new notation meaning "Show active data sources"
- `D01`: data source matching 'D01' for Files and Folders
- `D02`: data source matching 'D02' for System State"

> As you are using "I78" here, the data source ID must be in the new notation.

Expressions for advanced filter in Management Console (Legacy)

> Please note, we have new filter expressions which should be used as soon as you are able. These can be found here.

You can find devices matching certain conditions using the advanced filter. To access it, click the arrow next to the filter field and select the **Advanced search** option.



Below is the list of expressions for column titles and the names of active data sources.

Expressions for column titles

Primary device properties

Short name	Column title	Type of data
AN	Device name	String
QW	Password	String
AU	Device ID	String
AL	Device name alias	String
AR	Customer	String
CD	Creation date	Time
ED	Expiration date	Time
PN	Product	String
RU	Retention units	String
EM	Email	String

Installation details

Short name	Column title	Type of data
VN	Client version	String

Short name	Column title	Type of data
MN	Computer name	String
MF	Computer manufacturer	String
MO	Computer model	String
OS	OS version ?[1]	String
OT	OS type ?[2]	▪ `1` - workstation ▪ `2` - server ▪ `0` - undefined
MA	MAC address	String
IP	Internal IPs	String
TZ	Time offset	Number

Storage info

Short name	Column title	Type of data
LN	Storage location ?[3]	String
US	Used storage	Size
YS	Storage status	▪ `-2` - Offline ▪ `-1` - Failed ▪ `0` - Undefined ▪ `50` - Running ▪ `100` - Synchronized

Feature usage

Short name	Column title	Type of data
AP	Active data sources	String

---

[1]Name and version of Operating System
[2]Operating System type
[3]Location of the home node

Short name	Column title	Type of data
VE	LSV ?[1]	▪ 0 - Disabled ▪ 1 - Enabled
YV	LSV status	▪ -2 - Offline ▪ -1 - Failed ▪ 0 - Undefined ▪ 50 - Running ▪ 100 - Synchronized
IS	Seeding mode	▪ 0 - Undefined ▪ 1 - Normal ▪ 2 - Seeding ▪ 3 - PreSeeding ▪ 4 - PostSeeding

Miscellaneous

Short name	Column title	Type of data
AG	Device group name	String
AS	Archived size	String
AT	Account type	String
DF	Dashboard frequency	Bitmask
DL	Dashboard language	String
DS	Activity description	String
EI	External IPs	String
EN	Number of ESX virtual machines	String
ES	Encryption status	String
HN	Number of Hyper-V virtual machines	String
KU	SKU	String
OP	Profile	String

[1] LocalSpeedVault enabled

Short name	Column title	Type of data
OU	Own user name	String
OV	Profile version	String
PF	Customer reference	String
PU	SKU of the previous month	String
REM	Restore email	String
RDF	Restore dashboard frequency	Bitmask
RDL	Restore dashboards language	String
TS	Timestamp	Unix time

Backup statistics by the data source (continued)

Column title	System State	Files and Folders	Network Shares	VSS MSSQL	Exchange Stores	SharePoint data	Oracle	VMware virtual machines	Hyper-V data	MySQL status
Status	S0	F0	N0	Z0	X0	P0	Y0	W0	H0	L0
Number of files in selection	S1	F1	N1	Z1	X1	P1	Y1	W1	H1	L1
Number of changed files	S2	F2	N2	Z2	X2	P2	Y2	W2	H2	L2
Selected size	S3	F3	N3	Z3	X3	P3	Y3	W3	H3	L3
Processed size	S4	F4	N4	Z4	X4	P4	Y4	W4	H4	L4
Sent size	S5	F5	N5	Z5	X5	P5	Y5	W5	H5	L5
Protected size	S6	F6	N6	Z6	X6	P6	Y6	W6	H6	L6

Column title	System State	Files and Folders	Network Shares	VSS MSSQL	Exchange Stores	SharePoint data	Oracle	VMware virtual machines	Hyper-V data	MySQL status
Number of errors	S7	F7	N7	Z7	X7	P7	Y7	W7	H7	L7
Session duration	SA	FA	NA	ZA	XA	PA	YA	WA	HA	LA
Last successful session	SL	FL	NL	ZL	XL	PL	YL	WL	HL	LL
Status of the last successful session	SQ	FQ	NQ	ZQ	XQ	PQ	YQ	WQ	HQ	LQ
Status of the last completed session	SJ	FJ	NJ	ZJ	XJ	PJ	YJ	WJ	HJ	LJ
Timestamp of the last completed session	SO	FO	NO	ZO	XO	PO	YO	WO	HO	LO
Retention	SR	FR	NR	ZR	XR	PR	YR	WR	HR	LR
Color bar - last 28 days	SB	FB	NB	ZB	XB	PB	YB	WB	HB	LB
Session verification details	SK	FK	NK	ZK	XK	PK	YK	WK	HK	LK
Licence items count	-	-	NI	-	-	-	-	WI	HI	-

Backup statistics by the data source (continued)

Column title	Total	Microsoft 365 Exchange	Microsoft 365 OneDrive
Status	T0	G0	J0
Selected count	T1	-	-
Number of files in selection	-	G1	J1
Changed count	T2	-	-
Number of changed files	-	G2	J2
Selected size	T3	G3	J3
Processed size	T4	G4	J4
Sent size	T5	G5	J5
Protected size	T6	G6	J6
Errors	T7	-	-
Number of errors	-	G7	J7
Session Duration	-	GA	JA
Last successful session	TL	GL	JL
Last successful session status	TQ	-	-
Status of the last successful session	-	GQ	JQ
Last session status	TJ	-	-
Status of the last completed session	-	GJ	JJ
Last session time	TO	-	-
Timestamp of the last completed session	-	GO	JO
Retention	-	GR	JR
Last 28 days	TB	-	-
Color bar - last 28 days	-	GB	JB
Session verification details	TK	GK	JK
Protected user accounts	TM	-	JM
Protected shared accounts	T@	-	-
Protected regular mailboxes	-	GM	-

Column title	Total	Microsoft 365 Exchange	Microsoft 365 OneDrive
Protected shared mailboxes	-	G@	-
Protected grouped accounts	-	-	J@

Status outputs are displayed as one of the following numeric values:

Value	Meaning
[1]	InProcess
[2]	Failed
[3]	Aborted
[5]	Completed
[6]	Interrupted
[7]	NotStarted
[8]	CompletedWithErrors
[9]	InProgressWithFaults
[10]	OverQuota
[11]	NoSelection
[12]	Restarted

Restore statistics by the data source

Column title	System State	Files and Folders	Bare Metal Recovery data	Virtual Disaster Recovery data	MySQL
Status (restore)	RS0	RF0	RB0	RV0	RL0
Number of files in selection (restore)	RS1	RF1	RB1	RV1	RL1
Number of changed files (restore)	RS2	RF2	RB2	RV2	RL2
Selected size (restore)	RS3	RF3	RB3	RV3	RL3
Processed size (restore)	RS4	RF4	RB4	RV4	RL4
Sent size (restore)	RS5	RF5	RB5	RV5	RL5

Column title	System State	Files and Folders	Bare Metal Recovery data	Virtual Disaster Recovery data	MySQL
Number of errors (restore)	RS7	RF7	RB7	RV7	RL7
Session duration (restore)	RSA	RFA	RBA	RVA	RLA
Last successful session (restore)	RSL	RFL	RBL	RVL	RLL
Status of the last successful session (restore)	RSQ	RFQ	RBQ	RVQ	RLQ
Status of the last completed session (restore)	RSJ	RFJ	-	RVJ	RLJ
Timestamp of the last completed session (restore)	RSO	RFO	RBO	RVO	RLO
Color bar - last 28 days (restore)	RSB	RFB	RBB	RVB	RLB
Session verification details (restore)	RSK	RFK	RBK	RVK	RLK

Restore statistics by the data source (continued)

Column title	Total	Microsoft 365 Exchange	Microsoft 365 OneDrive	Network Shares	VSS MSSQL	Exchange stores	SharePoint data	Oracle	VMware virtual machines	Hyper-V data
Status (restore)	RT0	RG0	RJ0	RN0	RZ0	RX0	RP0	RY0	RW0	RH0
Number of files in selection (restore)	RT1	RG1	RJ1	RN1	RZ1	RX1	RP1	RY1	RW1	RH1
Number of changed files (restore)	RT2	RG2	RJ2	RN2	RZ2	RX2	RP2	RY2	RW2	RH2
Selected size	RT3	RG3	RJ3	RN3	RZ3	RX3	RP3	RY3	RW3	RH3

Column title	Total	Microsoft 365 Exchange	Microsoft 365 OneDrive	Network Shares	VSS MSSQL	Exchange stores	SharePoint data	Oracle	VMware virtual machines	Hyper-V data
(restore)										
Processed size (restore)	RT4	RG4	RJ4	RN4	RZ4	RX4	RP4	RY4	RW4	RH4
Sent size (restore)	RT5	RG5	RJ5	RN5	RZ5	RX5	RP5	RY5	RW5	RH5
Number of errors (restore)	RT7	RG7	RJ7	RN7	RZ7	RX7	RP7	RY7	RW7	RH7
Session duration (restore)	-	RGA	RJA	RNA	RZA	RXA	RPA	RYA	RWA	RHA
Last successful session (restore)	RTL	RGL	RJL	RNL	RZL	RXL	RPL	RYL	RWL	RHL
Status of the last successful session (restore)	RTQ	RGQ	RJQ	RNQ	RZQ	RXQ	RPQ	RYQ	RWQ	RHQ
Status of the last completed session (restore)	RTJ	RGJ	RJJ	RNJ	RZJ	RXJ	RPJ	RYJ	RWJ	RHJ
Timestamp of the last completed	RTO	RGO	RJO	RNO	RZO	RXO	RPO	RYO	RWO	RHO

Column title	Total	Microsoft 365 Exchange	Microsoft 365 OneDrive	Network Shares	VSS MSSQL	Exchange stores	SharePoint data	Oracle	VMware virtual machines	Hyper-V data
session (restore)										
Color bar - last 28 days (restore)	RTB	RGB	RJB	RNB	RZB	RXB	RPB	RYB	RWB	RHB
Session verification details (restore)	RTK	RGK	RJK	RNK	RZK	RXK	RPK	RYK	RWK	RHK
Microsoft 365 protected user accounts (restore)	RTM	-	-	-	-	-	-	-	-	-
Microsoft 365 protected shared accounts (restore)	RT@	-	-	-	-	-	-	-	-	-
Protected regular mailboxes (restore)	-	RGM	-	-	-	-	-	-	-	-
Protected shared mailboxes (restore)	-	RG@	-	-	-	-	-	-	-	-

Column title	Total	Microsoft 365 Exchange	Microsoft 365 OneDrive	Network Shares	VSS MSSQL	Exchange stores	SharePoint data	Oracle	VMware virtual machines	Hyper-V data
Protected user accounts (restore)	-	-	RJM	-	-	-	-	-	-	-
Protected grouped accounts (restore)	-	-	RJ@	-	-	-	-	-	-	-

Expressions for active data sources

Full Name	Shortname
Files and Folders	F
System State	S
MsSql	Q
MsExchange	X
NetworkShares	N
VMware	W
Total	T
MsSql (VSS)	Z
MsSharePoint (VSS)	P
Oracle	Y
MsHyperV (VSS)	H
MySql	L
Removable Media	R

For example, if you want to find the devices that back up "Files and Folders" and "System State" only, the advanced filter expression will look as follows:

```
AP=~"*F*" && AP=~"*S*"
```

Syntax for advanced filter in Management Console

> Please note, we have new filter expressions which should be used as soon as you are able. These can be found here.

Advanced filter syntax consists of numbers, identifiers and function calls, joined with comparison operators. The list of supported operands is below.

Operand	Description
`true`, `false`	Boolean
`"foo"`, `'bar'`	String
`123`, `234`	Integer number
`123.456`, `0.5`	Floating-point (real) number
`foo`, `bar.baz`	Identifier
`foo()`, `bar.foo()`	Function call

Identifiers and function calls are evaluated to booleans, strings and numbers during expression evaluation, thus they could appear anywhere those simple types are allowed.

Operators have precedence above each other, meaning some of them will be evaluated before others. Here is the list of operators in the descending order.

Operators	Description	Example
`.`	Dot operator, used to access object properties and methods	`foo.bar`, `bar.foo()`
`+ -`	Unary operation plus and minus operators	`+foo`, `-bar`
`* / %`	Multiplication, division and modulus operations	`foo * bar`
`+ -`	Addition and subtraction operators	`foo - bar`
`== != < > <= >=`	Equal, not equal, less, greater, less or equal, greater or equal operators	`foo != bar`
`<>`	Alias for `!=`	
`=~`	Match operator; right-hand operand is a string containing wildcard expression to match left-hand operand	`foo =~ "bar*"`
`in`	Set inclusion operator	`foo in (bar1, bar2)`

Operators	Description	Example
`! not`	Logical negation operator	`!foo , not foo =~ "bar*"`
`&& and`	Logical conjunction operator	`foo1 == bar1 && foo2 != bar2`
`|| or`	Logical disjunction operator	`foo1 == bar1 || foo2 != bar2`

Boolean expressions

Any complete expression used as display style match expression and any part of this expression used as operand with comparison, match and logical operators has to evaluate to boolean. It is also possible to use expressions evaluating string and numeric values, in which case they will be cast to boolean by the following rules:

Operand type	Description
Boolean	As is
String	True if not empty, false otherwise
Integer/Real Number	True if not zero, false otherwise

Management extensions

There are some useful extensions present to ease expressions writing.

Time duration extensions

All time-related operations are performed in seconds. Though you may simply write `5 * 60` to express 5 minutes, it is more readable and convenient to use one of the following helper functions:

Function	Description
`day(),days()`	Aliases, return X days as a number of seconds
`hour(),hours()`	Aliases, return X hours as a number of seconds
`minute(),minutes()`	Aliases, return X minutes as a number of seconds
`month(),months()`	Aliases, return X months as a number of seconds (approximating to 30 days in one month)
`second(),seconds()`	Aliases, return X itself
`week(),weeks()`	Aliases, return X weeks as a number of seconds
`year(),years()`	Aliases, return X years as a number of seconds (approximating to 365.25 days in one year)

For an example, see the "Duration Object" section.

Size extensions

All size-related operations are performed in bytes. You may as well write `15 * 1000 * 1000 * 1000` to express 15 gigabytes, but it is easier to use one of the following helpers:

Function	Description
`kilo(),kibi()`	Return X kilo- (×1000) or kibibytes (×1024) as a number of bytes
`mega(),mebi()`	Return X mega- ($\times 1000^2$) or mebibytes ($\times 1024^2$) as a number of bytes
`giga(),gibi()`	Return X giga- ($\times 1000^3$) or gibibytes ($\times 1024^3$) as a number of bytes
`tera(),tebi()`	Return X tera- ($\times 1000^4$) or tebibytes ($\times 1024^4$) as a number of bytes
`peta(),pebi()`	Return X peta- ($\times 1000^5$) or pebibytes ($\times 1024^5$) as a number of bytes
`exa(),exbi()`	Return X exa- ($\times 1000^6$) or exbibytes ($\times 1024^6$) as a number of bytes
`zetta(),zebi()`	Return X zetta- ($\times 1000^7$) or zebibytes ($\times 1024^7$) as a number of bytes
`yotta(),yobi()`	Return X yotta- ($\times 1000^8$) or yobibytes ($\times 1024^8$) as a number of bytes

For example, you could write `us > 10.giga() && us < 20.tera()` to select devices with used storage size between 10 gigabytes and 20 terabytes.

If you feel uncomfortable with those units differences, please refer to Wikipedia article on binary prefixes.

Duration Object

When there is a need in comparing time column values against some time relative to another, these helper functions may come in handy:

Function	Description
`until(T)`	Return Time object corresponding to X seconds before T
`ago()`	Alias to `X.until(Time.now())`
`since(T)`	Return Time object corresponding to X seconds after T
`from_now()`	Alias to `X.since(Time.now())`

For example, you can write `ts < 20.minutes().ago()` to select devices which have been inactive for the last 20 minutes.

Time Class

Function	Description
`now()`	Return Time object corresponding to current time

For example, you could write `ts > Time.now()` to select devices with incorrect time settings (naturally, no device could report its last activity time which is later than the current time).

Session Class

Number	Property	Description
1	In progress	The session is still running.
2	Failed	The session failed.
3	Aborted	The session was aborted.
5	Completed	The session was successful.
6	Interrupted	The session was interrupted because of a BackupFP crash during the system's scanning at the beginning of the session
7	Not Started	The device has no sessions at all
8	Completed With Errors	The last session was completed with errors
9	In Progress With Faults	A corresponding session status
10	Over Quota	The selection exceeds the limits

For example, you can write `t0 in (Session.Completed, Session.CompletedWithErrors)` to select devices having the "Completed" or "Completed with errors" total session status.

Device management in Management Console

The **Backup > Dashboard** lists all devices together with usage statistics for them.

Device definition

A device (aka "backup device") is client software installed on a computer to provide backup and recovery services. This applies to the data actually located on the current computer as well as remote resources accessible through this computer (network shares, virtual machines, databases and others).

> A device can be installed on **several computers**: the primary computer where data backup takes place and any number of other computers in the restore-only mode.

Access permissions

All types of users can **view** the module. **Editing** permissions are available to the following types of users:

- SuperUser
- Manager (all features except for the automatic device deployment)

> The automatic device deployment feature is available only to the SuperUser accounts belonging to the customers of a certain type (reseller or end-user).

You can find a list of user types here.

Adding devices

To enable backups, you need a device. Backup Manager device types differ depending on the intended installation method.

- **Quick Installation** - This method uses the Automatic Deployment feature to allow system administrators to quickly install the Backup Manager on multiple machines using a software distribution system. This installation method becomes available if a certain type of customer is selected (reseller or end-customer) and works for servers and workstations.
- **Legacy installation** - (Previously known as Manual Installation) Choose this method to install devices **one at a time**. You can perform the installation through a set-up wizard or through the command line in silent mode. This method of installation works for servers and workstations.

  > This option can be found by selecting the Alternative Installers toggle at the top right of the window

- **Documents** - This is a purpose-built data protection solution for **Windows and macOS workstations and laptops** only. It provides highly automated data protection of key office files (every Word doc, spreadsheet, presentation, text

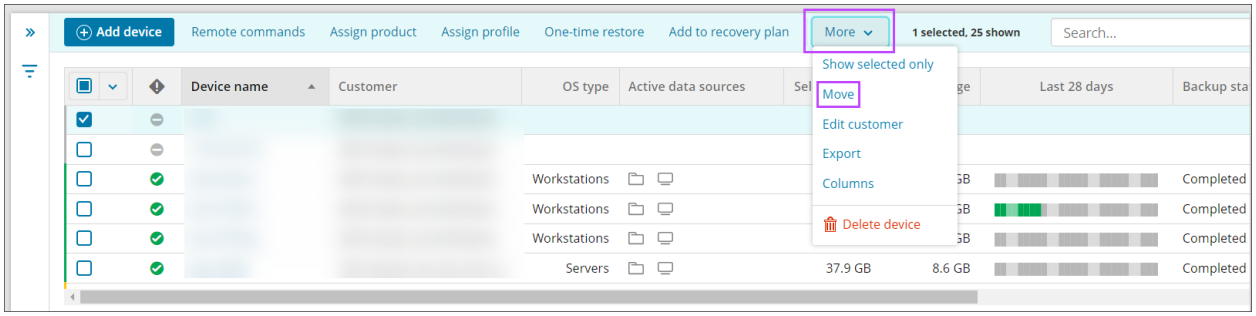
  > This option can be found by selecting the Alternative Installers toggle at the top right of the window

- **Microsoft 365** - This service enables the protection of Microsoft 365 domains for full Exchange, OneDrive and SharePoint protection. This option lets you recover email messages, calendar items, files and contacts from Exchange, OneDrive and SharePoint data from protected accounts long after they were cleaned or lost from Microsoft databases.

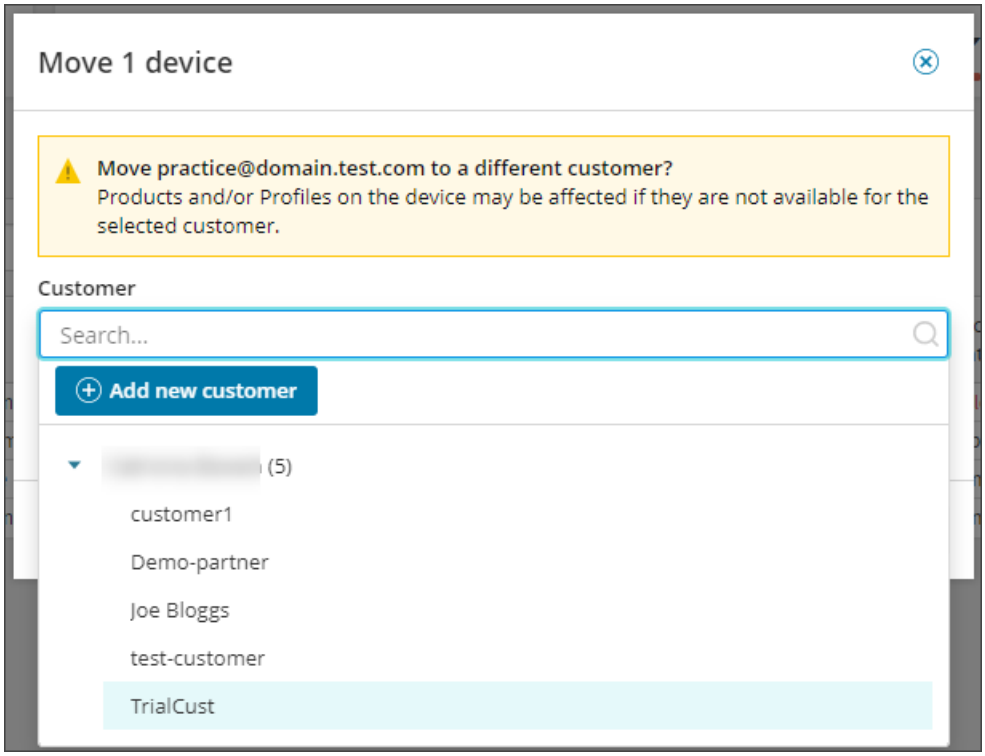
Moving Devices

You can move devices from one customer to another using the **Move** function on the Management Console.

1. In **Backup > Dashboard**, select the device(s) to move
2. Click **More > Move** on the toolbar



3. In the **Assign Backup Product** window, select the new partner to assign from the dropdown

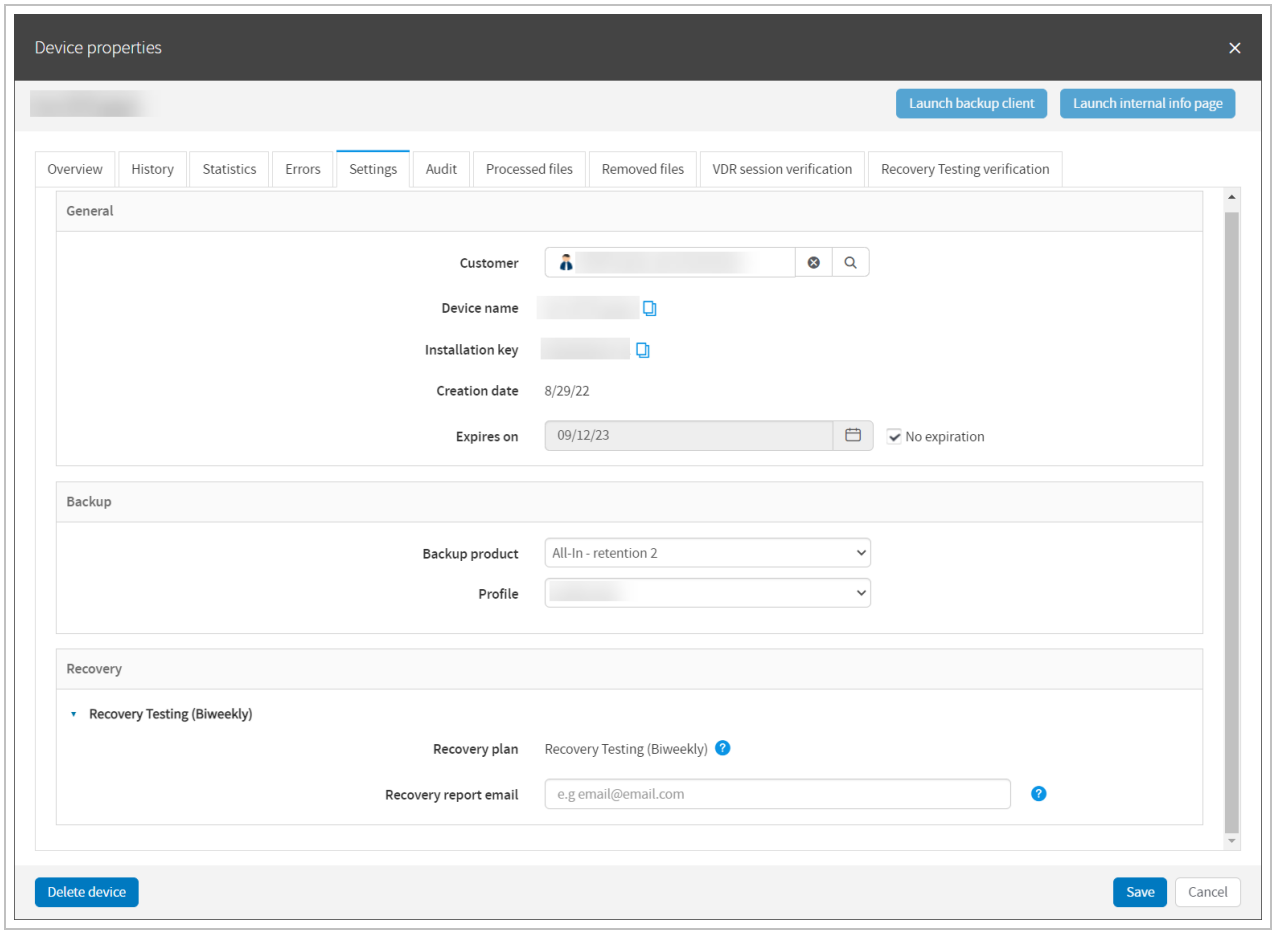


4. Click **Save**

> If Products or Profiles are assigned to the device that is not available for the selected customer, these will be removed upon save. You will need to create them at the appropriate customer level and re-assign to the device.

Editing devices

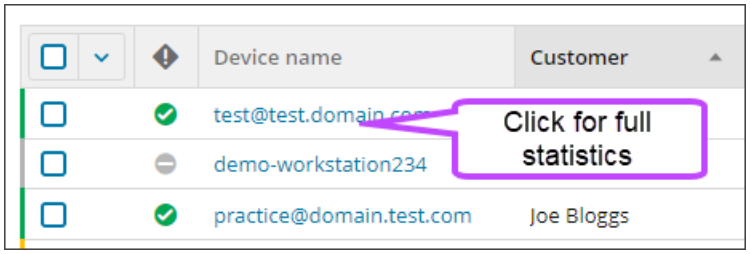
1. To edit an existing device, click the device name to view the device properties
2. Navigate to the **Settings** tab. The following options are available to edit:
   - Assign the device to another customer
   - Change the **product** assigned to the device
   - Change the **profile** assigned to the device
   - If compatible, assign the device to a **Recovery Testing plan**
     - Add or edit the Recovery report email address
   - Change the **Expiry date**, or set the device to **No exiration**
3. Save any changes made



You cannot edit device names and passwords.

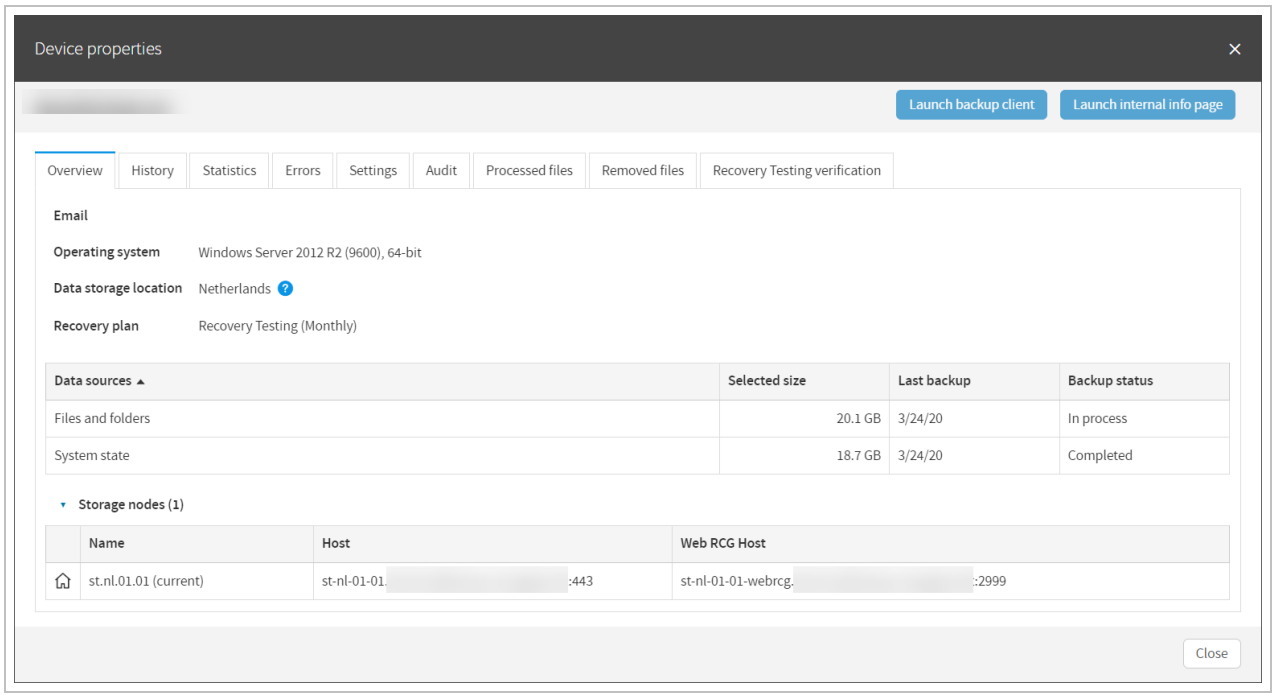
Viewing statistics for devices

The most important device statistics appear right in the **Devices** widget. To get all details for a device, click on its name.



The **Device Properties** dialogue will open. Use the tab bar to switch between different views.

Regular Backup

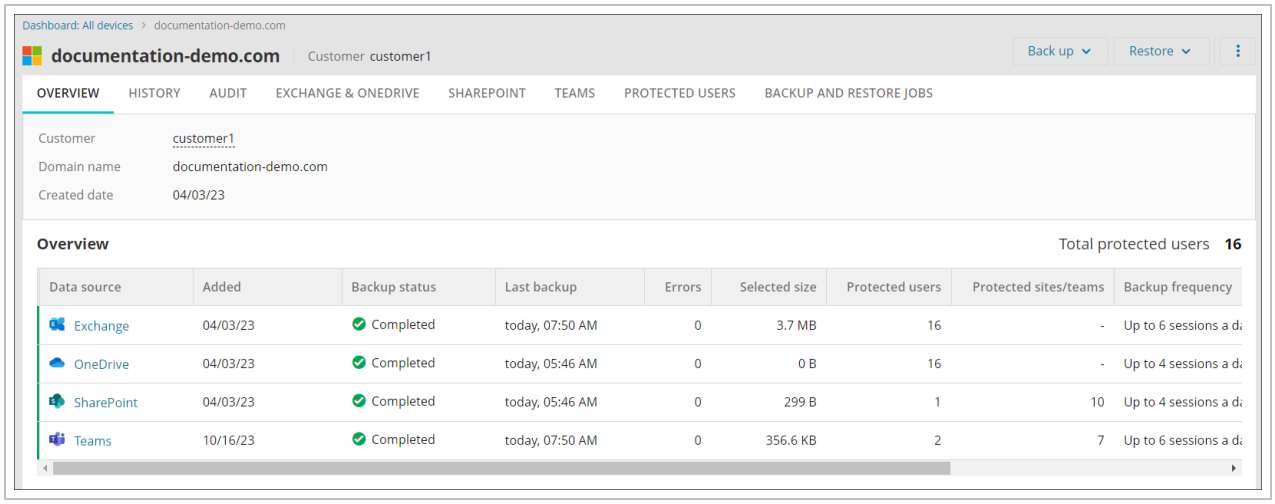


Each tab within the **Device Properties** dialogue contains different information. The tab selection you see may differ depending on the user account type or the device type.

Tab	Description
Overview	A general overview of the device, including: ▪ Operating system ▪ Data storage location ▪ Recovery plan assigned (if one is assigned) ▪ Data sources with their selected size, last backup date and the status of the most recent backup ▪ Storage Node informmation
History	Recent backup session history showing the time the jobs started for the device, the duration, data source that was ran, action taken, backup status, number of errors, the selected size of the job, number of files scanned for the job, the processed size of the job, number of files backed up or recovered, the transferred size of all files once compressed, number of files removed after clean and any flags against the session - all of which can be filtered on
Statistics	Information about Backup Manager on the device, including but not limited to the version of the client installed, amount of storage spaces used, make and model of the device and LocalSpeedVault settings.
Errors	Any errors that have occurred during the backup, gives you a breakdown of what has happened and when.
Settings	Broken into several sections, this tab contains:

Tab	Description
	▪ **General** - This section provides the main device details: ▪ **customer** - Who device belongs to, can be changed to move the device to a different customer ▪ **Device name** - Cannot be changed ▪ **Installation key** - (Password) Cannot be changed ▪ **Creation date** - Cannot be changed ▪ **Expires on** - Can be amended to a date in the future, or set to **'no expiration'** if required ℹ You may also see the Request Passphrase button here if the device is set up to use this instead of its own security code/encryption key ▪ **Backup** ▪ **Backup product** - Use the dropdown to change the Product used by the device ▪ **Profile** - Use the dropdown to change the Profile applied to the device
Audit	This tab shows you what operation was carried out against the device, when, by which user account and any additional details to the action.
Processed Files	In here you will see a breakdown of each file that was processed during the backup, how long scanning and backup took and the size of the file before and after compression
Removed Files	This tab details the file name and path of each instance of the filed that are no longer within the retention period and so have been cleaned from the storage account.
Recovery Testing Verification	This tab will only be available if the device is assigned to a Recovery Testing plan, e.g. Recovery Testing (Monthly) or Recovery Testing (Bi-weekly). In this tab, you can view the screenshot, the recovery session status, time and duration as well as the System Log information.

Microsoft 365 Backup



At the top right of the **Device Properties** view, you will find an Action Menu, allowing you to action backup or restores for the configured data sources.

Tab	Description
Overview	A general overview of the device, including the services enabled for backup and the status of the most recent backup.
History	Recent backup session history showing the time the jobs started for the device, the duration, service that was ran, action taken, status, number of errors and the number of accounts processed in the job.
Audit	This tab shows you what operation was carried out against the device, when, by which user account and any additional details to the action.
Exchange & OneDrive	In here you will see a breakdown of the Exchange and OneDrive backup selection and have the ability to add or remove backup for accounts. You will only see this tab if Exchange or OneDrive are enabled as services.
SharePoint	In here you will see a breakdown of the SharePoint backup selection and have the ability to add or remove backup for sites. You will only see this tab if SharePoint is enabled as a service.
Teams	In here you will see a breakdown of the Teams backup selection and have the ability to add or remove backup for Teams and Teams data. You will only see this content if Teams is enabled as a service, if not, you will be prompted to add Teams backup.
Protected Users	The Protected Users tab provides a list of all backed up Exchange and OneDrive users and SharePoint sites. You can filter in here by **User Type** and **Service**.
Backup And Restore Jobs	This tab details any backup or restore jobs that are currently in progress. It will provide information on the time the job was started, the service, whether it is a backup or restore, the jobs status, the number of protected users or sites being backed up or restored, any errors encountered and a progress bar. You may cancel a restore job that is in progress, but backup jobs cannot be canceled.

To get detailed statistics on the software/hardware environment the device is installed on, choose the **Launch internal info page** option.

Session Flags

You can find flags within the **History** tab of the **Device Properties** dialogue box.

Flag Letter	Flag Name	Description
A	Archived	The backup session has been archived
C	Cleaned	The backup session has been cleaned as it is outside of the retention period
L	LocalStorage	The backup session has not yet synchronized to the cloud storage

Deleting device(s)

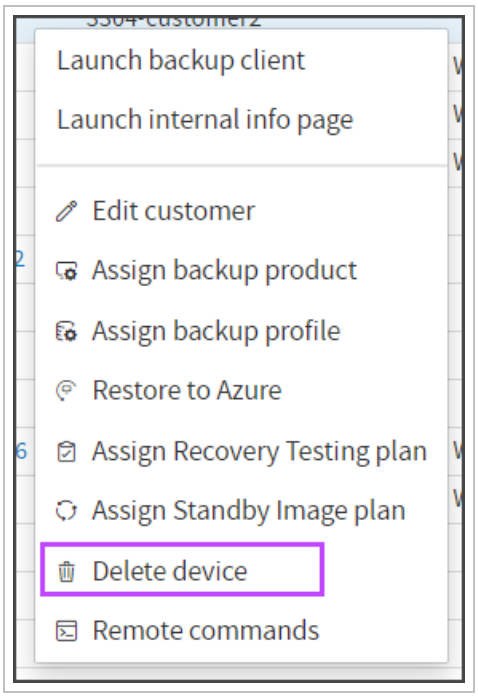
Devices are removed together with **all data** that has been backed up for them.

The previously backed up data is **permanently deleted 28** days after the device is deleted.

There is **no way** to restore the data after the device has been deleted from the system.

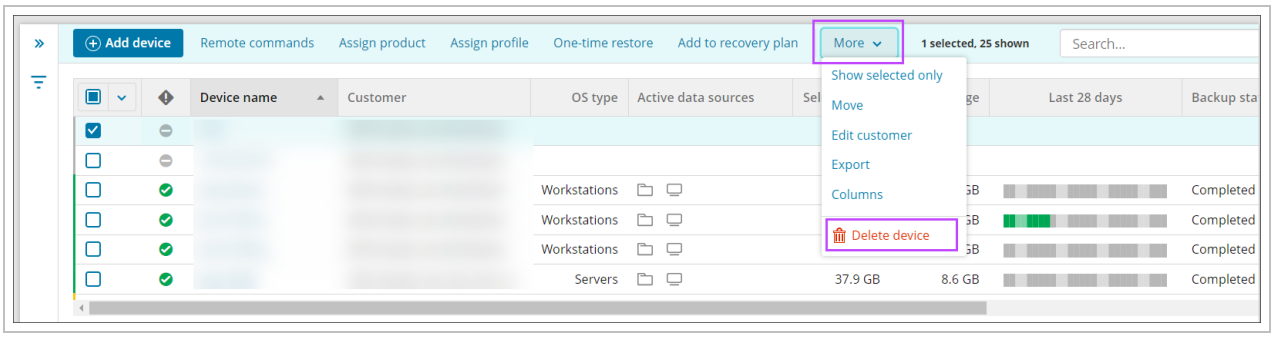
To delete one or multiple devices:

1. Select the three vertical dots to the right of the device and click **Delete device** on the action menu

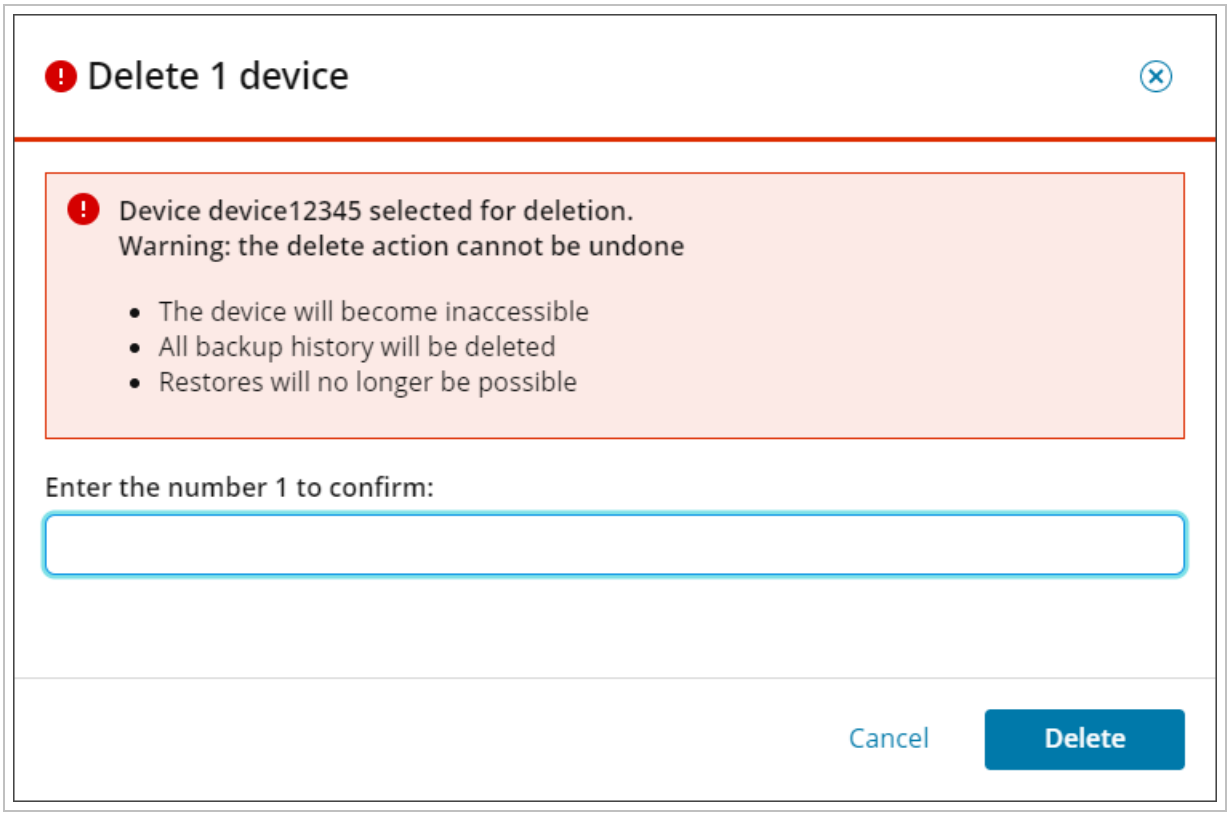


Or

2. Select the checkbox next to each of the devices, select **More** from the toolbar then **Delete Device**



3. Confirm the number of devices to be deleted by typing the number in the text box



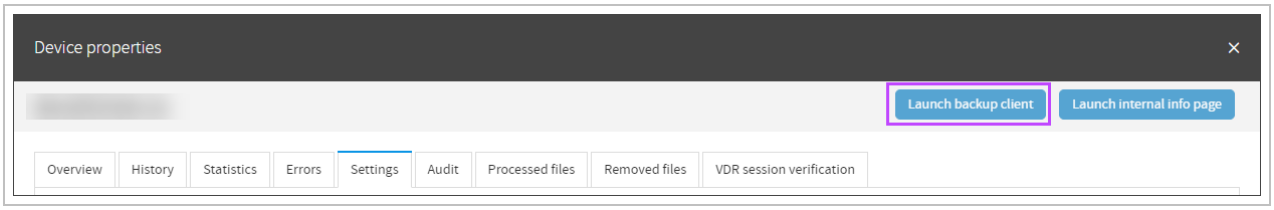
4. Click **Delete**

> It is also possible to delete devices individually from the **Device Properties** > **Settings** tab.

Launching devices Backup Client remotely

Any of the devices' Backup Manager's can be opened in a browser (no installation necessary). This is possible at the time the device is running on a remote computer. The Backup Manager you are connecting to should allow remote connections (the **Accept remote connections** setting should be on if the Backup Manager has this setting).

1. Open a web browser and go to https://backup.management
2. Find the device on the list
3. Click the device name to open the Device Properties window
4. Select **Launch backup client**



If the connection cannot be established, you can manage the device using remote commands. See remote commands for full details.

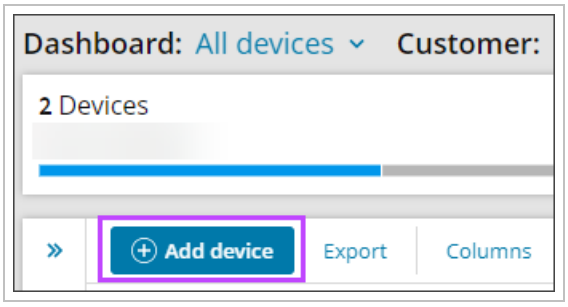
If the **Launch backup client** button is greyed out for a device, this means that the device is offline or the Backup Service is not running.

> If the device is a laptop, it must be open and logged on in order for the backup processes to run and allow remote access through the console.

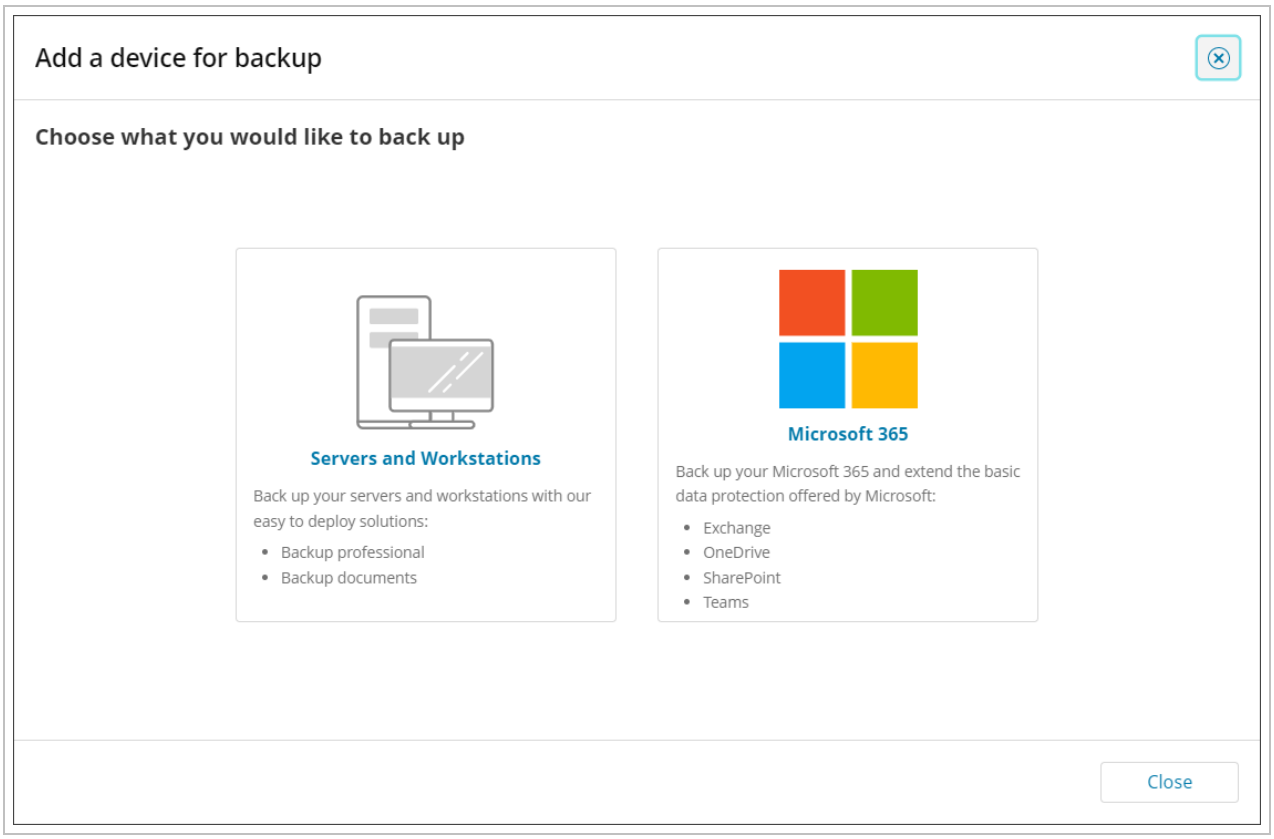
Adding Devices for Quick installation in Management Console

To add devices for Automatic Deployment (quick installation), follow the below steps:

1. Log in to the Console under a SuperUser account belonging to a reseller or end-customer



2. Click **Add devices**, select **Servers of Workstations**

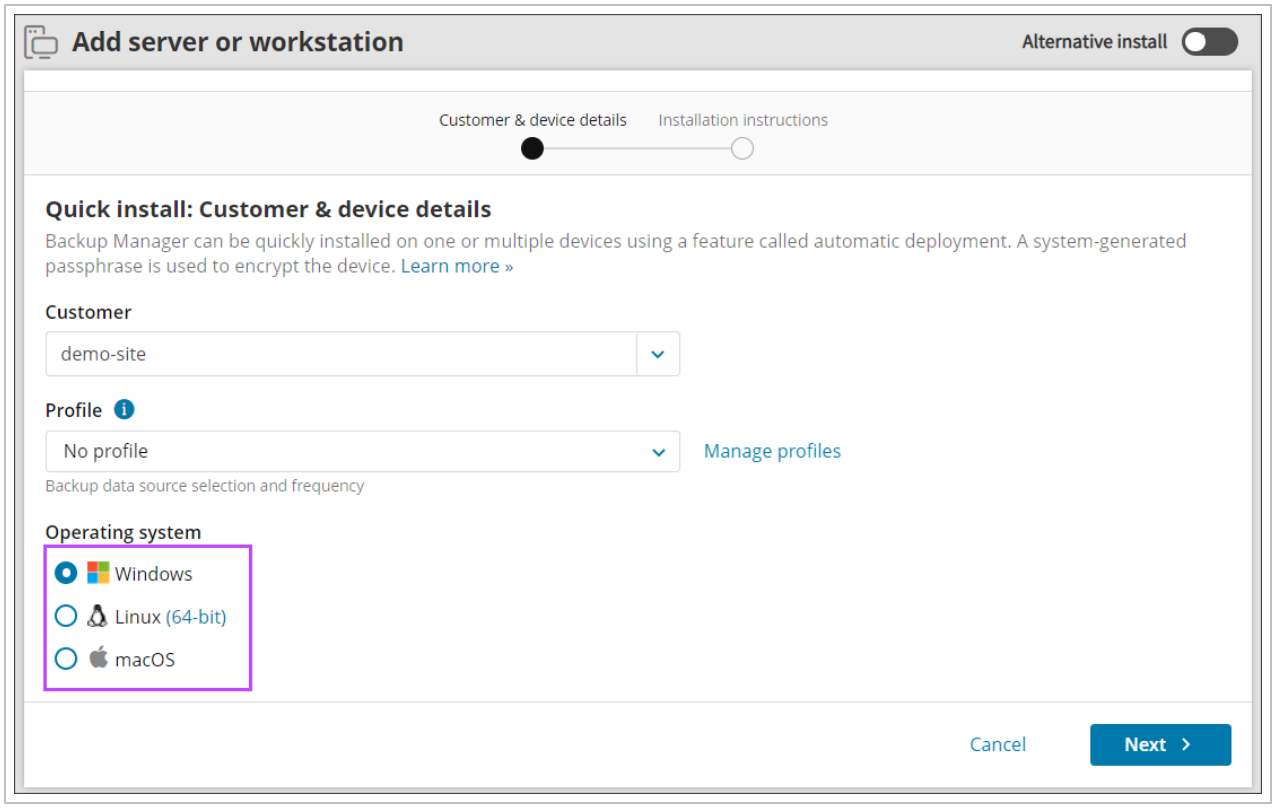


3. Select the customer to install the device for from the dropdown

4. Select a backup profile (optional)

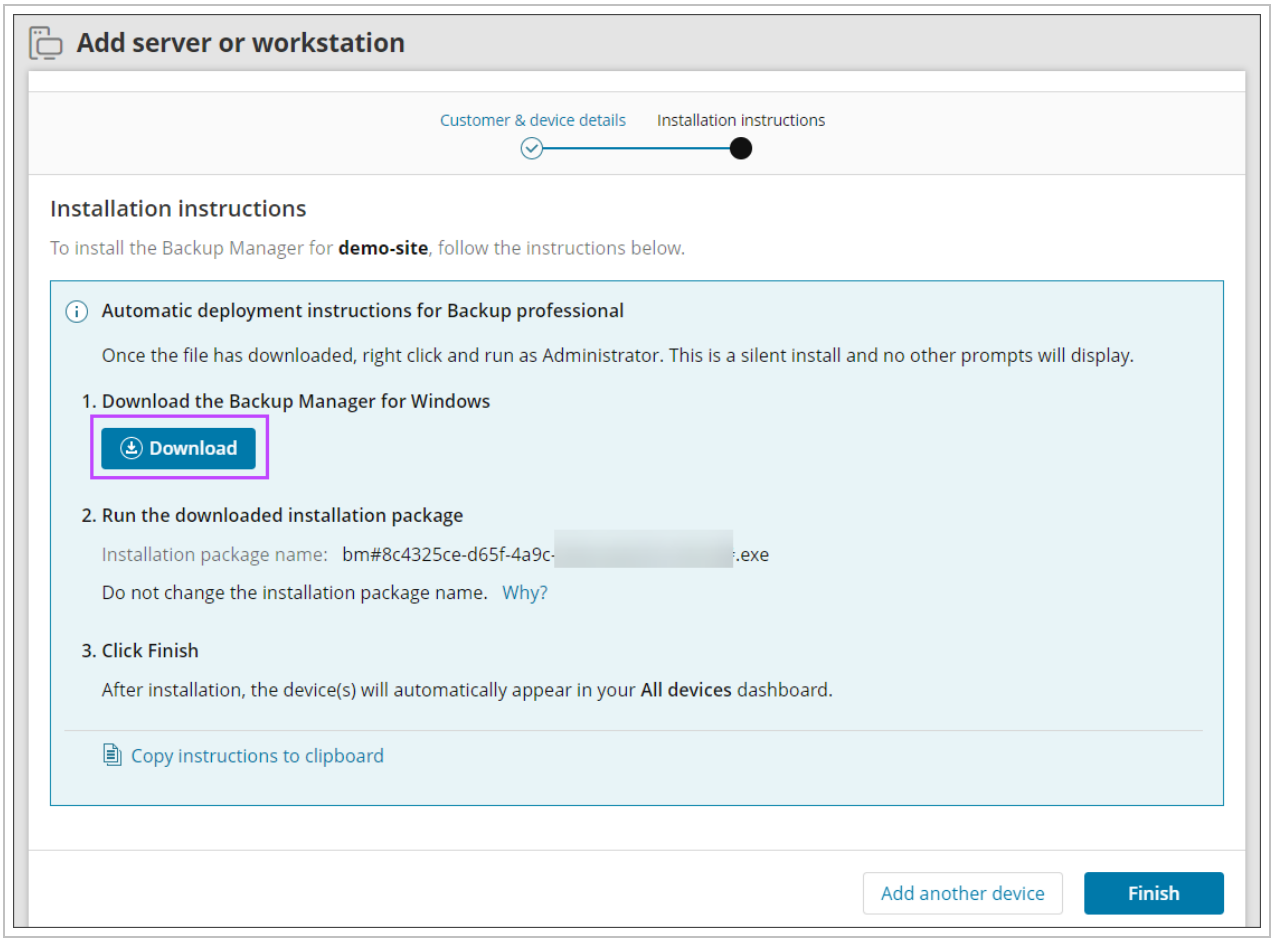
> Backup profiles let you configure multiple devices for backup simultaneously (learn more).

5. Select the operating system for the device



6. Click **Next**
7. Download the **installation package** from the download link and take a note of the **installation package name**

> Do **not** change the installation package name from the one provided on your dialog. This is because the package name is a unique identifier for the specific customer and doing so would stop the installation from functioning appropriately.



8. Click **Finish**
9. Run the Installation package on the device where the backup is required

> If the installer does not run after downloading, check the file has not been renamed by your system and check properties of the install file to ensure that it has not been blocked by your system upon download. Attempt to run as the Administrator on the device.

Ways to **run the installation package**:

- Double-click on the installer executable
- Submit the name of the installer to a terminal emulator or a software distribution system. For example: `demobm#a55x00rf-d604-429e-1f87-n800004e755#5038#.exe`

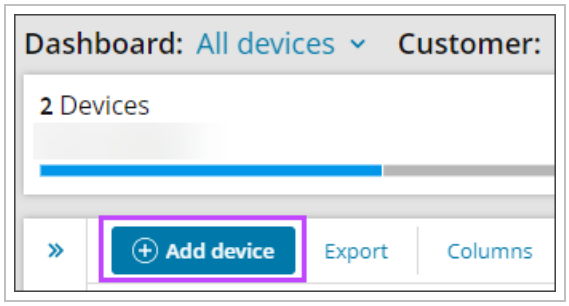
> Please note, the installer name will be specific to you.

See Quick Installation of the Backup Manager for detailed instructions.

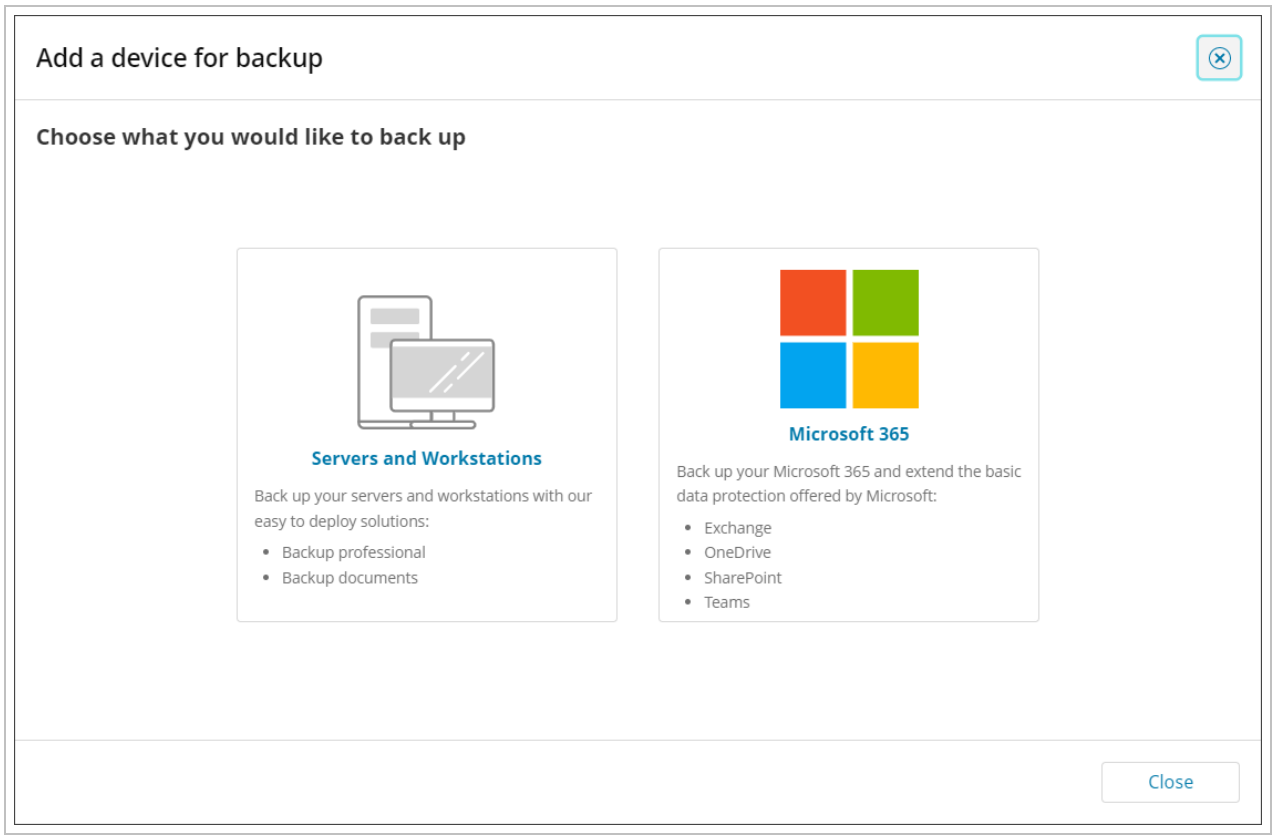
Adding Devices for Legacy Installation in Management Console

To add devices for legacy installation (manual installation), follow the steps below:

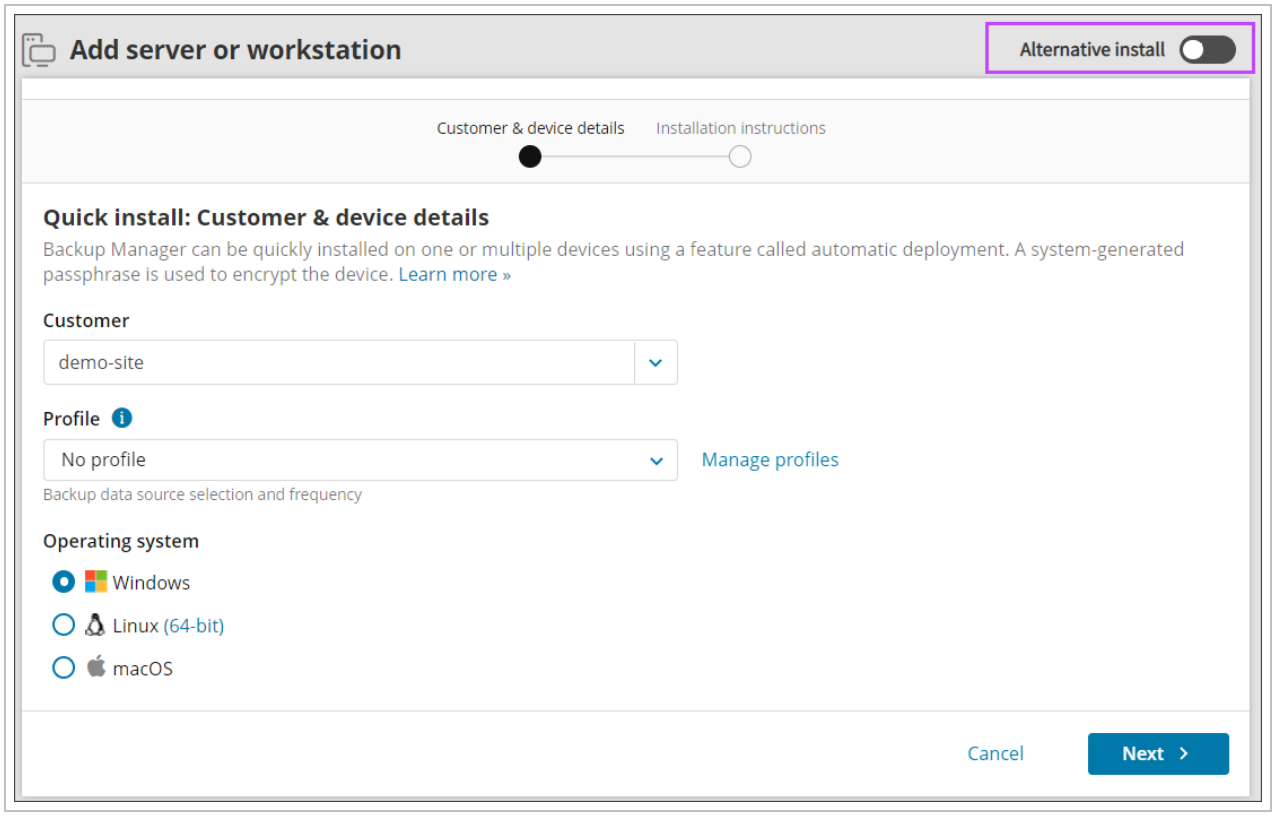
1. Log in to the Console under a SuperUser account belonging to a reseller or end-customer



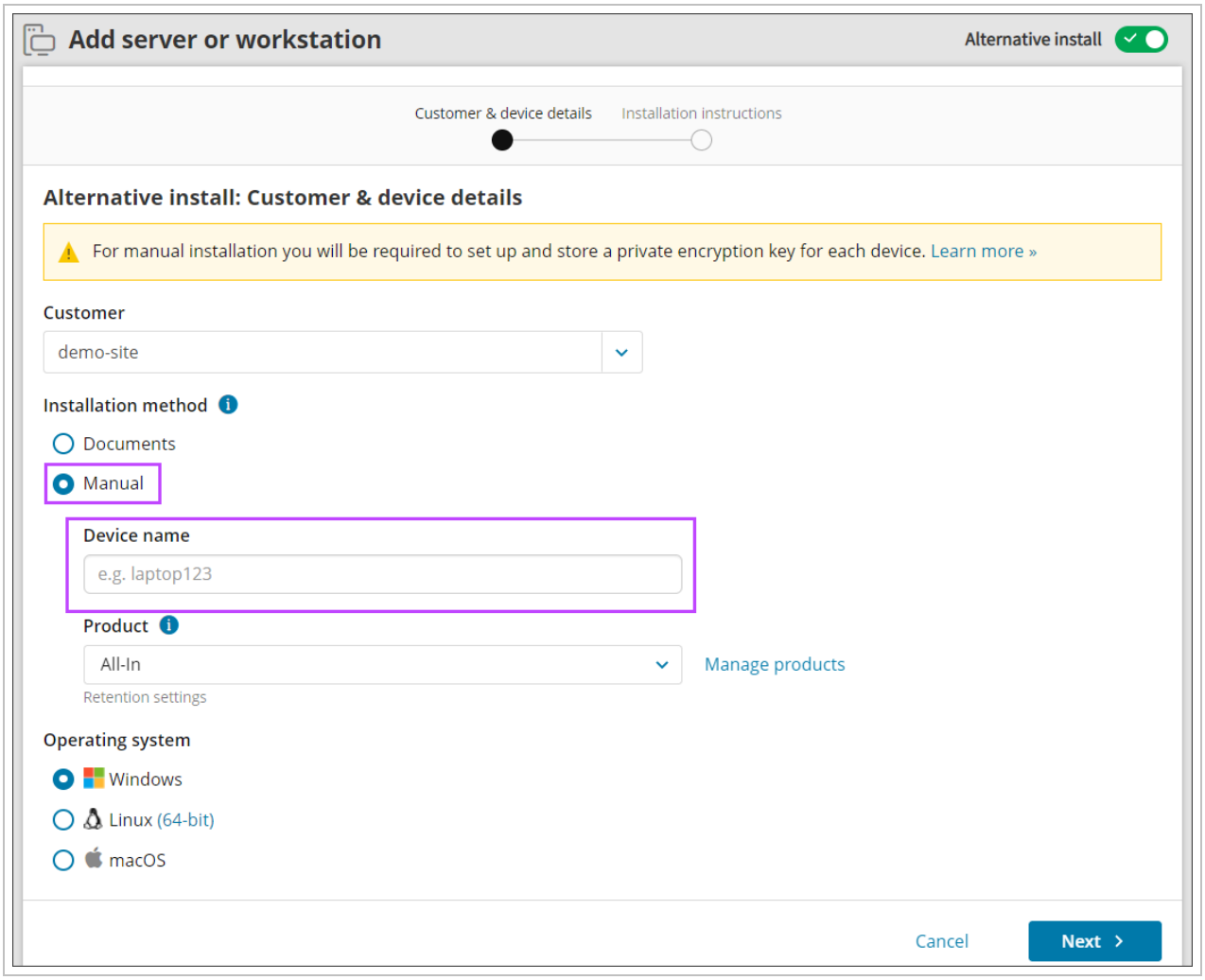
2. Click **Add devices**, select **Servers of Workstations**



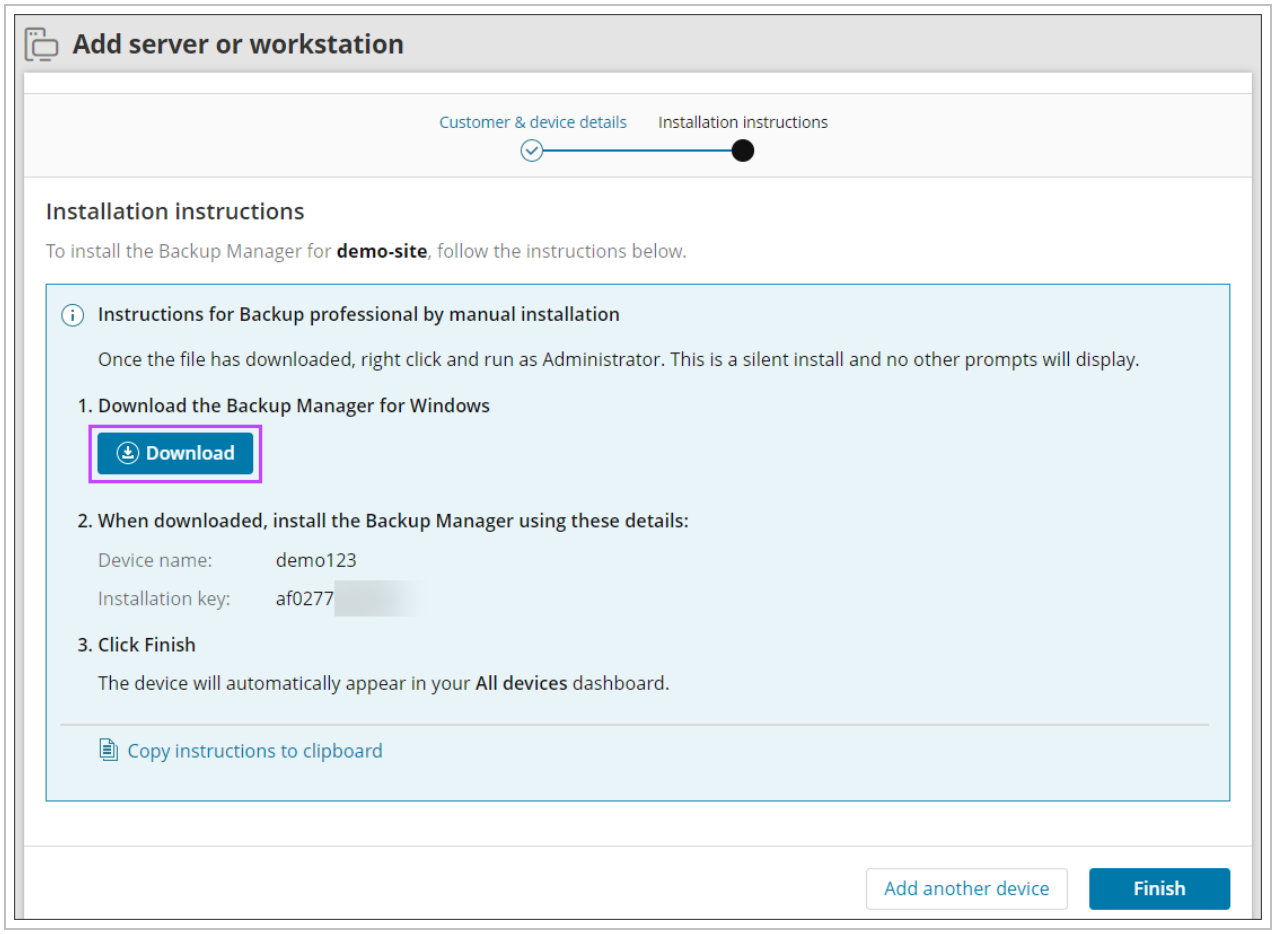
3. Using the toggle in the upper right-hand corner of the wizard, enable **Alternative install**



4. Select the **Customer** to install the device for from the dropdown
5. Choose the **Manual** Installation method



6. Give the device a memorable name
7. Select a product for the device (if applicable). The product determines the set of features and storage options allocated to the device (learn more).
8. Select the operating system
9. Click **next**
10. Download the Backup Manager installer



You will need the **Device name** and **Installation key** for installation, so it is recommended you take a copy here, though these can be found at a later date from the device properties Settings tab if this is closed before taking a note.

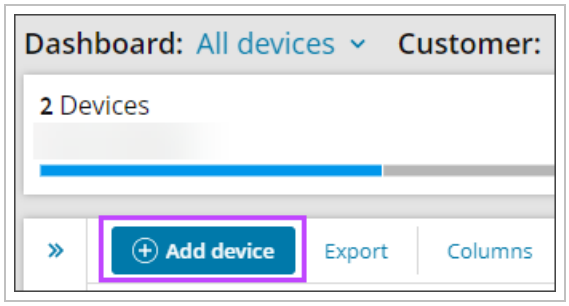
11. Run the installer and follow the instructions provided on screen

If the installer does not run after downloading and attempting to run, check the properties of the install file to ensure that it has not been blocked by your system upon download or attempt to run as the Administrator on the device.

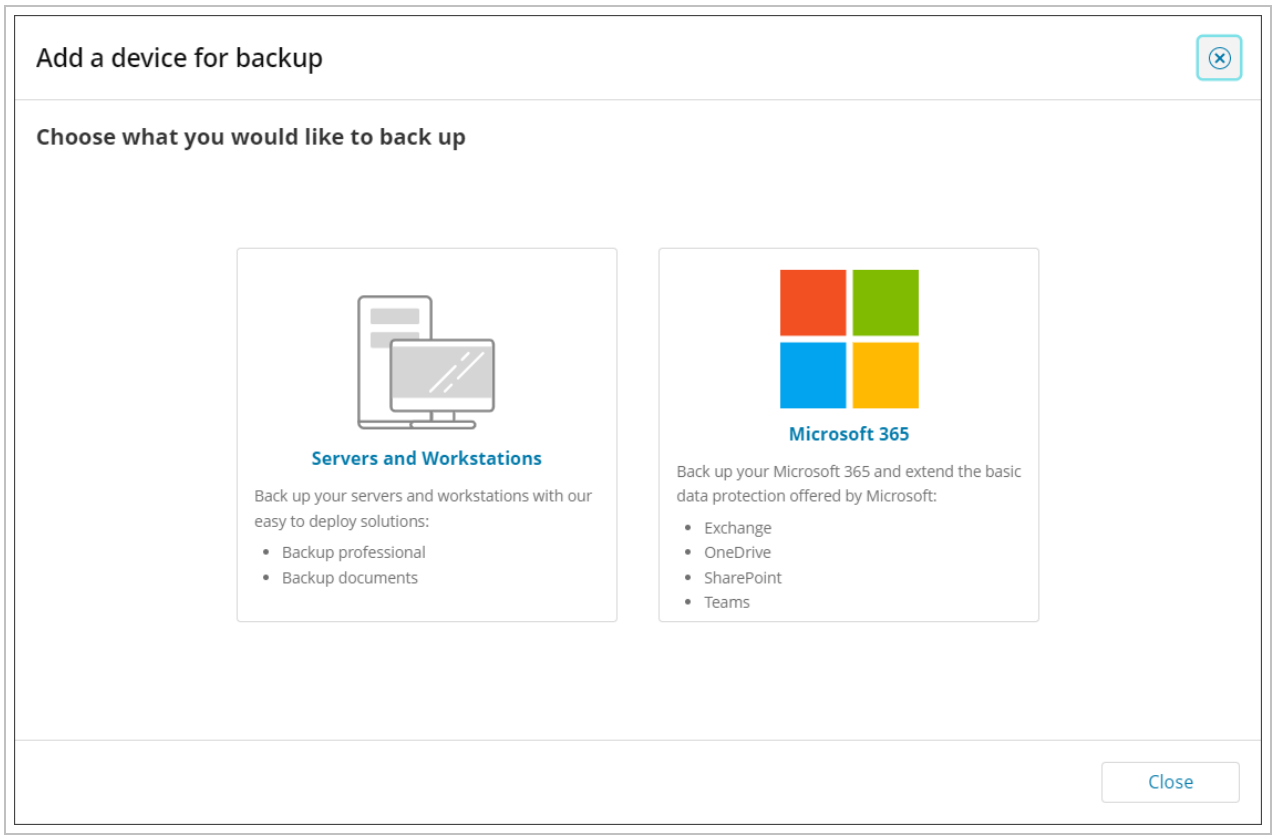
Adding Devices for Documents in Management Console

To Add devices for Documents, follow the steps below:

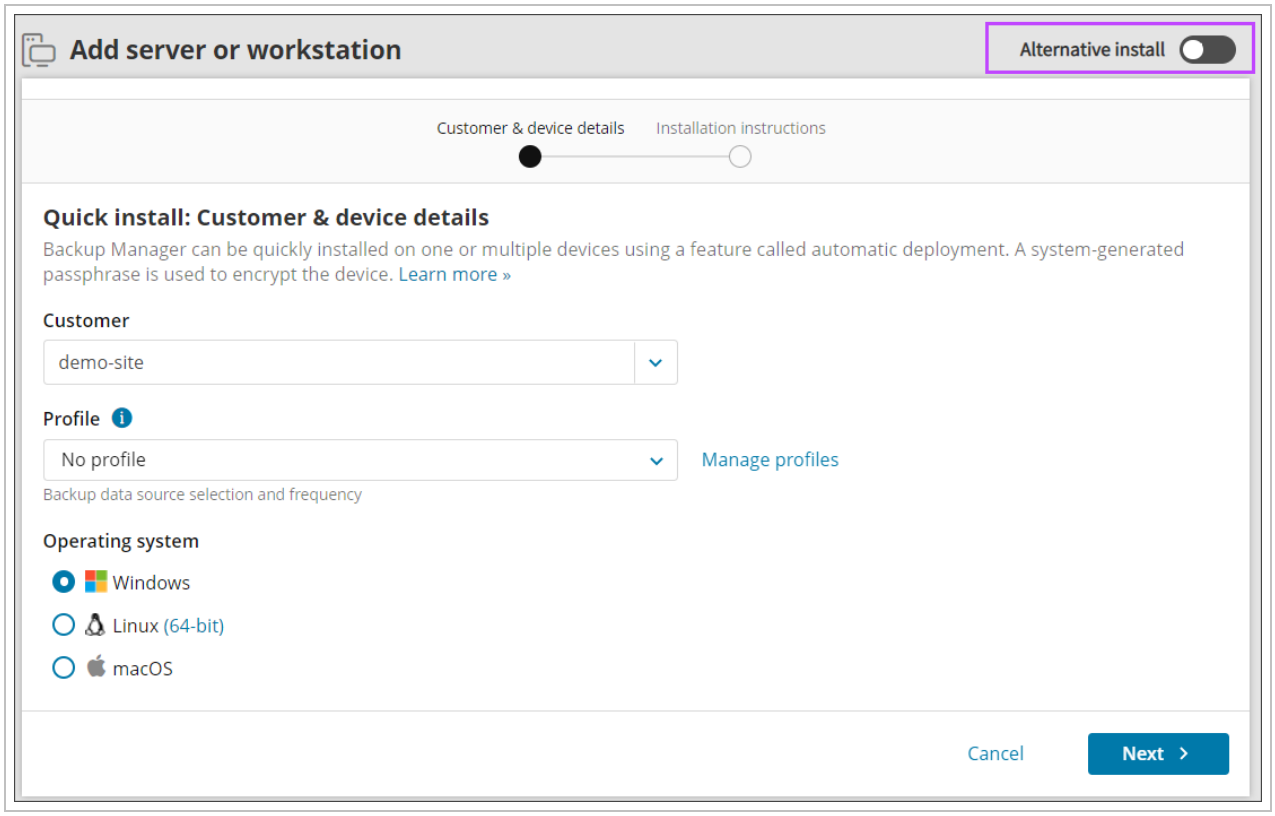
1. Log in to the Management Console under a SuperUser account belonging to a reseller or end-customer



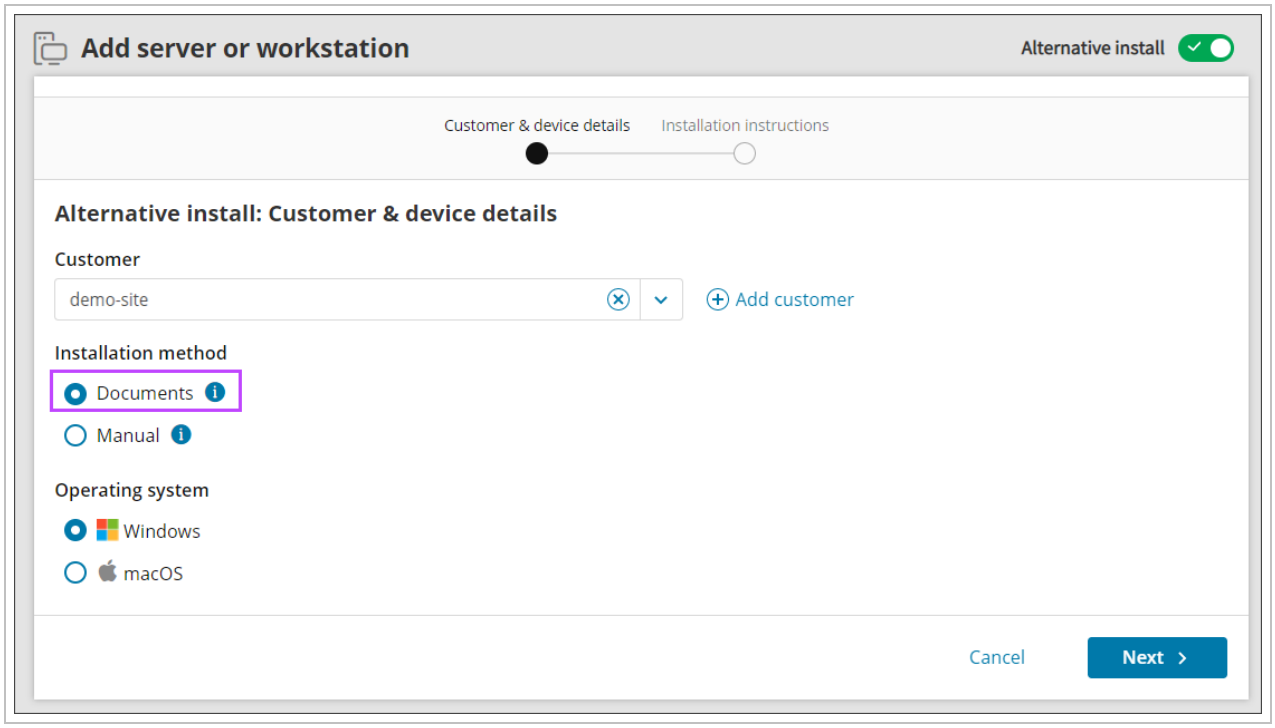
2. Click **Add device**, select **Servers of Workstations**



3. Using the toggle in the upper right-hand corner of the wizard, enable **Alternative install**

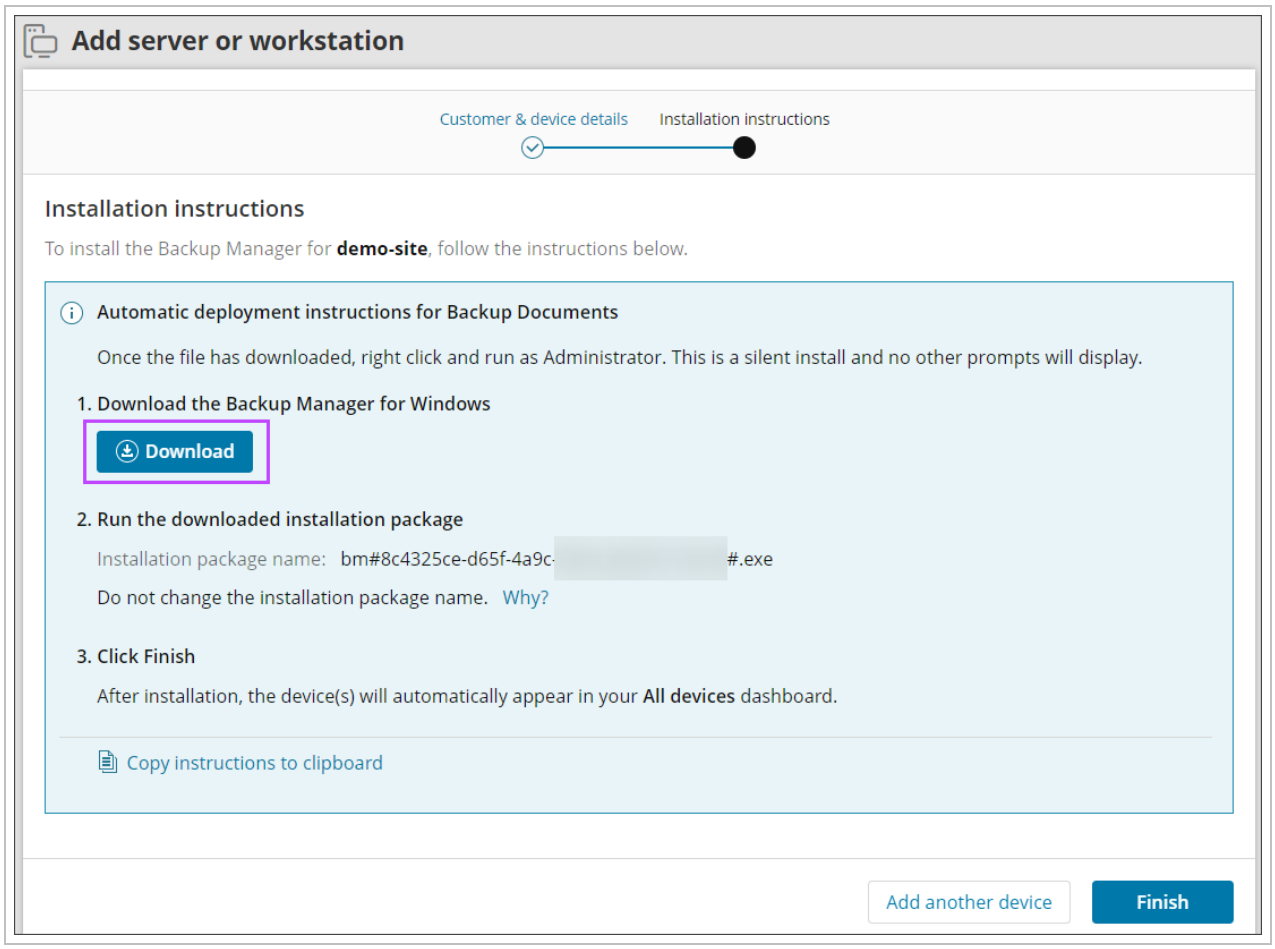


4. Select the **Customer** to install the device for from the dropdown
5. Choose the **Documents** Installation method



6. Select the Operating System for your device:
   - Windows
   - macOS
7. Click **Next**
8. Download the **installation package** from the download link and take a note of the **installation package name**

> Do **not** change the installation package name from the one provided on your dialog. This is because the package name is a unique identifier for the specific customer and doing so would stop the installation from functioning appropriately.



9. Click **Finish**
10. Run this installer on any number of machines to enable Documents

> If the installer does not run after downloading, check the file has not been renamed by your system and check properties of the install file to ensure that it has not been blocked by your system upon download. Attempt to run as the Administrator on the device.

Ways to **run the installation package**:

- Double-click on the installer executable
- Submit the name of the installer to a terminal emulator or a software distribution system. For example: `demobm#a55x00rf-d604-429e-1f87-n800004e755#5038#.exe`

> Please note, the installer name will be specific to you.

Sending remote commands to devices in Management Console

You can manage the devices belonging to your company and your customers through remote commands. Some of the typical actions that can be performed remotely are:

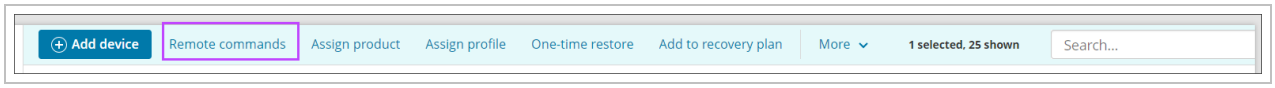
- start or cancel a backup
- edit a backup schedule
- update the backup software

> Be aware, if a remote command is sent to a device when it is offline, the remote command will *not* be processed until the device comes back online. This is because remote commands are sent via the cloud to the storage node and then on from the storage node to the device.

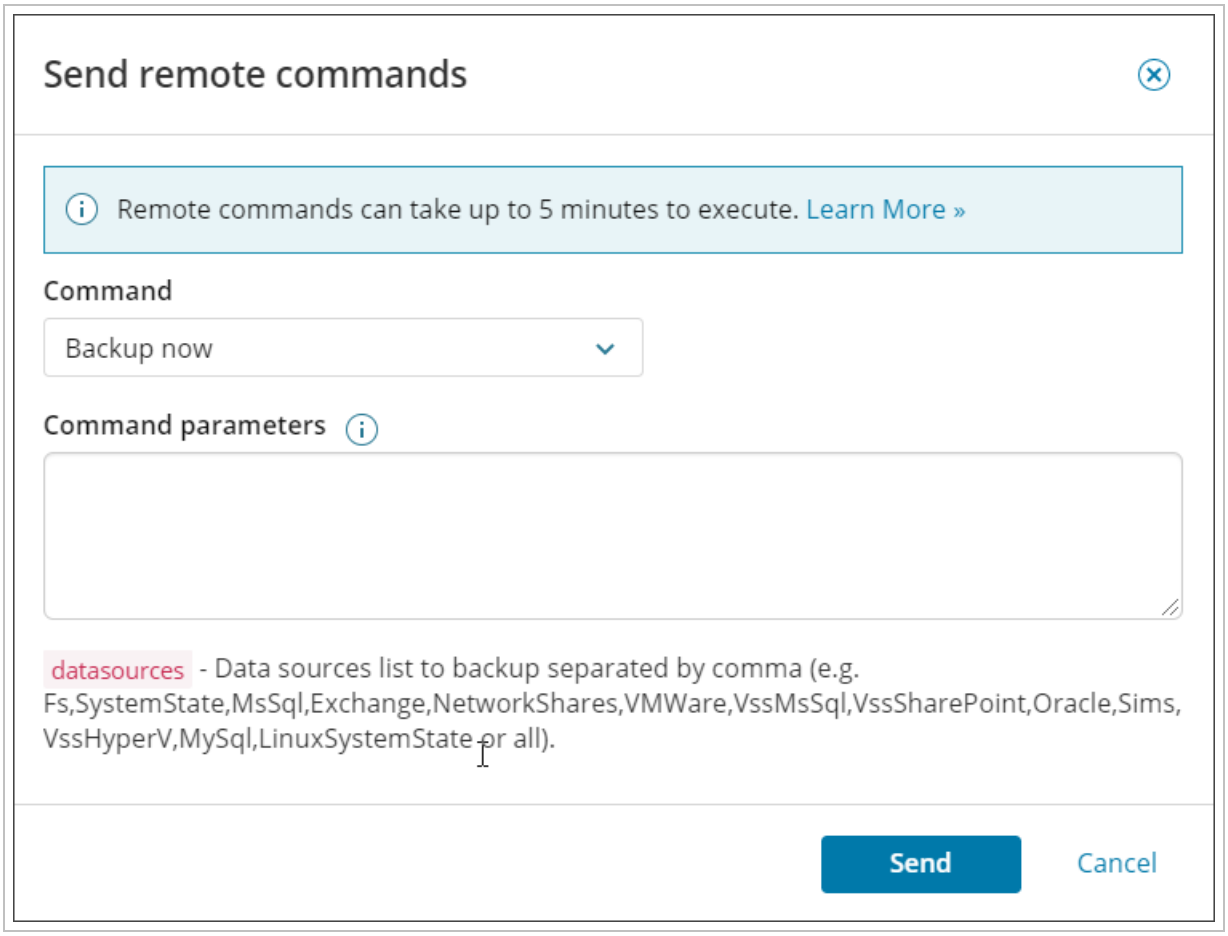
> The Documents solution does not support remote commands. So if you select such a device, the **Remote Commands** option will be disabled.

Instructions

1. Log in to the Management Console under a **SuperUser** account
2. Select one or more devices to send the remote command to
3. Click **More** on the toolbar
4. Select **Remote commands** from the list



5. Using the dropdown on the **Send remote commands** window, select the command you want to submit
6. Configure any Parameters for remote commands (if applicable)



7. Click **Send**

Syntax for parameters

- Parameters must be entered one per line
- After the name of a parameter, enter a space and then a value, for example `datasources Fs`
- Use a comma (,) without spaces to separate the names of data sources, days, weeks and months, for example `unlimitedDays Thursday,Saturday`
- Use a vertical bar (|) without spaces to separate backup filters, for example `add *.doc|*.txt|*.xlsx`

Primary commands

- **Backup now** - starts a backup for the selected device. Unless specified otherwise, all data sources included into the backup selection are backed up
- **Cancel backups in progress** - cancels all backup sessions that are currently in progress on the selected device(s). No parameters are necessary

  All **in progress** restores will also be canceled.

- **Restart backup process** - use this command to restart the internal process associated with Backup Manager. No parameters are necessary

- Set Backup Manager password – use this command to limit access to Backup Manager. It will be necessary to enter the password you have assigned to open Backup Manager. All the preferences stay unchanged and backups continue running according to the schedule
- **Update Backup Manager** – updates the backup software to the latest version. No parameters are necessary

Secondary Commands

- Check Consistency - checks stability of the devices storage and allows any issues found to be repaired. Unless specified, all aspects will be included in the check
- **Check LSV Consistency** - checks stability of the Local Speed Vault or the device selected
- Clear backup selections – removes backup selections from data sources
- Recheck backup selections - enables Backup Manager to perform a full scanning of the backup selection during the next backup session
- Restore – initiates data recovery. Unless specified otherwise, all data sources included into the backup selection are restored
- Set backup archiving – enables the archiving of selected backup sessions (archived sessions will not be deleted from the cloud after their retention period expires)
- Set backup bandwidth – enables bandwidth limitation during backup and restore sessions
- Set backup filter – applies filters to the backup selection
- Set backup scheduling – sets a backup schedule for the selected device
- Set backup selection – lets you configure the backup selection for the selected device
- Set backup settings – lets you configure different settings for the selected device
- Set logging level – sets a custom logging level

Advanced commands

There is a group of advanced commands reserved for some special cases. We **do not recommend using** them unless instructed by a support engineer.

- **Force Activity Start** - forces any periodical activity to start
- **Force commit backup register** - allows re-checking and committing of a backup register. No parameters are required
- Force Update Backup Register - in order to specify tables for updating, fill the names of tables separated by a space in the parameters box

  ✗ this is a legacy command only for use with older versions of (15x and 16x of Cove Data Protection) and is used to update the backup register.

- **Ignore revision** - sends an ignore command in case of an issue with the revision number's synchronization. No parameters are necessary
- **Start Over** - this resets the device as if it were a brand new installation. Before sending this command, you should rename the storage folder for the device. No parameters are necessary
- **Upload audit** – updates audit information for the selected device on a remote server. No parameters are necessary
- Upload logs – Service providers and system administrators who have access to the storage can upload application logs from the selected device there

Parameters for remote commands

Backup now

Parameter	Definition	Required	Supported values
`datasources`	The data sources to back up.	No	▪ `Fs` - Files and Folders ▪ `SystemState` - System State ▪ `MsSql` - MS SQL ▪ `Exchange` - MS Exchange ▪ `NetworkShares` - Network Shares ▪ `VMWare` - VMware ▪ `VssMsSql` - VssMsSql ▪ `VssSharePoint` - MS SharePoint ▪ `Oracle` ▪ `VssHyperV` - Hyper-V ▪ `MySql` - MySQL ▪ `all` (default value)

Here are some examples.

- Run a backup for all data sources:

```
datasources all
```

- Run a backup for Files and Folders and System State:

```
datasources Fs,SystemState
```

Set Backup Manager password

Parameter	Definition	Supported values
`password`	Enter the password that will be required to start Backup Manager	Text. ▪ To **disable** the feature, submit the parameter with no value. ▪ To **reset** the current password, submit the command with a new password.
`restore_`	The parameter sets Backup Manager to the restore-only	▪ `allow`

Parameter	Definition	Supported values
`only`	mode when the GUI password is enabled.	▪ `disallow`

Here are some examples.

- Set new password and set the device to Restore-Only mode when the password is set:

```
password 213TestingS3curE
restore_only allow
```

- Remove password and allow full mode if a new password is set:

```
password
restore_only disallow
```

Check Consistency

Parameter	Definition	Required	Supported values
`level`	What do you want to check	No	▪ `MissingCabinets` ▪ `MissingSlices` ▪ `WrongCabinetLocations`
`repair`	Would you like the check to repair any issues found	No	▪ `true` ▪ `false`

Here is an example.

- Check for and repair any missing cabinets and slices found:

```
level MissingCabinets,MissingSlices
repair true
```

Clear backup selections

Parameter	Definition	Required	Supported values
`datasources`	The data sources to remove selections from.	Yes	▪ `Fs` - Files and Folders ▪ `SystemState` - System State ▪ `MsSql` - MS SQL ▪ `Exchange` - MS Exchange

Parameter	Definition	Required	Supported values
			▪ `NetworkShares` - Network Shares ▪ `VMWare` - VMware ▪ `VssMsSql` - VssMsSql ▪ `VssSharePoint` - MS SharePoint ▪ `Oracle` ▪ `VssHyperV` - Hyper-V ▪ `MySql` - MySQL ▪ `all` (default value)

Here are some examples.

- Remove all data sources:

```
datasources all
```

- Remove Files and Folders and Ms SharePoint data sources:

```
datasources Fs,VssSharePoint
```

Recheck backup selections

Parameter	Definition	Required	Supported values
`datasources`	The data sources to re-check.	No	▪ `Fs` - Files and Folders ▪ `SystemState` - System State ▪ `MsSql` - MS SQL ▪ `Exchange` - MS Exchange ▪ `NetworkShares` - Network Shares ▪ `VMWare` - VMware ▪ `VssMsSql` - VssMsSql ▪ `VssSharePoint` - MS SharePoint ▪ `Oracle` ▪ `VssHyperV` - Hyper-V ▪ `MySql` - MySQL ▪ `all` (default value)

Here are some examples.

- Check all data sources:

```
datasources all
```

- Check just Files and Folders and System State:

```
datasources Fs,SystemState
```

Restore

Parameter	Definition	Required	Supported values
`datasource`	The data sources you want to recover data from (one at a time).	Yes	▪ `Fs` - Files and Folders ▪ `SystemState` - System State ▪ `MsSql` - MS SQL ▪ `Exchange` - MS Exchange ▪ `NetworkShares` - Network Shares ▪ `VMWare` - VMware ▪ `VssMsSql` - VssMsSql ▪ `VssSharePoint` - MS SharePoint ▪ `Oracle` ▪ `VssHyperV` - Hyper-V ▪ `MySql` - MySQL
`restore_to`	The directory you want to recover the data to. If the parameter is skipped or if no value is submitted, the recovery will be performed to the original location (in-place restore).	No	A path, for example `C:\Users\Admin\Documents\Reports`
`selection`	The file or directory to restore. If the parameter is skipped or if no value is submitted, all data from the selected session is restored.	No	A path, for example `C:\Users\Admin\Desktop`
`time`	The session to restore (identified by the date and time).	Yes	A time and date in the following format: `YYYY-MM-DD HH:MM:SS`.

Here are some examples.

- Restore all data sources to the Restore folder in Documents folder from the backup session at 1am on the 1st of December 2019:

```
datasource all
restore_to C:\Users\user_name\Documents\Restore
time 2019-12-01 01:00:00
```

- Restore just the given files from File System to the Restore folder in Documents from the backup session at 1am on the 1st of December 2019:

```
datasources Fs
restore_to C:\Users\user_name\Documents\Restore
selection C:\Users\user_name\Documents\MyProjects\Project1.zip
selection C:\Users\user_name\Desktop\SystemInformation-do-not-overwrite.txt
time 2019-12-01 01:00:00
```

Set backup archiving

Parameter	Definition	Required	Supported values
`clear`	Removes all archived schedules This does not delete any Archived sessions	No	N/A
`datasources`	The data sources to archive	Yes	▪ `Fs` - Files and Folders ▪ `SystemState` - System State ▪ `MsSql` - MS SQL ▪ `Exchange` - MS Exchange ▪ `NetworkShares` - Network Shares ▪ `VMWare` - VMware ▪ `VssMsSql` - VssMsSql ▪ `VssSharePoint` - MS SharePoint ▪ `Oracle` ▪ `VssHyperV` - Hyper-V ▪ `MySql` - MySQL ▪ `all` (default value)
`name`	The name to assign to the new archiving rule.	Yes	Text
`time`	The time when to enable archiving. The archiv-	Yes	Time in the following format:

Parameter	Definition	Required	Supported values
	ing rule will be applied to the nearest backup session that starts after this time.		`HH:MM`
`months`	The months during which to enable archiving.	Yes	Any of the following: ▪ `Jan` ▪ `Feb` ▪ `Mar` ▪ `Apr` ▪ `May` ▪ `Jun` ▪ `Jul` ▪ `Aug` ▪ `Sep` ▪ `Oct` ▪ `Nov` ▪ `Dec` ▪ `all`
`weekday`	The days of the week on which archiving must be performed. This parameter requires the `monthweeks` parameter and cannot be used together with the `monthdays` parameter in the same remote command.	Yes	▪ `Mon` ▪ `Tue` ▪ `Wed` ▪ `Thu` ▪ `Fri` ▪ `Sat` ▪ `Sun`
`monthweeks`	The weeks during which archiving must be performed. This parameter requires the `weekday` parameter and cannot be used together with the `monthdays` parameter in the same remote command.	Yes (unless the `monthdays` parameter is used)	Any of the following: ▪ `first` ▪ `second` ▪ `third` ▪ `fourth` ▪ `last` ▪ `all` Multiple values can be submitted.
`monthdays`	The days of the month on which archiving must be performed.	Yes	The numbers of days separated by a comma (e.g. `1,3,5`) or a slash for periods

Parameter	Definition	Required	Supported values
	This parameter cannot be used together with `weekday` and `monthweeks` in the same remote command.		(e.g. `5-15`).

Here are some examples.

- A one-time archiving rule:

```
name Feb-2018 archive
datasources Fs,VssSharePoint
months Feb
monthdays last
time 07:00
```

- A recurring archiving rule:

```
name Weekly archive (recurring)
datasources Fs,VssSharepoint
time 07:00
weekday Sat
monthweeks all
months all
```

Set backup bandwidth

Parameter	Definition	Supported values
`enable`	The current state of the bandwidth limitation feature	▪ `true` - enabled ▪ `false` - disabled
`start`	Start time of the bandwidth limitation (24-hour time format)	Time (`HH:MM`)
`stop`	End time of the bandwidth limitation (24-hour time format)	Time (`HH:MM`)
`upload`	Maximum upload bandwidth during the specified time interval (kbit/s). Applies to backup sessions.	Number or `unlimited` for unlimited bandwidth
`download`	Maximum download bandwidth during the specified time interval (kbit/s). Applies to recovery sessions.	Number or `unlimited` for unlimited bandwidth
`unlimitedDays`	The days of the week on which bandwidth limitation must be disabled	▪ `Monday` ▪ `Tuesday` ▪ `Wednesday` ▪ `Thursday`

Parameter	Definition	Supported values
		▪ `Friday` ▪ `Saturday` ▪ `Sunday`
`datasources`	The names of data sources that must not be backed up during the bandwidth limitation period (active backup sessions for them will be aborted when the limitation period starts).	▪ `Fs` - Files and Folders ▪ `SystemState` - System State ▪ `MsSql` - MS SQL ▪ `Exchange` - MS Exchange ▪ `NetworkShares` - Network Shares ▪ `VMWare` - VMware ▪ `VssMsSql` - VssMsSql ▪ `VssSharePoint` - MS SharePoint ▪ `Oracle` ▪ `VssHyperV` - Hyper-V ▪ `MySql` - MySQL ▪ `all` (default value)

In the following example, bandwidth limitation is enabled and applied between 08:30 and 18:30 Monday to Friday. The maximum upload (backup) bandwidth is capped at 5000 kbit/s (5 mbit/s), download (restore) bandwidth is not restricted. During the bandwidth limitation period, System State, MS SQL, VMware, MS SharePoint, Oracle, Hyper-V and MySQL backups will not run.

```
enable true
start 08:30
stop 18:30
upload 5000
download unlimited
unlimitedDays Saturday,Sunday
datasources SystemState,VssMsSql,VMWare,VssSharePoint,Oracle,VssHyperV,MySql
```

Set backup filter

At least 1 parameter is required.

Parameter	Definition	Supported values
`add`	Adds a new filter	One or more filters separated by a vertical bar (|). Sample filters are provided below.
`del`	Deletes existing filters	One or more filters separated by a vertical bar (|)
`clean`	Deletes all filters that are currently applied to the backup selection	N/A

Filter formatting tips:

- The asterisk (*) represents zero, any or all characters.
- The question mark wildcard (?) represents any single character.

Here are some sample filters:

- **a*** - Excludes all files starting with the letter a.
- ***.mp3** - Excludes all files with the .mp3 extension.
- **C:\data*.*** - Excludes all files from `C:\data\` path.
- **C:\data*.mp3** - Excludes all .mp3 files from `C:\data\`.
- **C:\data*.m??** - Excludes all files from `C:\data\` with a three character extension starting with .m and ending with any two other characters, such as (.mob, .mov, .mpa, .mpg, .mp3, etc).

Set backup scheduling

Parameter	Definition	Supported values
`clear`	Remove all backup schedules from the device	N/A
`datasources`	The names of data sources to include into the backup schedule	▪ `Fs` - Files and Folders ▪ `SystemState` - System State ▪ `MsSql` - MS SQL ▪ `Exchange` - MS Exchange ▪ `NetworkShares` - Network Shares ▪ `VMWare` - VMware ▪ `VssMsSql` - VssMsSql ▪ `VssSharePoint` - MS SharePoint ▪ `Oracle` ▪ `VssHyperV` - Hyper-V ▪ `MySql` - MySQL ▪ `all` (default value)

Parameter	Definition	Supported values
`name`	The name to assign to the schedule (for your own reference)	Text
`time`	Indicates when to start backup according to the schedule	Time in the following format: "HH:MM"
`days`	The days on which backup must be performed	▪ `Mon` ▪ `Tue` ▪ `Wed` ▪ `Thu` ▪ `Fri` ▪ `Sat` ▪ `Sun` ▪ `all`

Here are some examples.

- Set a schedule to backup File System, System State, MsSql and Exchange at 8pm every week day with the name 'Daily backup':

```
name Daily backup
datasources Fs,SystemState,MsSql,Exchange
time 20:00
days Mon,Tue,Wed,Thu,Fri
```

- Remove all schedules from the device:

```
clear
```

> Be aware, this will delete the schedule for the backup and mean that no backup will run on the device(s) - even if you have a data source selection configured.

Set backup selection

Parameter	Definition	Supported values
`datasource`	The names of data sources to include into the backup selection	▪ `Fs` - Files and Folders ▪ `SystemState` - System State ▪ `MsSql` - MS SQL ▪ `Exchange` - MS Exchange ▪ `NetworkShares` - Network Shares

Parameter	Definition	Supported values
		▪ `VMWare` - VMware ▪ `VssMsSql` - VssMsSql ▪ `VssSharePoint` - MS SharePoint ▪ `Oracle` ▪ `VssHyperV` - Hyper-V ▪ `MySql` - MySQL
`include` or +	The files and directories to include into the backup selection	Path
`exclude` or –	The files and directories to exclude from the backup selection	Path

Here is an example.

- If you want to select the Files and Folders and System State data sources for backup but exclude the given path from Files and Folders you would have to split the command into two and run each part individually:

```
datasource Fs
exclude C:\Users\user_name\Documents\MyProjects-copy\
```

```
datasource SystemState
include System State
```

Set backup settings

Parameter	Definition	Supported values
`user`	A username for access to the remote server	Text
`password`	A password associated with the user name (for access to the remote server)	Text
`passwordPolicy`	Set a policy for the password such as the example given which means 'scrambled password has to contain 6 letters, one	e.g. A-Z,a-z:6|a-z:1|0-9:2|!,$,#,%:2"

Parameter	Definition	Supported values
	of them in a lower case, 2 numbers and 2 symbols from the set {!,$,#,%}' ■ "|" – separator of rules ■ "-" – diapason of rules ■ "," – enumeration of rules ■ ":" – separator of symbols and quantity in a rule	
`EncryptionKey`	Provide an Encryption Key (also known as a Security Code) for the device	Text
`EncryptionMethod`	Use the setting to change the encryption method	■ AES-128 ■ AES-256 (default) ■ Blowfish-448
`ConnectionCheckInterval`	The interval between connection checks	Seconds
`SynchronizationThreadCount`	The number of simultaneous connections during backup (determines data transfer speed)	A whole number from 1 to 10
`LsvSynchronizationThreadCount`	The number of simultaneous connections to the LocalSpeedVault	A whole number from 1 to 10

Parameter	Definition	Supported values
	during backup (determines data transfer speed)	
`Server`	Server IP	IP Address
`UseProxy`	Enables a connection to the Internet through a proxy server	▪ `true` ▪ `false`
`ProxyType`	The type of the proxy server to use	▪ `HTTP` ▪ `SOCKS4` ▪ `SOCKS5`
`ProxyAddress`	The host name or IP address of the proxy server	"192.188.33.55" or "some.server.com"
`ProxyPort`	The port number of the proxy server	Number (0 by default)
`UseProxyAuthorization`	Prompts the Backup Manager that the proxy requires authorization by username.	▪ `true` - authorization required ▪ `false` - no authorization required
`ProxyUsername`	A username for access to the proxy server	Text, for example "domain\username" or "username"
`ProxyPassword`	The password associated with the username for access to the proxy server	Text
`ReconnectAttempts`	How many times the device will attempt to reconnect if an issue is encountered	A whole number from 1 to 3
`PathToLocalStorage`	Indicates where the local copy of	A path. Default values:

Parameter	Definition	Supported values
	the Backup Register is stored	▪ Windows Vista and greater: `C:\ProgramData\MXB\Backup Manager\storage\` ▪ Windows XP and Windows Server 2000: `C:\Documents and Settings\All Users\MXB\Backup Manager\storage\` ▪ Linux: `/opt/MXB/var/storage/` ▪ macOS: `/Library/Application Support/MXB/Backup Manager/storage/`
`LogsLocation`	The location of the application log on the hard drive	A path. Default values: ▪ Windows XP and Windows Server 2003: `C:\Documents and Settings\All Users\Application Data\MXB\Backup Manager\logs\BackupFP` ▪ All Windows versions starting from Windows Vista (for client versions) and Windows Server 2008 (for server versions): `C:\ProgramData\MXB\Backup Manager\logs\BackupFP` ▪ macOS: `/Library/Logs/MXB/Backup Manager/BackupFP` ▪ GNU/Linux: `/opt/MXB/var/log/BackupFP`
`TempDir`	The location of the temporary files created by Backup Manager	A path (set to the system Temp directory by default)
`MsSqlDeltaRestore`	MsSQL delta	▪ `true`

Parameter	Definition	Supported values
	restore	▪ `false`
`SuppressCircularLoggingMessage`	Use this setting to hide a message prompting users to disable circular logging before backing up MS Exchange	▪ `true` ▪ `false` (default)
`MailAddress`	Email address used for dashboard emails	Text
`MailSendPeriodicity`	The days on which backup reports are sent out	▪ `0` - daily ▪ `1` - on Wednesdays and Saturdays ▪ `2` - on Saturdays ▪ `3` - never
`HyperV::UseSnapshotLimitsOnBackup`	Use HyperV snapshot limits on backup	▪ `true` ▪ `false` (default)
`HyperV::LimitSnapshotComponentsCount`	Set a limit for number of components that the snapshots can include	A whole number (0 for unlimited)
`HyperV::LimitSnapshotSizeGB`	Set a limit for the maximum snapshot size	A whole number (0 for unlimited)
`MsSql::UseSnapshotLimitsOnBackup`	Use MsSQL snapshot limits on backup	▪ `true` ▪ `false` (default)
`MsSql::LimitSnapshotComponentsCount`	Set a limit for number of components that the snapshots can include	A whole number (0 for unlimited)
`MsSql::LimitSnapshotSizeGB`	Set a limit for the maximum snapshot size	A whole number (0 for unlimited)
`BackupThreadsCount`	The number of con-	A whole number from 1 to 10 (default is

Parameter	Definition	Supported values
	nections the backup device can make at once	4 even when no configuration set)
`IgnoreMissedScheduledBackup`	Ignore a backup if the schedule is missed	▪ `true` ▪ `false`
`LocalSpeedVaultUnavail-abilityTimeoutInDays`	Period in days that specifies the allow-able LocalSpeedVault unavailability time	A whole number
`ConnectTimeout`	Period in seconds that specifies how long is allowed until the con-nection times out	Time in seconds. Default: 10 seconds

Here are sample **proxy** settings for your reference:

```
UseProxy true
ProxyType HTTP
ProxyAddress 192.188.33.55
ProxyPort 25
UseProxyAuthorization true
ProxyUsername kowalsky
ProxyPassword 123456
```

Set logging level

Parameter	Definition	Required	Supported values
`level`	The new logging level to apply.	Yes	▪ `0` - debug (includes debug, warning, error and log levels) ▪ `1` - warning (includes warning, error and log levels) ▪ `2` - error (include error and log levels) ▪ `3` - log. This is the default

Here is an example.

- Set logging level to debug:

```
level 0
```

Advanced commands

Force Update Backup Register

> This is a legacy command and only works for devices running older versions of Backup Manager (15x and 16x).

Parameter	Definition	Required	Supported values
`tables`	Tables separated by spaces (e.g. os.d st.d).	Yes	A table, for example `os.d`

Here is an example.

- Update the os.d and st.d tables:

```
tables os.d,st.d
```

Upload logs

By default, the path to the log on the storage node is as follows:

- Windows: `c:\storage\`**`<device_name>`**`\dumps\logs\`**`<device_name>`**
- Linux: `/storage/`**`<device_name>`**`/dumps/logs/`**`<device_name>`**

`<device_name>` is the name of the device the log was created for.

Parameter	Definition	Required	Supported values
`server`	The address of the server to upload logs to.	No	`scheme://address:port`
`user`	A username for access to the remote server.	No	Text
`password`	A password associated with the user name (for access to the remote server).	No	Text

Here is an example.

- Upload logs to this server using these login details:

```
server scheme://1.1.0.0:8443
user user_name
password user_password
```

Backup Profiles in Management Console

Backup profiles let system administrators configure backup settings for multiple devices as one.

> Profiles are available to the following types of customers: **distributors**, **sub-distributors**, **resellers**, **end-customers** and **sites**.

> Profiles are supported for Windows, macOS and Linux backup devices

Two default profiles are available for use:

- **1 hour RPO** - To configure hourly backups
- **24 hour RPO** - To configure daily backups

> Custom Profiles can be created by following the steps on Create Custom Backup Profiles

Backup profiles versus products

Profiles are similar to products but they are more specific. Unlike products, backup profiles are **optional**.

Permissions configured through the backup profiles are added up to the product permissions. To be available on a device, a setting must be activated both in the product and in the profile.

Limitations

- Custom Profiles cannot be moved to different customers
- Pre- and post-backup scripts are not compatible with backup profiles

  > Once a profile is assigned to a device, the **Scripts** tab under Backup Manager Preferences will not be displayed.

- When a profile is assigned to a device, the Performance tab of the Backup Manager GUI will no longer display the **Abort backups and do not start backups when limited time frame is reached for these backup data sources** option
- Profiles can only be used for the customer it was created for, or child customers of this

  > i.e. a Profile created at Reseller1 can be used on devices for this customer or any end-customers or sites of this customer, but cannot be used at the distributor or sub-distributor level, or on Reseller2.

LocalSpeedVault settings in backup Profiles

To prevent data loss caused by the profile applying the incorrect LocalSpeedVault credentials when not fully synchronized, LocalSpeedVault settings can no longer be applied in a profile.

The profile must be disabled before configuration of the LocalSpeedVault can be applied.

1. Disable device profile
   - In Management Console, select device checkbox in the dashboard > *Assign Profile* > Choose *no profile*
2. Restart Backup Service Controller on affected device to apply the changes

   > Alternatively, wait 15 minutes and the changes will be applied automatically

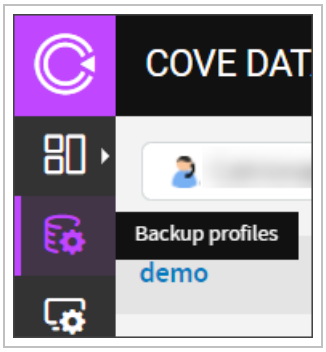
3. Launch the Backup Manager and change the LocalSpeedVault details to the correct location and save
4. Re-apply the profile
   - In Management Console, select the device checkbox in the dashboard > *Assign Profile* > Choose the profile you removed in step 1

   > Once the LocalSpeedVault is fully synchronized, further changes can be made from the profile

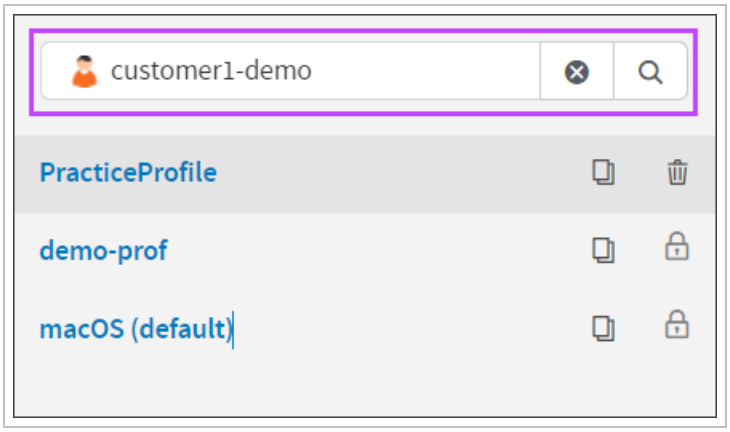
Managing Profiles

Edit Existing Profiles

1. Log in to the Management Console
2. Select **Profiles** from the vertical menu on the left-hand side of the page



3. Choose the Customer the Profile belongs to from the dropdown



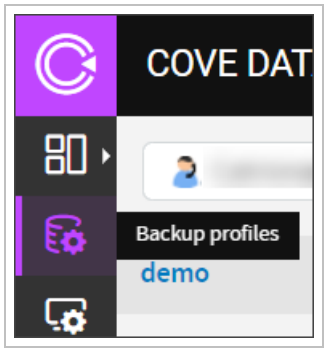
4. Click on the Profile name to edit

5. The Profile will open on the panel to the right, make any required changes
6. **Save** the changes at the bottom of the page

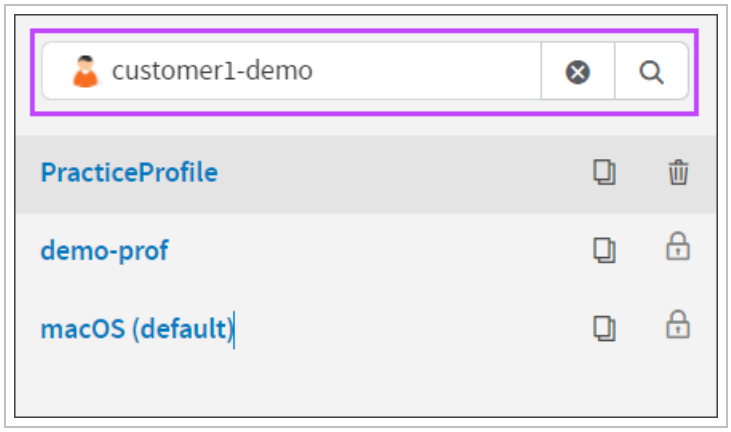
Find a Profile ID and Version

Backup Profile IDs are generated automatically when the automatic deployment is enabled.

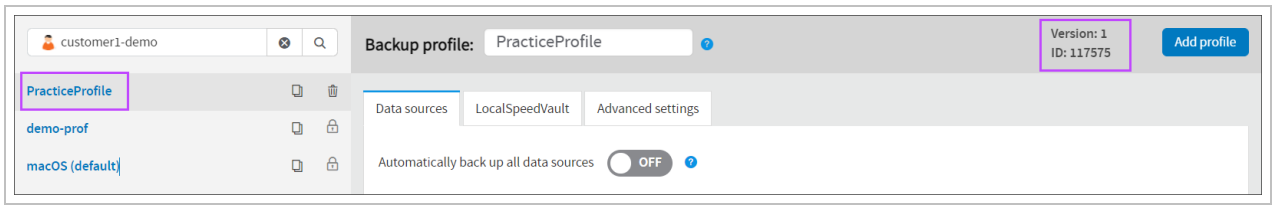
1. Log in to the Management Console
2. Select **Profiles** from the vertical menu on the left-hand side of the page



3. Choose the Customer the Profile belongs to from the dropdown



4. Click on the Profile name you need the ID or Version for

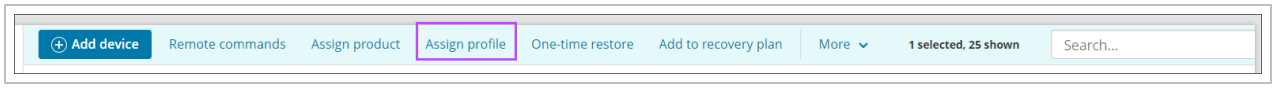


5. The ID and Version number can be found at the top right of the page

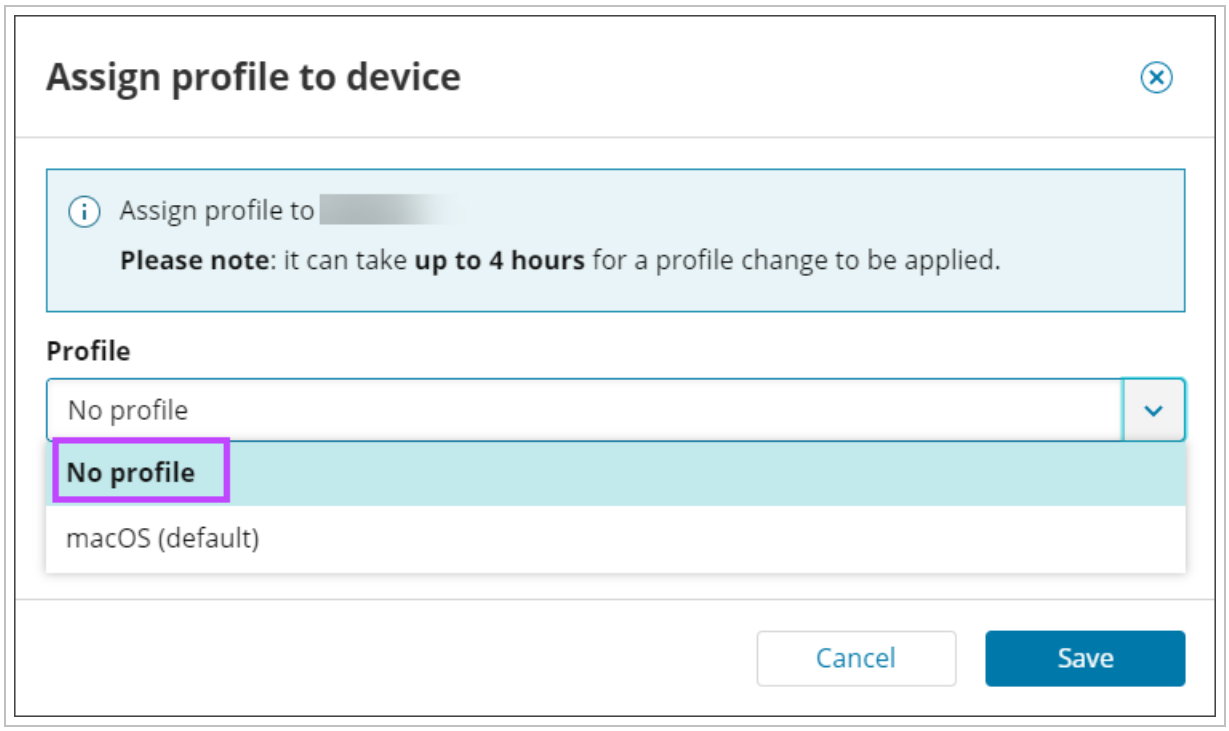
Removing and Deleting Profiles

Remove a Profile

1. In the Management Console, select the devices to remove the profile from
2. Click **Assign Profile** on the toolbar



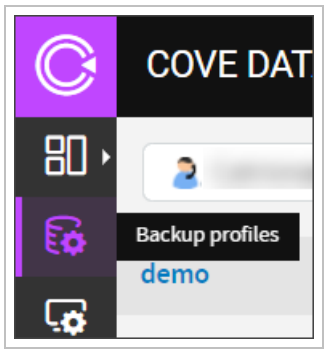
3. Select **No Profile** from the dropdown



4. Click **Save**

Delete a Profile

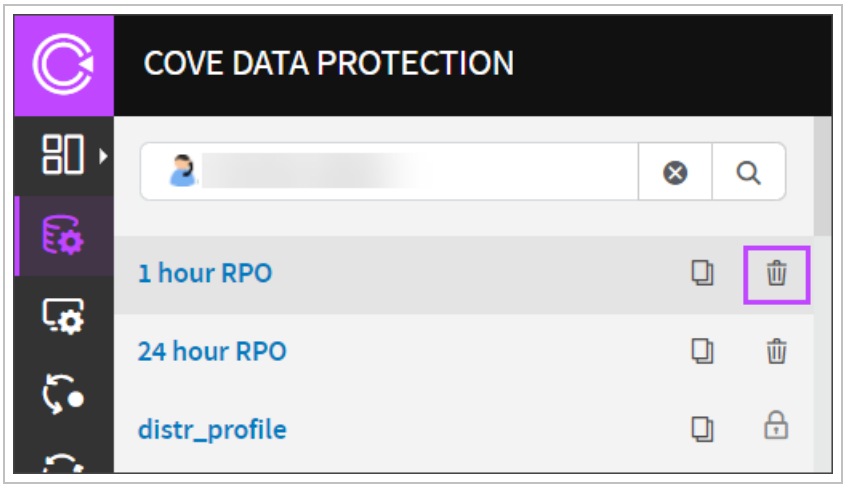
1. Log in to the Management Console under a **SuperUser** account
2. Select **Profiles** from the vertical menu



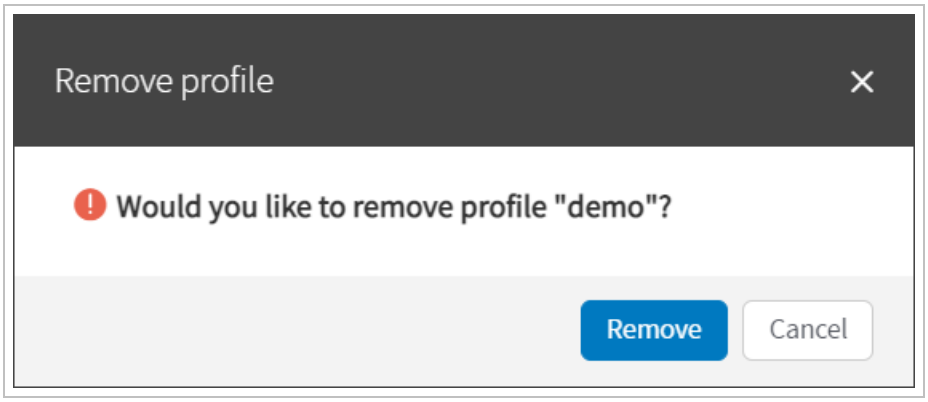
3. Find the profile you wish to delete

> Only those profiles that are **not assigned to any devices** can be deleted.

4. Click the trashcan icon to the right of the profile name



5. You will be prompted to confirm you wish to delete the profile. Click **Remove**



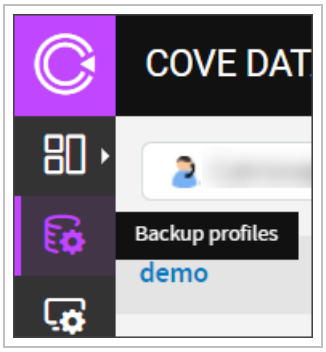
> Profiles that have been deleted **cannot** be restored. If you need a profile that has been deleted, you must recreate it manually.

Create Custom Backup Profiles

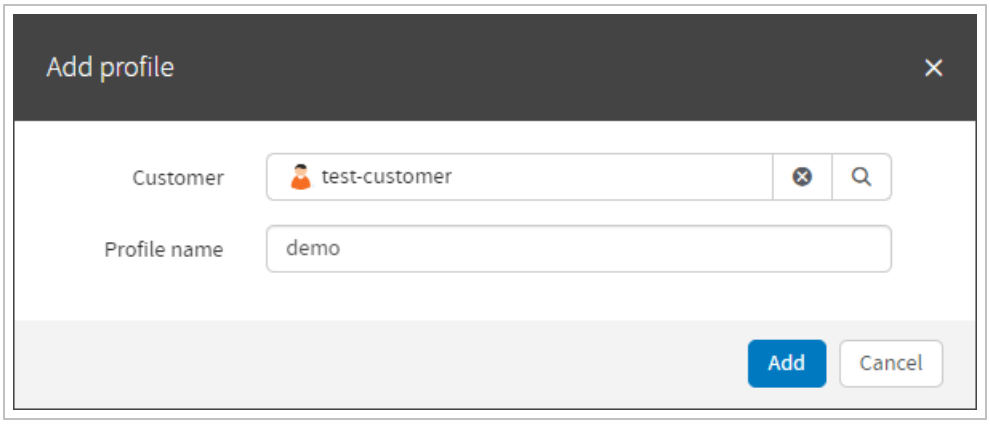
Add a Profile

From New

1. Log in to the Management Console under a **SuperUser** account
2. Select **Profiles** from the vertical menu



3. Click **Add profile**
4. Assign a name to the profile and specify the name of the customer the profile will be available to



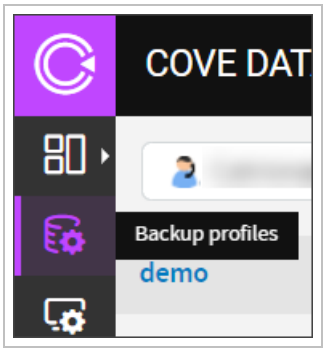
5. Click **Add**

> **Tip:** Create a separate backup profile for each operating system.

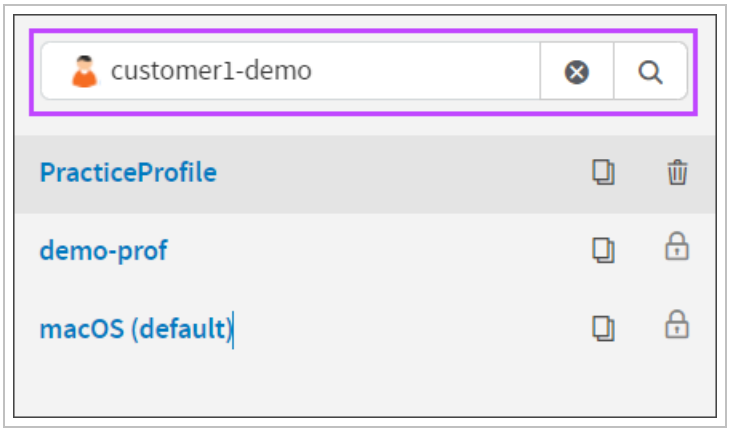
By Copying Existing Profiles

If you have an existing profile which you need to duplicate, this can be done by:

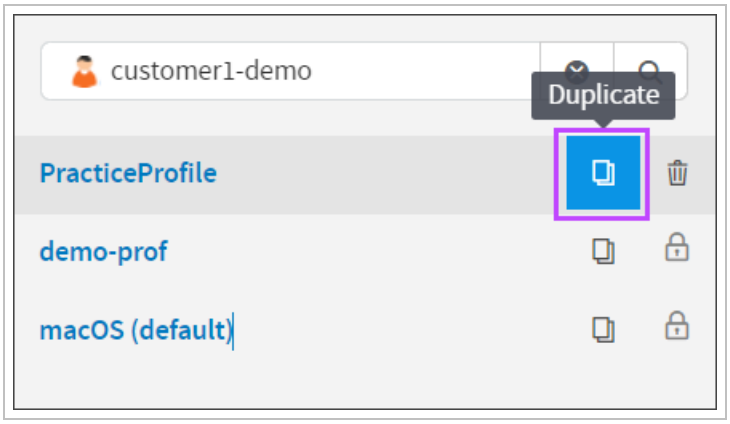
1. Log in to the Management Console
2. Select **Profiles** from the vertical menu on the left-hand side of the page



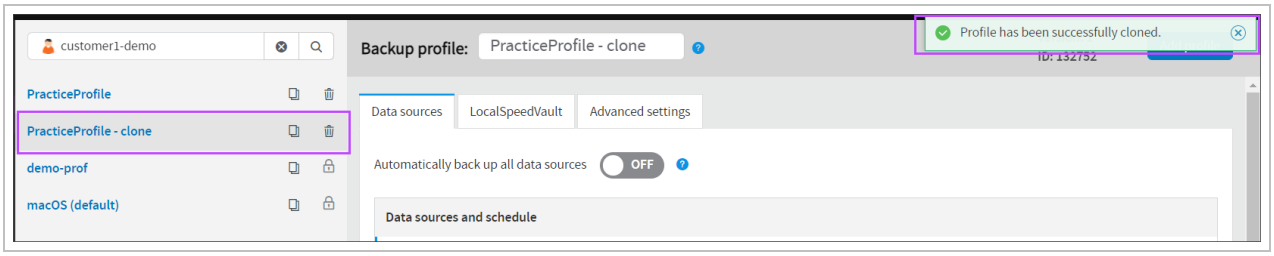
3. Choose the Customer the Profile belongs to from the dropdown



4. Find the Profile you need to duplicate and click the **duplicate** icon to the right of the profile name



5. Once the profile has been copied, a banner will be displayed to advise the profile has been successfully cloned and it will appear in the Profiles list with the same profile name '***ExistingProfileName* - clone**'



6. Make any required changes to the copied profile
7. Click **Save** at the bottom of the page

Configure the Profile

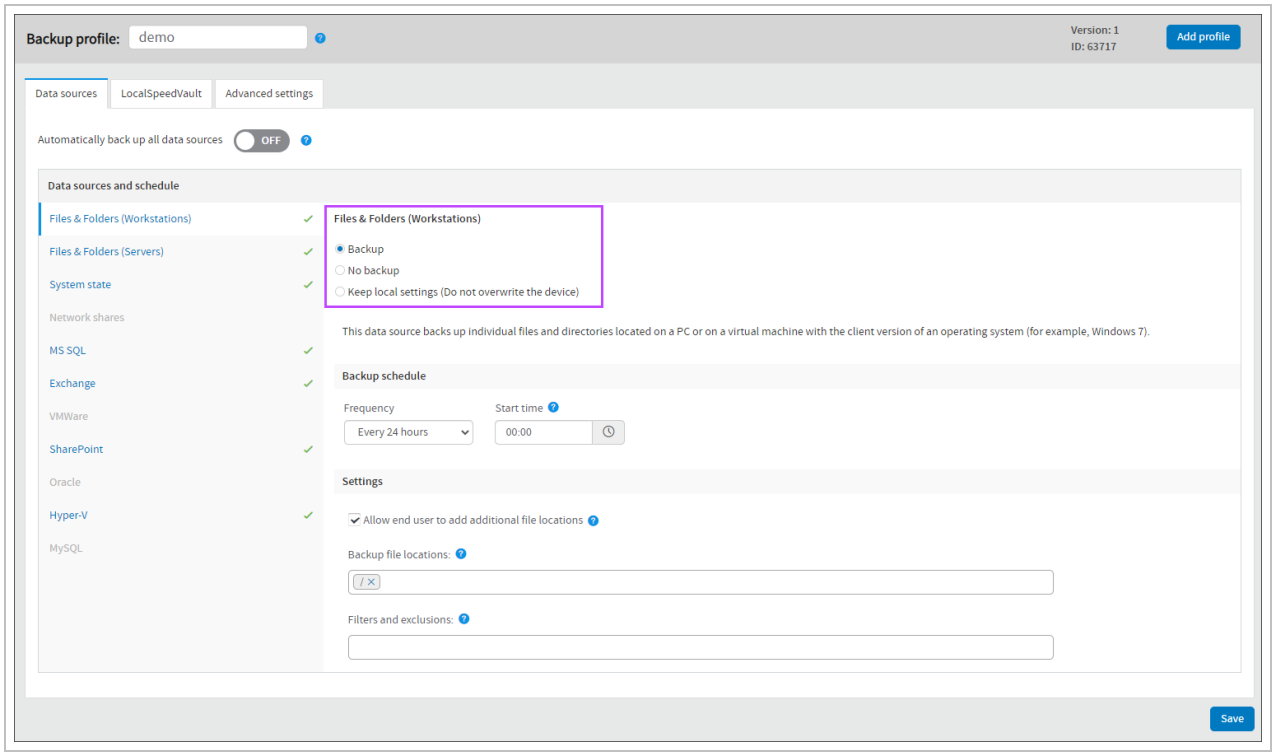
Once the profile has been created, either from new or by duplicating an existing one, you can configure all settings required:

> These steps must be followed for **each data source** you wish to configure under the profile

1. Select the Data Source
2. Select the **Backup Policy** to use

   There are 3 **backup policies** to choose from:

   - **Backup** - a force backup policy (overwrites local settings). It covers both the backup schedule and the backup selection. It is unavailable for data sources that require access credentials (such as Oracle or Network shares)
   - **No backup** - excludes a data source from backup, even if it is included in the backup selection locally
   - **Keep local settings**. This is a mixed option using which the backup schedule is configured through the profile while the backup selection is configured locally



3. Configure the policy **Backup Schedule**
   a. Select the Frequency

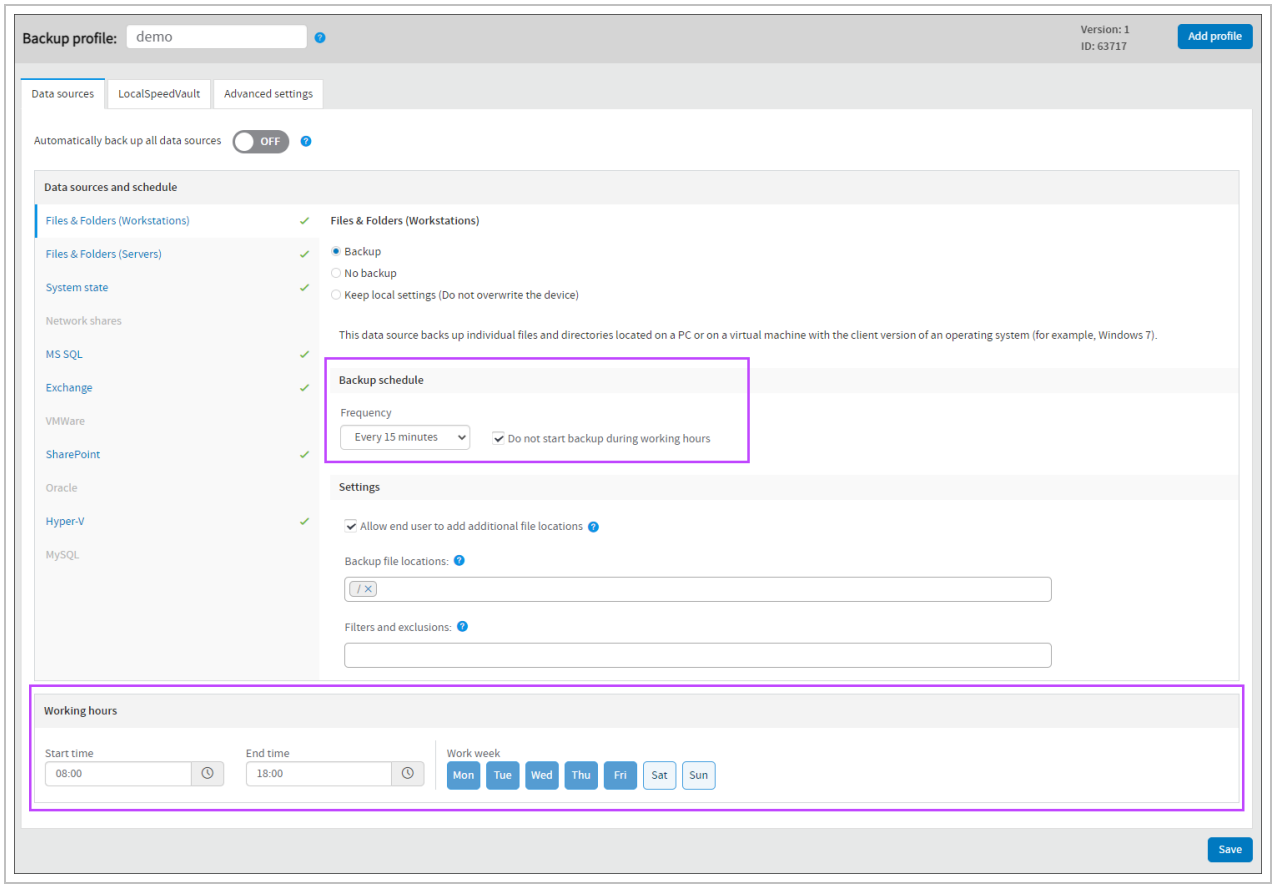
      The following frequencies can be selected:

      - Every 24 hours
      - Every 12 hours
      - Every 6 hours
      - Every 4 hours
      - Every 2 hours
      - Every 1 hour
      - Every 30 minutes
      - Every 15 minutes

   b. Choose a start time for the schedule

      > Start Times can only be provided for the 24 hour, 12 hour and 6 hour frequencies

   c. If not using the **Every 24 hour** frequency, you will also be provided with an option to prevent backups starting during working hours. When selected you will be required to provide working hours at the bottom of the screen



> Prior to the 18.4 release, backup schedules configured through the profiles ran on a certain **day/time** basis. Those older schedules were automatically converted to the new **frequency-based** format, which allows backups to run more frequently and make sure all file changes are protected.

4. Apply additional settings as required, such as:
   - **Auto select locations** - Checking this allows the profile to auto-populate the backup selection with documents, images and videos that have been detected on the machine

     > This option will **only** be available for profiles where the setting was previously enabled.

   - **Backup file locations**[1] - This option is only available if **Auto Select Locations** is un-checked and allows you to select the specific locations to be backed up
   - **Fail backup if data source not present** - Only available on certain data sources including MS SQL, Exchange, SharePoint and Hyper-V, this setting - when enabled - will cause the backup to fail if the source is not present on the device where this profile is assigned
   - **Filters or exclusions** - Enter any file types or locations to be excluded from the backup

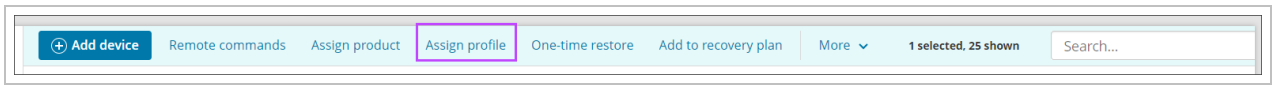
     > For a list of predefined filters, examples of file type exclusions and suggested additional filters, see Backup Filters and Exclusions

5. Click **Save**

Assign the profile to devices on the Management Console

When the profile is ready, you can assign it to devices:

1. In the Management Console, select the devices to assign the profile to
2. Click **Assign Profile** on the toolbar



3. Select the profile from the list
4. Click **Save**
5. (optional) Add the **Profile** column to the view (to see the profiles assigned to each device)

> You can edit, rename and delete existing profiles. Only those profiles that are not assigned to any devices can be deleted.

Backup Filters and Exclusions

Backup filters can be used when creating backup Profiles, or in the configuration of individual backup devices via the Management Console.

Benefits

Adding additional filters to the exclusion lists can benefit you in a number of ways:

---

[1]The path to a local volume where files for backup are located, e.g. D:\User\Data (Windows) /Users/Data (Linux) / (Unix)

- **Backup speed** can increase as there are less files and changes to these files to process
- **Bandwidth** use can decrease as there is less data to send
- **Storage space**can decrease as less is required due to the drop in data
- **Restore speed** can increase as there is less data to restore

Predefined filters

Some files are automatically **excluded from backup** on Windows devices **only**, except when using certain security features of Products.

> These predefined filters only work on Windows devices by the use of a standard 'files not to backup' entry in the **Windows Registry**, meaning there is no alternative for Linux or macOS devices.

What files are automatically excluded from backup:

1. All files indicated in the registry subkey:

   ```
   HKEY_LOCAL_
   MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup
   ```

   Typical examples:

   - `\Pagefile.sys`
   - `\hiberfil.sys`
   - `%TEMP%\* /s`

2. All files from the Backup Manager installation folder
3. Temporary files of no importance:

   - ```
     C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer\IconCacheToD
     elete
     ```

     > There is such a file for every user account registered in the system

   - ```
     C:\Users\<username>\AppData\Local\Microsoft\Internet
     Explorer\DomainSuggestions
     ```

     > There is such a file for every user account registered in the system

   - ```
     C:\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\CLR
     Security Config\v2.0.50727.312\64bit
     ```

   - Files from the **Print Spooler** folder
     ```

4. Files/folders matching the following masks:
   - `*\Local Settings\Temporary Internet Files\*`
   - `?:\RECYCLER`
   - `?:\System Volume Information`
   - `%systemdrive%\$WINDOWS.~??` (for example `C:\$WINDOWS.~BT` or `C:\$WINDOWS.~WS`
   - `%SYSTEM_ROOT%/Windows/*.config.cch`
   - `?:\swapfile.sys`
   - `?:\pagefile.sys`
   - `?:\hiberfil.sys`
   - `*\AppData\Local\Temp\*` (on Windows Vista and Windows 7)
   - `*\Local Settings\Temp\*` (on Windows XP)

File Type Examples

Filters based on file type are the same across all Operating Systems.

Here are some example filters you can add:

- **a*** - excludes all files starting with the letter "a"
- ***.mp3** - excludes all files with the .mp3 extension
- `C:\Data\*.*` - excludes all files in the `C:\Data\..` path and underlying folders
- `C:\Data\*.mp3` - excludes all files in the `C:\Data\..` path, with the .mp3 extension
- `C:\Data\*.m??` - excludes all files in the `C:\Data\..` path, with a three-character extension starting with .m and ending with any two other characters, such as .mob, .mp3, .mov or .mpg

> The filters are applied to **upcoming backup sessions**. Older backups stay as they are.

Suggested Additional Filters

We would strongly advise to add the following additional exclusions to your filters:

Windows temp locations

- `*\Microsoft\Windows Defender\Scans\mpcache*`
- `*\AppData\Local\Microsoft\Outlook\*.ost`

Chrome/Edge/Firefox browser cache and update files

- `*\Chrome\User Data\*\Cache\*`
- `*\Local\Microsoft\Edge\User Data\Default\Cache\*`
- `*\Local\Mozilla\Firefox\Profiles\*\cache\*`

N-central cache directories

- `*\PME\archives\*`
- `*\NablePatchCache\*`
- `*\SolarWinds.MSP.CacheService\cache\*`
- `*\N-able Technologies\UpdateServerCache\*`

AV Defender cache files

- `*\ThreatScanner\Antivirus*\Plugins\cache.*`

EDR/SentinelOne

- `*\ProgramData\Sentinel\data\*`

Product management in Management Console

In the Console, a **Product** refers to a service package based on a combination of features and storage options.

You can use products in many ways. Here are some typical examples.

1. As **real-world products** that your clients actually sell or subscribe to (e.g. "Windows Files & Folders w/100 GB Storage & 30-day Retention" or "Database Backup, Unlimited Storage")
2. As internal **system administration tools** to differentiate feature access across devices. It helps prevent the accidental inclusion of unnecessary files (especially large ones) into a backup selection or an unwanted restore that would overwrite the current files on a user's computer. Examples of such products: "MS Sharepoint backup, scripts & selection off" or "Full system state backup w/o restore"
3. As a **temporary measure** to limit access to the service (for example, in case of an overdue payment)

Each time you add a device, you need to assign a product to it. This can be a pre-defined product such as **All-In** or, you can create custom products based on your requirements.

Our **All-in** product has all features enabled, all security selection options are set to "Unlimited" and the retention period (History Limits) of 28 days.

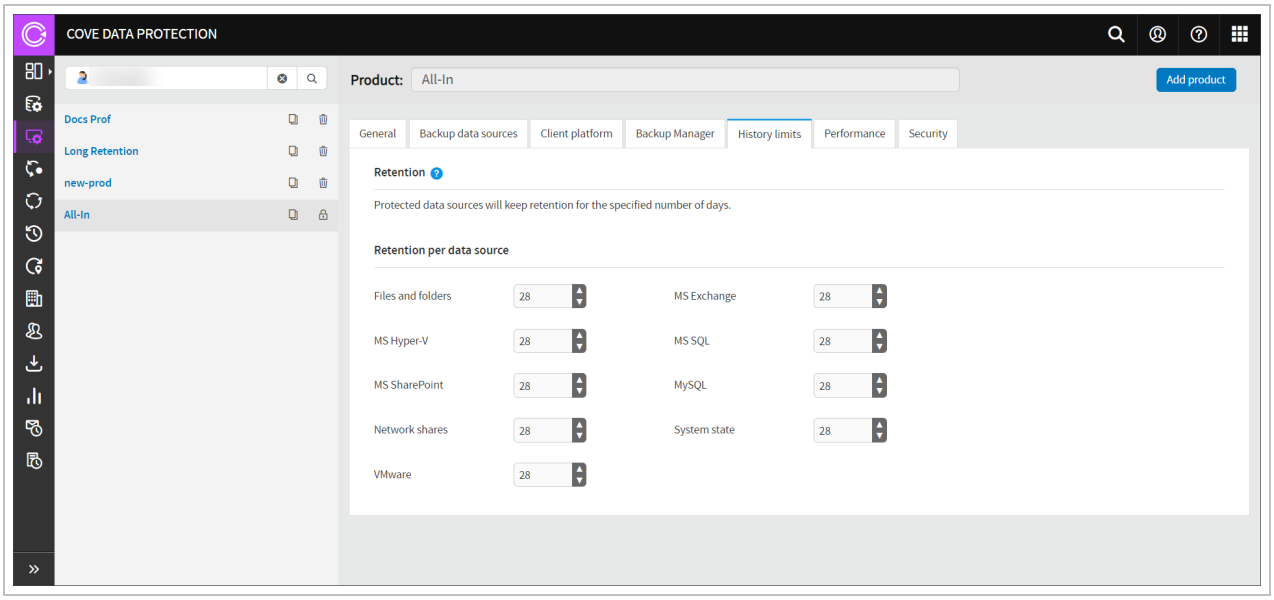
> The maximum retention on any custom product is **365 days**.

> Backup session data can be stored for longer than the retention period by using Archiving backup sessions in Backup Manager.

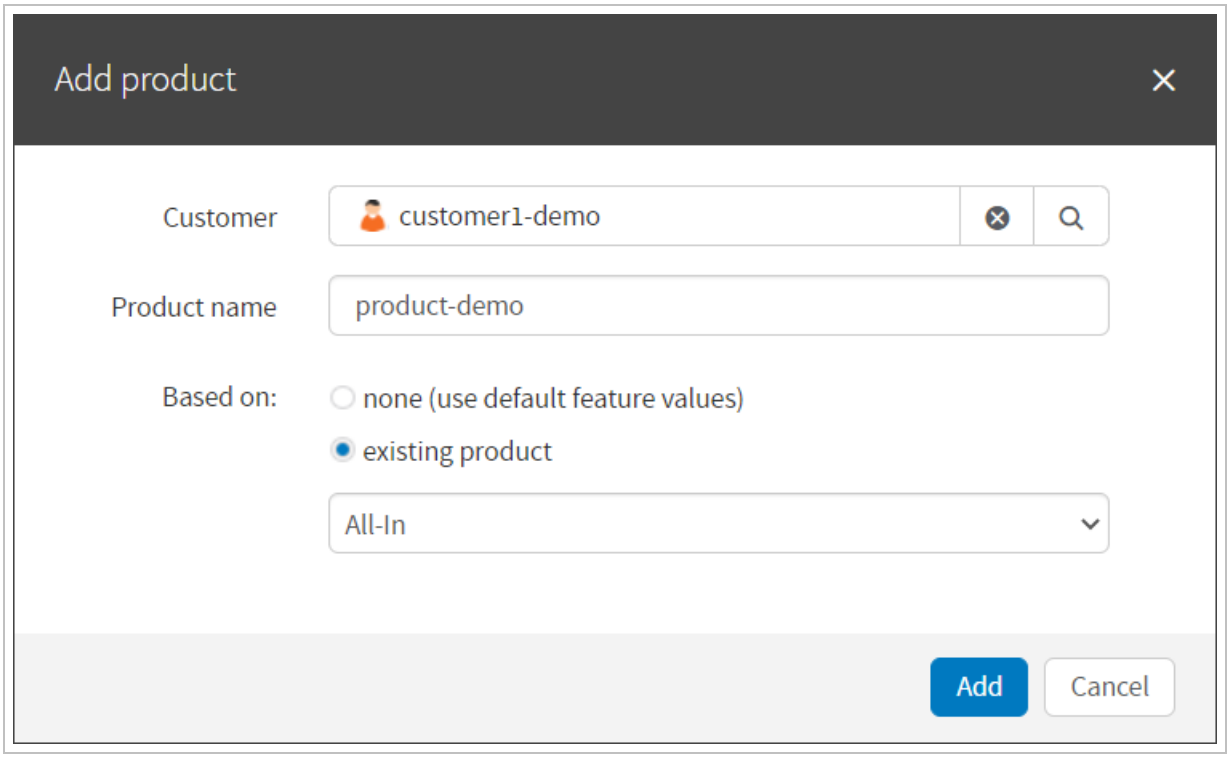
Creating custom products

Here is how to create a custom product:

1. In the vertical menu, click **Products** to view the Product Management page



2. Select the customer to create the product for
3. Click **Add product**
4. Fill out the fields and click **Add**



Custom product options

The following options are available when adding or editing a custom product. Place a tick the box to allow the product feature.

Option	Permission
General	
Advanced scheduling	Allows scheduled backups (if disabled, only manual backups are available).
Archiving	Mark set backup sessions as archive points so they are not cleared after the retention period expires. For information on configuring the retention period, see **History Limits** below.
Automatic File Selection	Enables the "Automatic file selection" option for Files and Folders which automatically detects documents, images and videos for backup.
Backup Accelerator	Enables use of the Backup Accelerator driver which avoids unnecessary scanning of the full system (and whole files) by tracking changes as they happen on the device.
Bare metal recovery	Enable and perform a bare metal recovery.
Directory size calculation	This displays directory sizes in the Backup Manager UI when navigating file systems.
No restore	Sets the device to a mode where the restore options on the device are no longer available.
Pre- and post-backup actions	Allows script execution to run before and/or after backups. These scripts run once per backup source.
Priorities	Mark critical files and folders as high priority. Backups perform those of high priority items first.
Proxy	Allows connection through a proxy server. We support HTTP, SOCKS4 and SOCKS5 proxies.
Restore only	Sets the device to a mode where the backup options on the device are no longer available.
Standby Image	A legacy continuous restore feature which restored directly to VHD. It remains available **only** to customers who used this feature prior to its removal and are still using it. The feature was succeeded by the Recovery Console's continuous restore functionality.
VSS snapshot management	Enables optimized VSS snapshot creation, minimizing memory consumption.
Virtual disaster recovery	Enable the virtual disaster recovery. Further steps are required to perform this. See Virtual disaster recovery guide
Virtual drive	Use the Virtual Drive utility to browse backups like a file system and access data faster.
Backup Data Sources	
Backup Data	Allows the backup selection of the data sources. If unticked, these data source will not be available

Option	Permission
Sources	for backup in the Backup Manager: ▪ MS Exchange ▪ MS Hyper-V ▪ MS SQL ▪ MS SharePoint ▪ MySQL ▪ Network Shares ▪ System State ▪ VMware
Client Platform	
Windows OS	Select the Windows operating system versions to allow the Backup Manager to be installed on. If unticked, these operating systems will not be available for Backup Manager.
Other OS	Select the operating systems to allow the Backup Manager to be installed on. If unticked, these operating systems will not be available for Backup Manager: ▪ Linux ▪ macOS
Backup Manager	
Adjustable backup selection	Allows the backup selection to be edited via the Backup Manager
Allow filters	Exclude the specific file types from backups.
Branding	Apply branding to the Backup Manager. Branding is configured in the Backup Console. You can remove references to the developer, enter a custom name, logo, color scheme and icons.
Restore to network shares only	Forces restores to be performed to a network share rather than the local device.
Search in restore	Filter the data available for recovery.
Settings	Enable the **Preferences** menu in the Backup Manager.
History Limits	
History Limits	Protected data sources will keep retention for the specified number of days. By default we store backup sessions for 28 days. We will store any backup sessions marked as archives until a user deletes the session.
Retention per data	The number of days to keep sessions for.

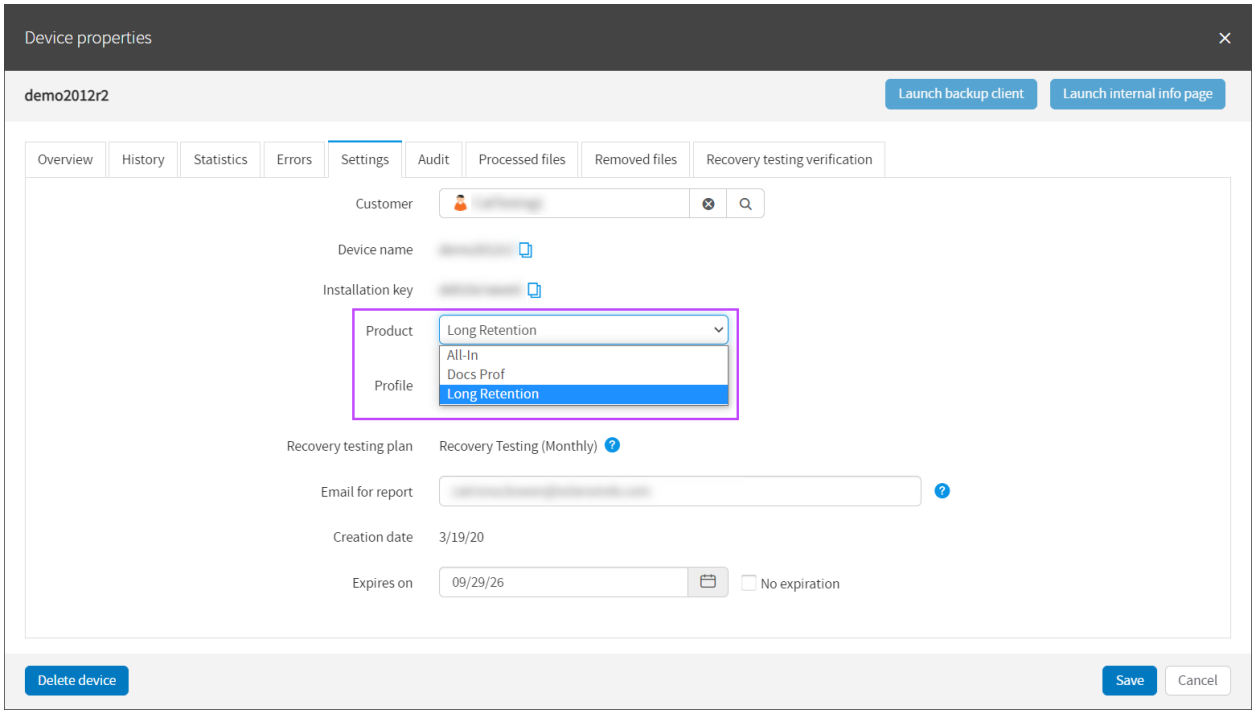
Option	Permission
source	The maximum is 365 days
Performance	
Bandwidth throttling	Limit the bandwidth used by the Backup Manager during the specified time periods.
LocalSpeedVault	Allows enabling of the LocalSpeedVault.
Maximum Bandwidth (Kbit/s)	Set the upper bandwidth limit (cap) for a device.
Security	
Backup users rights	Allows restoring data with the same permissions as were used during the backup.
Ignore FilesNotToBackup registry key (Windows Only)	The following registry key will be ignored: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup` This means that you will need to define your own system exclusions either directly in each backup manager, or more conveniently, in Backup Profiles in Management Console. This setting is not recommended for most devices.
Remote Management	Permit remote access and management through the Backup Manager.
Maximum file size	Set the threshold for the maximum size of a single file in the backups. If the **Maximum file size** is set to Unlimited, this means there is no limit. Files of *any size* can be backed up.
Maximum selection size (data source)	Set the threshold for the maximum selection amount allocated per data source.
Maximum selection size (total)	Set the threshold for the maximum selection amount allocated per backup job.
Maximum used storage	Set the threshold for the maximum storage amount allocated for backups from a device.

Assign Product

Assigning a product to a device can be done one of two ways within the Management Console:

From Device Properties

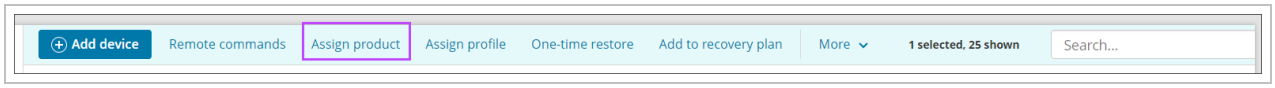
1. Click the device name to open Device Properties
2. Navigate to the **Settings** tab
3. Select the **Product** to assign to the device from the Product dropdown



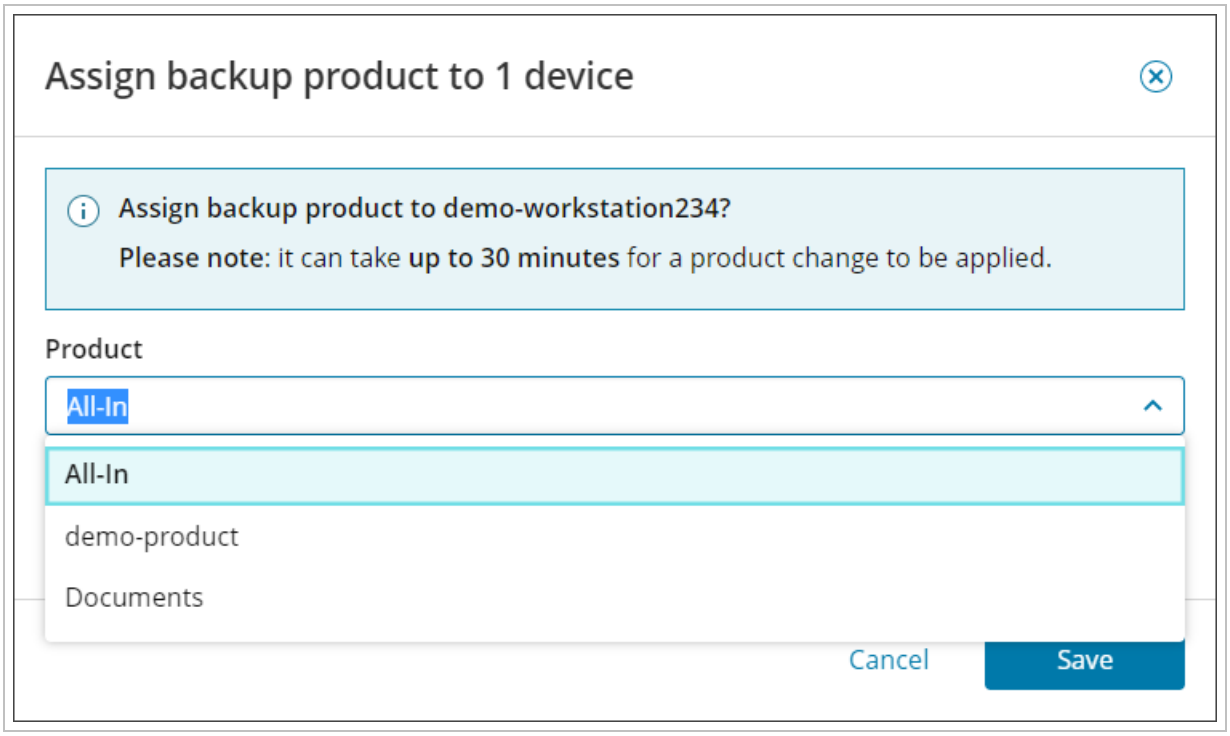
4. Click **Save**

From the Assign option on the Toolbar

1. In **Backup > Dashboard**, select the devices to assign a profile to
2. Click **Assign Products** on the toolbar



3. In the **Assign Backup Product** window, select the product to assign from the dropdown



4. Click **Save**

> If the **Save** function is not available, this means the selected product is already assigned to the device.

Edit Product

To edit an existing product, do the following:

1. In the **Customers** filter, select the customer that owns the product
2. In the **Products** list, select the product you want to change
3. Edit the options on the right

The devices to which this product is assigned will be updated within the next 15 minutes.

If reducing the History Limits (retention period) of a product when editing it, all data that is no longer within this retention period will be removed during the cleaning phase of the next backup unless the session is marked as an archive point.

> You can only edit products created by your own company and your customers. All other products are locked.

Rename product

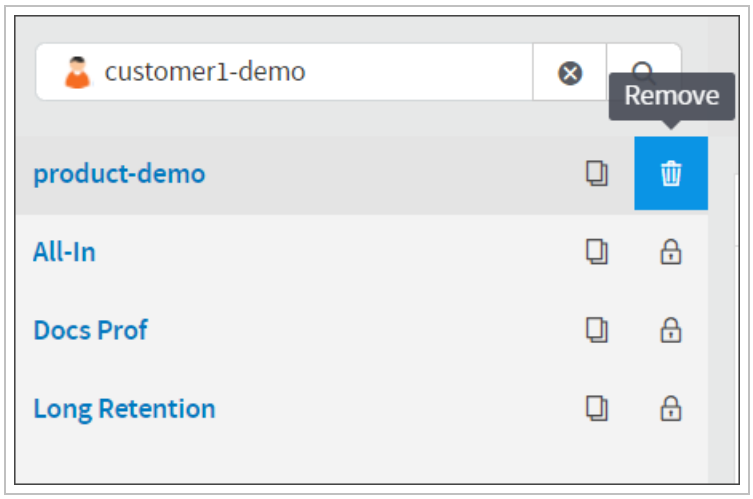
To rename a product:

1. Open the product on the **Product Management** page
2. Rename the product in the text box at the top
3. Click **Save**

Remove product

If you no longer need a product, it can be removed by:

1. Open the product on the **Product Management** page
2. Click the **Remove** icon



3. Confirm your intention to remove the product by clicking **Remove** on the Remove Product popup

> If the remove icon is replaced by a padlock, this means the product has been created by a user at a higher level than yourself. Products can only be removed by the user level it was created at or higher.

> If you remove a product from a device which gave the device a longer retention period than the default 28 days, all data that is no longer within the retention period will be removed during the cleaning phase of the next backup unless the session is marked as an archive point.

Continuity In Management Console

Management Console contains different continuity services that can be used for disaster recovery:

- One-Time Restores - Cove has two separate methods of recovering data on an on-demand basis:
  - To Hyper-V - This service runs to restore data to a Hyper-V or Local VHDX as configured in Add Recovery Locations
  - To Azure - This service runs to restore data to an Azure Virtual Machine as configured in Azure Recovery Locations
- Standby Image - Cove has three separate methods of running a continuous restore of your data:
  - Standby Image to Hyper-V - This service runs a continuous restore of a device to a Hyper-V or Local VHDX as configured in Add Recovery Locations
  - Standby Image to ESXi - This service runs a continuous restore of your data to ESXi
  - Standby Image to Azure - This service runs a continuous restore of your data to Microsoft Azure and boots based on the frequency set during configuration of the plan
- Recovery Testing - This service runs and provides a screenshot as proof that the device is recoverable

Benefit

With these tools, we provide proof of recoverability and the ability to failover in case of a disaster.

Requirements

The following requirements must be met:

- The following **must** be backed up:
  1. The full System State of the device
  2. The whole system disk – `C:\` or another disk that has your operating system and that the OS boots from (the **Files and Folders** data source)
- For setup, you must be logged into the Backup console as a **SuperUser** or **Manager**

  > To manage devices and recovery locations, any other user role will suffice.
- You are required to enter the devices encryption key/security code, however, in cases where the device has been installed using Quick Installation of the Backup Manager you will be required to provide the passphrase instead

Operating System

Recovery Testing and Standby Images are available on **Windows** operating systems only (servers and workstations):

- Windows 8 / 8.1
- Windows 10
- Windows 11
- Windows Server 2012 / 2012 R2 (limited[1])
- Windows Server 2016 (limited[2])
- Windows Server 2019 (limited[3])
- Windows Server 2022 (limited[4])

> Recovery Testing and Standby Image only support **64-bit** architecture.

One-Time Restores

Cove has two separate methods of recovering data on an on-demand basis:

- To Hyper-V - This service runs to restore data to a Hyper-V or Local VHDX as configured in Add Recovery Locations
- To Azure - This service runs to restore data to an Azure Virtual Machine as configured in Azure Recovery Locations

What's inside:

---

[1]New features such as Docker-based containers, Storage Spaces Direct and Shielded VMs are not.
[2]Only the features compatible with Windows Server 2012 R2 are supported.
[3]Only the features compatible with Windows Server 2012 R2 are supported.
[4]Only the features compatible with Windows Server 2012 R2 are supported.

One-Time Restore to Hyper-V

Cove Data Protection (Cove)'s **One-Time Restore** feature allows you to restore data to Hyper-V or Local VHDX as configured in Add Recovery Locations on an on-demand basis.

> It **is** possible to run one-time restores on devices assigned to either the Recovery Testing or Standby Image plans.

Requirements:

- Backup Manager version 17.4 and newer
- Devices and Recovery Locations must belong to the same Customer
- A Cove Data Protection (Cove) SuperUser or Manager account
- Recovery Locations must be added to the Management Console and the Recovery service must be installed on the recovery location **before** one-time restore can occur

> - Recovery Location is an environment where restores will be performed
> - Recovery service is a service which perform restores on that Recovery location

Limitations

- One-Time Restores cannot be used on the RMM integrated version of Backup (Managed Online Backup) or on the N-central integrated version of Backup (Backup and Recovery)
- One-Time Restores are **not** available for devices with disabled 'Virtual disaster recovery' feature in an assigned Product
- 32-bit architecture is not supported
- Due to a Microsoft limitation, Hyper-V **does not** support FAT/FAT32/ExFAT formatted drives. For this reason, please use NTFS formatted drives for Standby Image. More information can be found in the Microsoft Documentation for Hyper-V
- Maximum supported capacity for virtual hard disks is **64 TB** per disk
- Devices can only be assigned to **one** Recovery Location

What is restored?

The following data sources are supported and restored to the Hyper-V recovery location given that they are selected for backup in the Product, or data source selection:

- System State
- Files and Folders
- Exchange
- SharePoint
- MS SQL

What's inside:

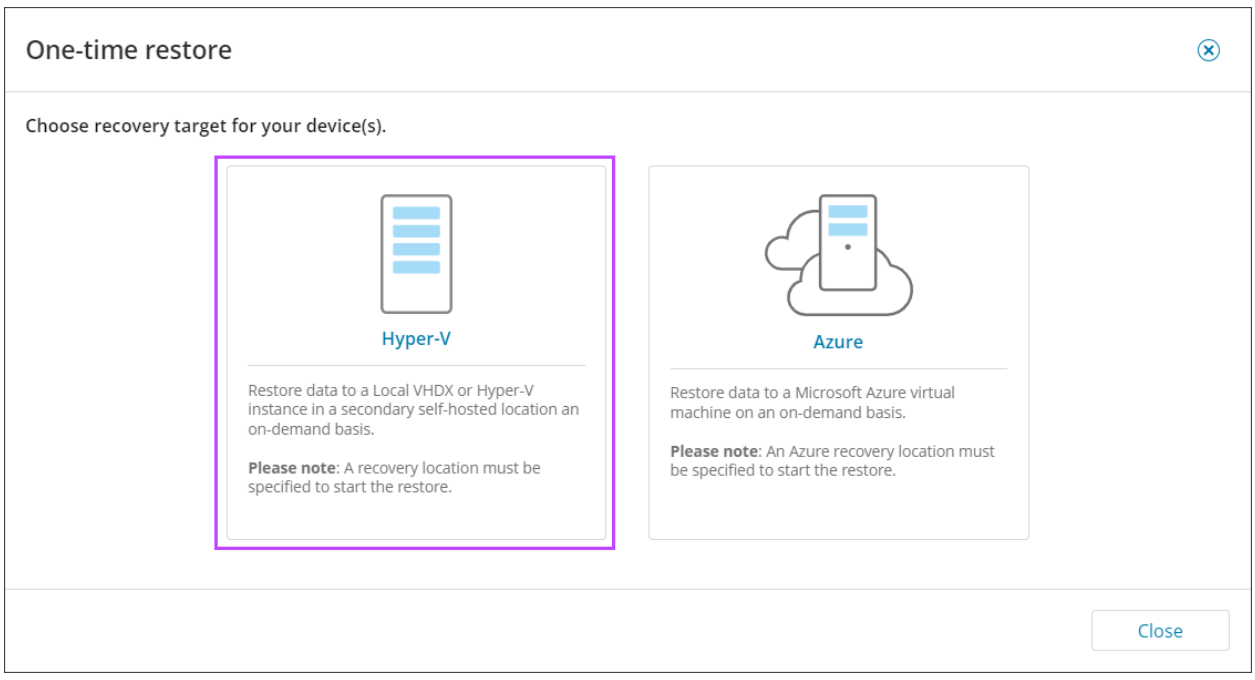
Configure One-Time Restore to Hyper-V

Before starting a One-Time Restore to Hyper-V, ensure you have checked all requirements and limitations, including setting up a Recovery Location.

From Backup Dashboard

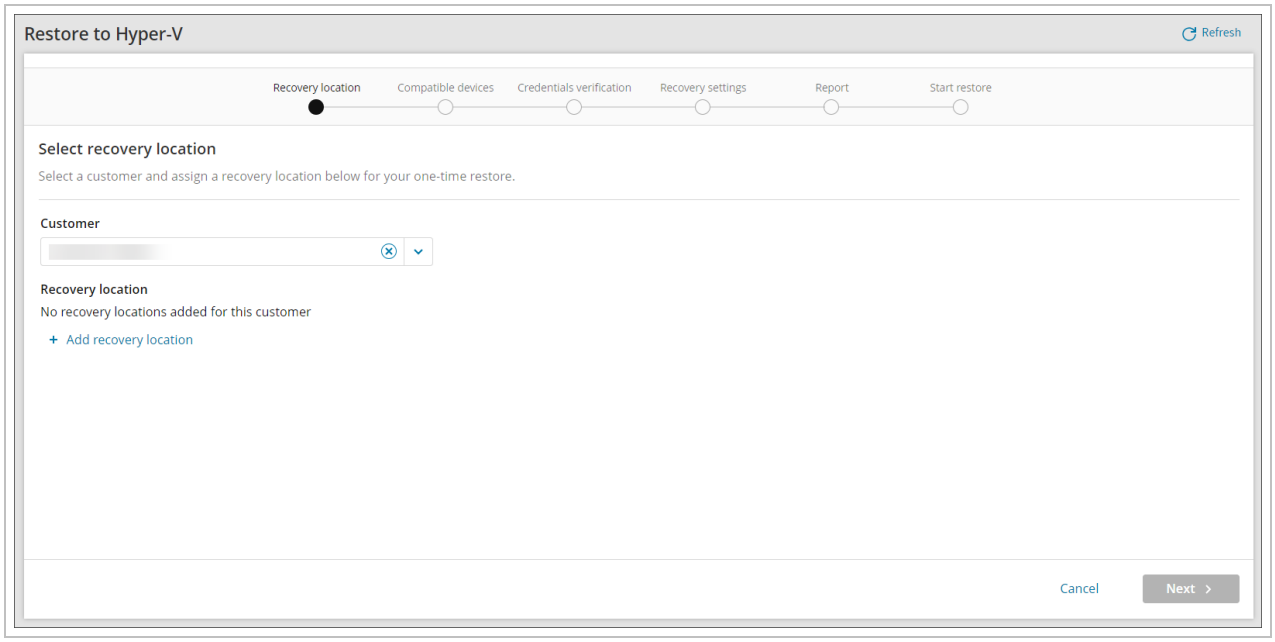
1. Log in to the Management Console under a **SuperUser** account
2. In the Backup Dashboard, tick the checkbox to the left of the device(s) to restore
3. Click **One-Time Restore**

4. Select the **Hyper-V** target

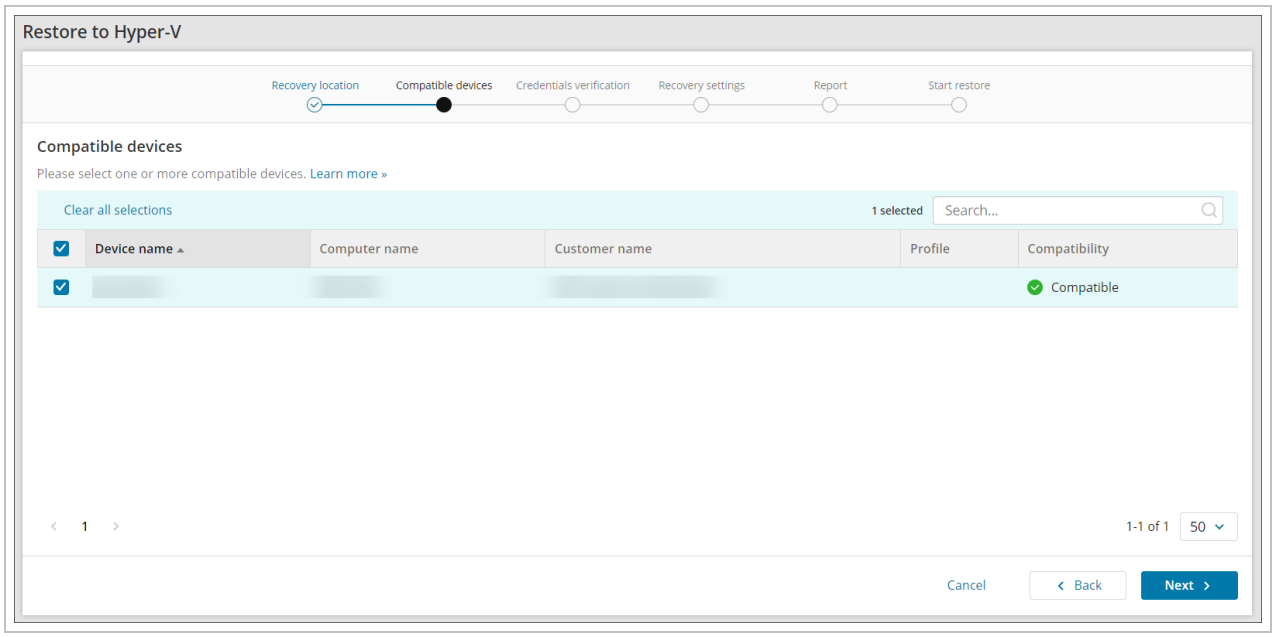


5. Select the Customer

6. Select the Recovery Location for the restore or click **+ Add recovery Location** to follow the steps to create a new Recovery Location



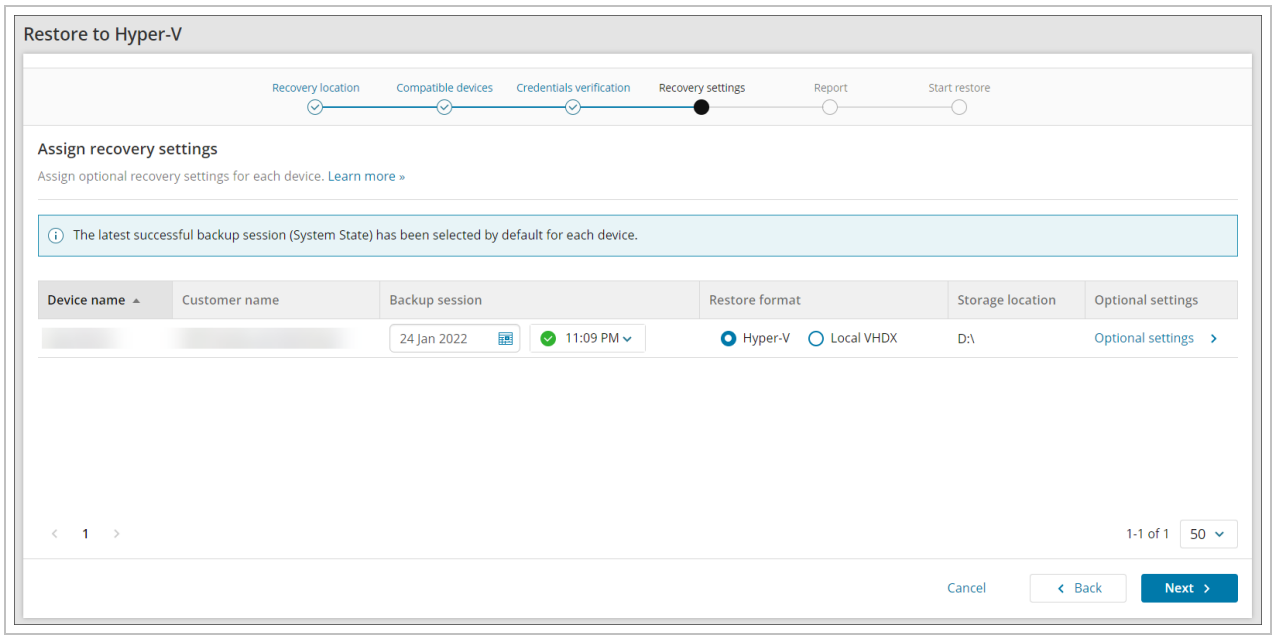
7. Click **Next**
8. Confirm compatibility of device(s) and click **Next**



9. Enter the security code/encryption key or passphrase for the device(s). This can be either:
   - **Private encryption key** - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryption
   - **Passphrase encryption** - These are generated on demand for automatically installed devices. You can find information on this here

> If you are logged in as a security officer, this will be detected automatically.

10. Click **Next**
11. Select the date and time of the backup session to restore

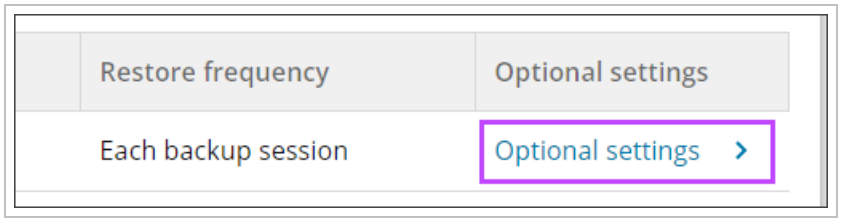


> During this step, **all** available sessions for **all devices** listed will be loaded in the backup session column. **Please allow time for these to load**, if the load of sessions fails, a message stating so will be displayed with a refresh button to try again.

> If the **Backup Target VM** option is enabled for one or more devices, be aware that if the backup agent is still running in backup mode on the source VM, this will lead to corrupted backup data for both the source and target VMs.

12. Choose the restore format:
    - Hyper-V
    - Local VHDX

13. Configure the **Optional Recovery Settings** for the restore format selected by clicking **Optional Settings** to the right of the storage location:



- Hyper-V optional settings:

OPTIONAL RECOVERY SETTINGS

Restore OS disk only

Backup target VM

FRS and DFSR services

Local Speed Vault

CPU cores

4

RAM (GB)

4

Virtual switch

default switch

Enter a virtual switch to enable network settings

VM Subnet mask

255.255.255.0

VM gateway

10.16.10.1

VM DNS server

10.16.10.5.8.8.8.8

Separate multiple DNS servers with a comma or semicolon

VM IP address

10.16.10.24

IP addresses will increment by 1, if applied to all devices

- **Restore OS disk only** - Restoring the OS disk only will speed up restores
- **Backup target VM** - Continuing to backup your target VM will protect the device according to its existing backup schedule
- **FRS and DFRS services** - If you are restoring Active Directory with multiple domain controllers, you should change the FRS and DFSR services to authoritative in the domain controller that will be started in the first place. Avoid marking several FRS/DFSR services as authoritative in the production environment as it can result in data loss. When the feature is on, the FRS and DFSR services are started on the target VM in the authoritative mode. The NETLOGON and SYSVOL shares become available, so the Active Directory and DNS services become functional again

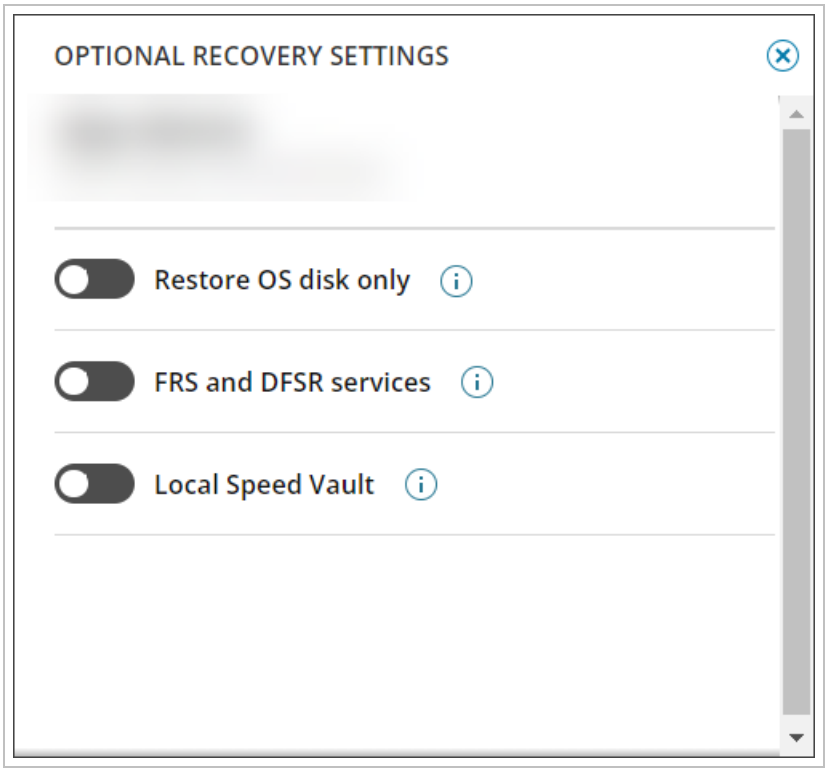
  > More information about FRS/DFSR is available in the Microsoft Knowledge Base. Article IDs: KB2218556 and KB290762

- **LocalSpeedVault** - If a LocalSpeedVault (LSV) is enabled on a backup device, the data is sent to both the LSV and the cloud or private storage location. During a restore, data is automatically downloaded from the LSV first to the local device which makes restore faster. If the LSV is not available or not synchronized, the restore data will be pulled from the cloud or private storage location. This takes place automatically and cannot be reconfigured
- **CPU Cores** - Select the number of CPU Cores to be allocated to the new virtual machine
- **RAM (GB)** - Select the amount of RAM in Gigabites to be allocated to the new virtual machine
- **Virtual switch** – Enter the Hyper-V network adapter that will be used by your new virtual machine
- **VM subnet mask** – Assign a custom subnet mask to the virtual machine
- **VM gateway** – Assign a custom gateway to the virtual machine
- **VM DNS servers** – Assign the list of custom DNS servers (separated by comma), Example:

  ```
  8.8.8.8 or 8.8.8.8,7.7.7.7
  ```

- **VM IP address** – Assign a custom IP address to the virtual machine

- Local VHDX optional settings:



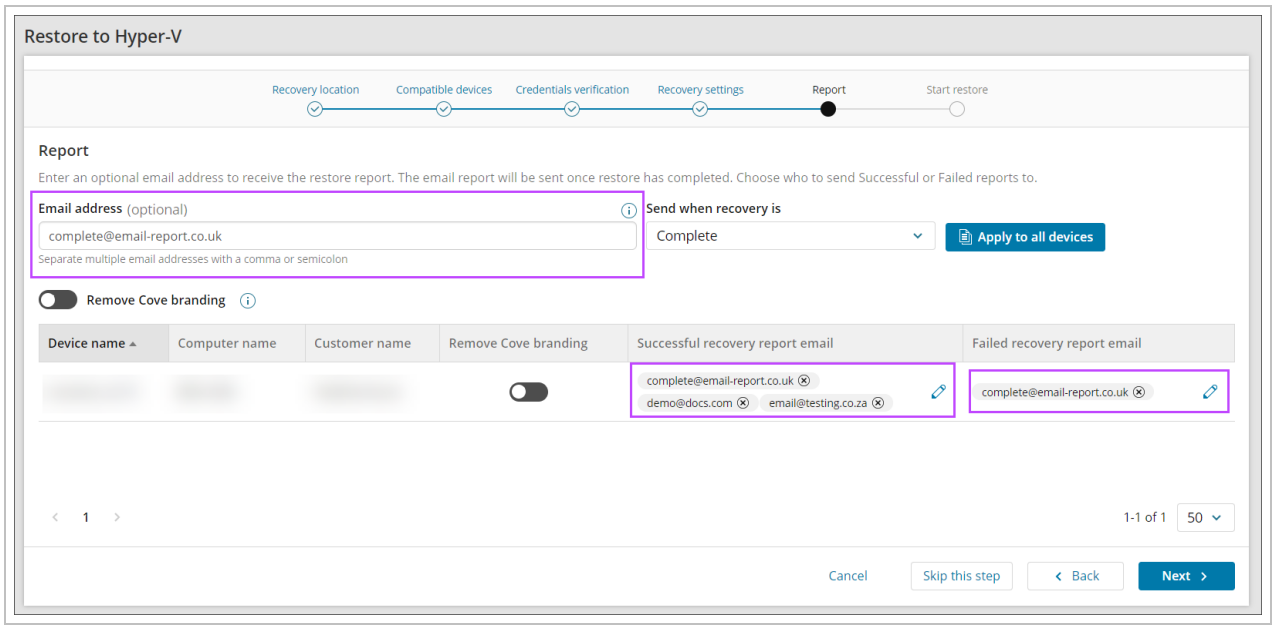
  - **Restore OS disk only** - Restoring the OS disk only will speed up restores
  - **FRS and DFRS services** - If you are restoring Active Directory with multiple domain controllers, you should change the FRS and DFSR services to authoritative in the domain controller that will be started in the first place. Avoid marking several FRS/DFSR services as authoritative in the production environment as it can result in data loss. When the feature is on, the FRS and DFSR services are started on the target VM in the authoritative mode. The NETLOGON and SYSVOL shares become available, so the Active Directory and DNS services become functional again

    > More information about FRS/DFSR is available in the Microsoft Knowledge Base. Article IDs: KB2218556 and KB290762

  - **LocalSpeedVault** - If a LocalSpeedVault (LSV) is enabled on a backup device, the data is sent to both the LSV and the cloud or private storage location. During a restore, data is automatically downloaded from the LSV first to the local device which makes restore faster. If the LSV is not available or not synchronized, the restore data will be pulled from the cloud or private storage location. This takes place automatically and cannot be reconfigured

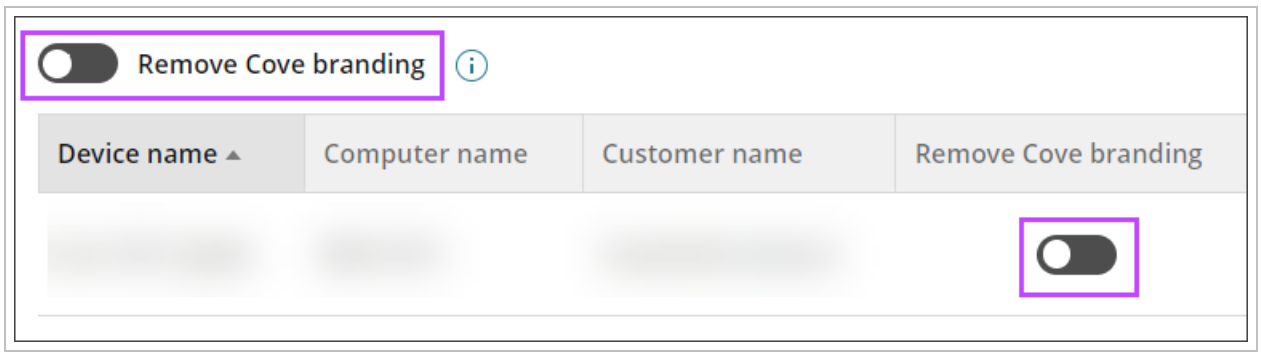
14. Click **Next** to progress to the **Report** window to enter one or more email addresses to receive a report when:
    a. The recovery is complete (Successful or Failed)
    b. The recovery was successful
    c. The recovery failed

> Multiple addresses should be separated using a comma or semi-colon



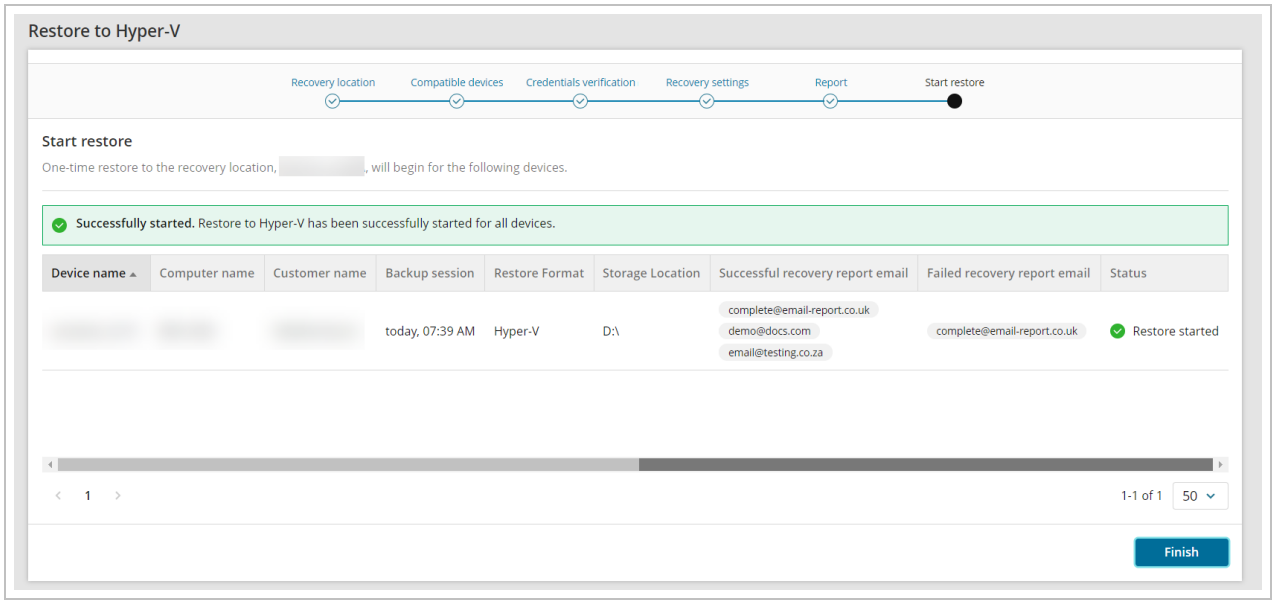
> If you do not want to add an email address to receive reports, click **Skip this step**

15. To remove all branding from the reports, use the **Remove Cove branding** toggle per device, or above the device list to apply the changes to all devices in this window



16. Confirm assigning the plan to the device(s)

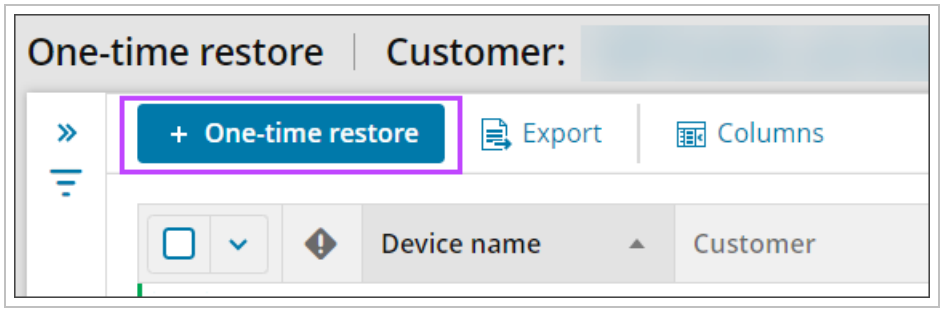
17. Wait for the plan to be assigned until you see a confirmation banner on the page



18. Click **Finish**

From One-Time Restore Overview

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to the **One-Time Restore** overview by selecting **Continuity** > **One-time Restore** from the vertical menu on the left hand side
3. Click **One-time restore** from the top bar



4. The wizard will open to target selection window, follow the above steps from Step #4 onwards

Recovery Reports

When the device(s) assigned to the plan have **Successful recovery report email** or **Failed recovery report email** recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox.

Here is an example report **with** Cove branding:

Cove Data Protection

Recovery completed

On demand restore to Hyper-V

Last recovery session completed successfully: April 05 2023 7:12:10 PM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Restore to Hyper-V dashboard.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Server
Operating system	Windows Server 2019 Standard Server (17763), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 05 2023 7:12:10 PM
Recovery status	Completed
Recovery duration	40 minutes and 58 seconds
Recovery location	

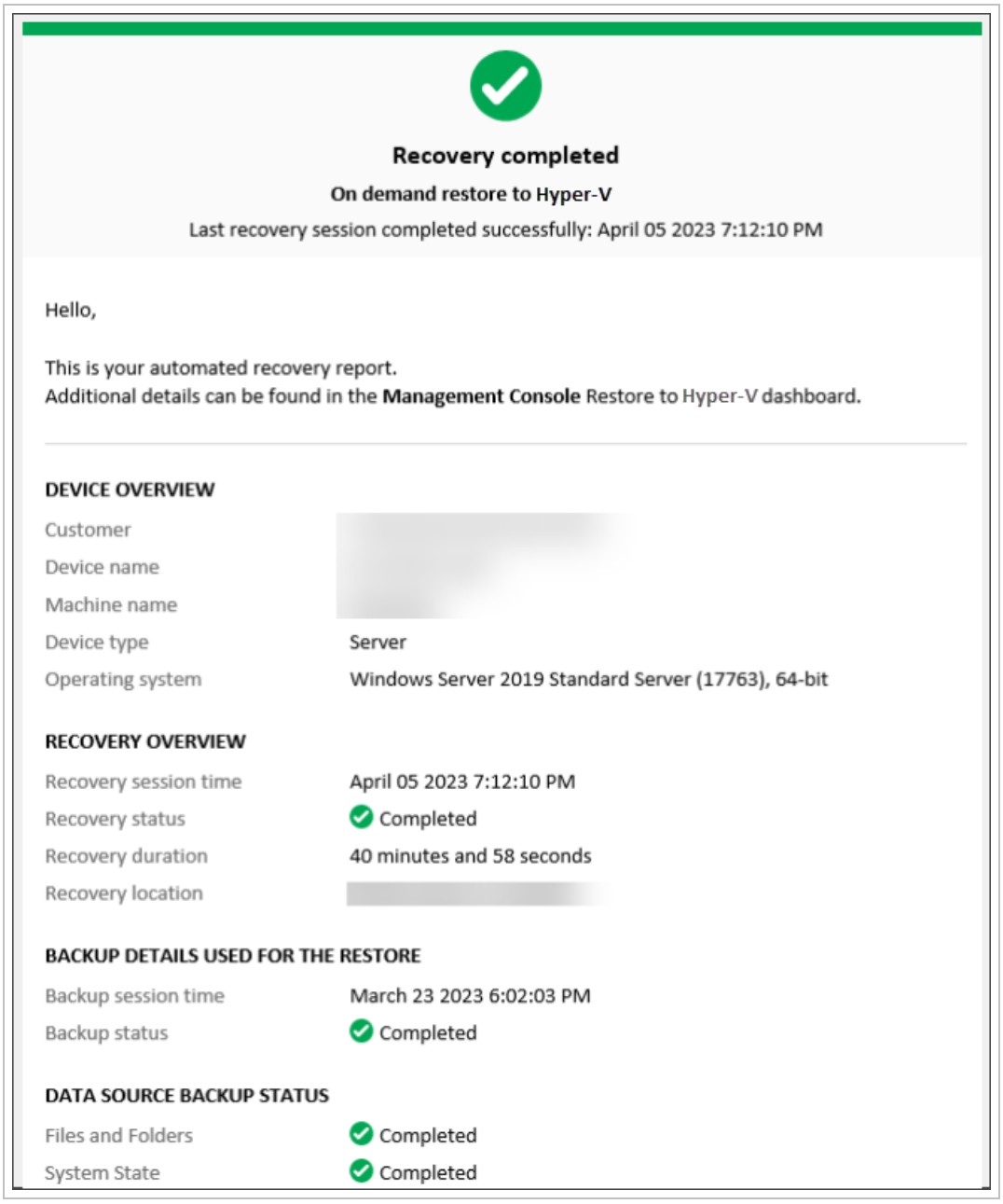
BACKUP DETAILS USED FOR THE RESTORE

Backup session time	March 23 2023 6:02:03 PM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

Here is an example **without** Cove branding:



Recovery completed

On demand restore to Hyper-V

Last recovery session completed successfully: April 05 2023 7:12:10 PM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Restore to Hyper-V dashboard.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Server
Operating system	Windows Server 2019 Standard Server (17763), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 05 2023 7:12:10 PM
Recovery status	Completed
Recovery duration	40 minutes and 58 seconds
Recovery location	

BACKUP DETAILS USED FOR THE RESTORE

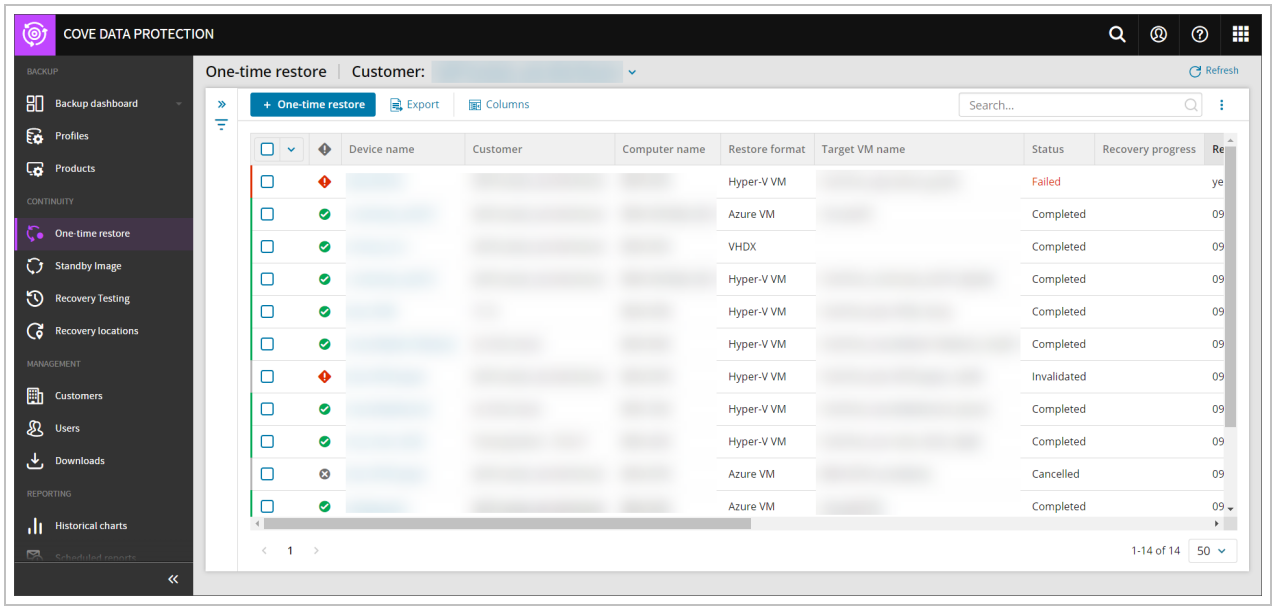
Backup session time	March 23 2023 6:02:03 PM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

Monitor Hyper-V Restore Progress

From the Management Console, you can view the dedicated One-Time Restore overview by selecting **Continuity** > **One-time Restore** from the vertical menu on the left hand side.



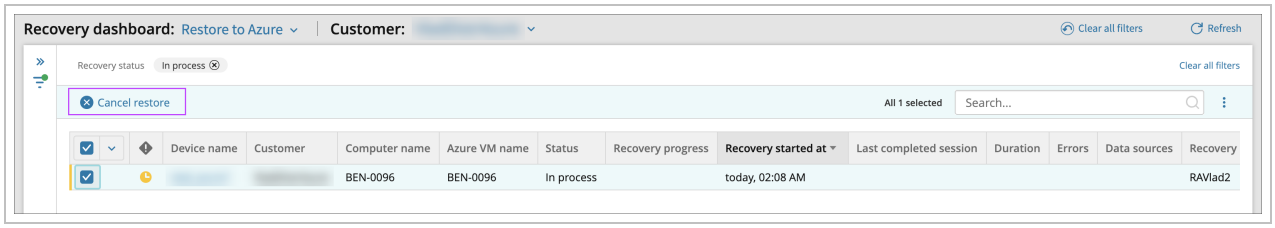
From this dashboard, you will see a specified set of columns detailing information relevant to devices using **One-time Restore**, including the status, restore format and data sources, along with other information relating to Azure and Hyper-V.

If no devices are active, the dashboard will display a message to advise.

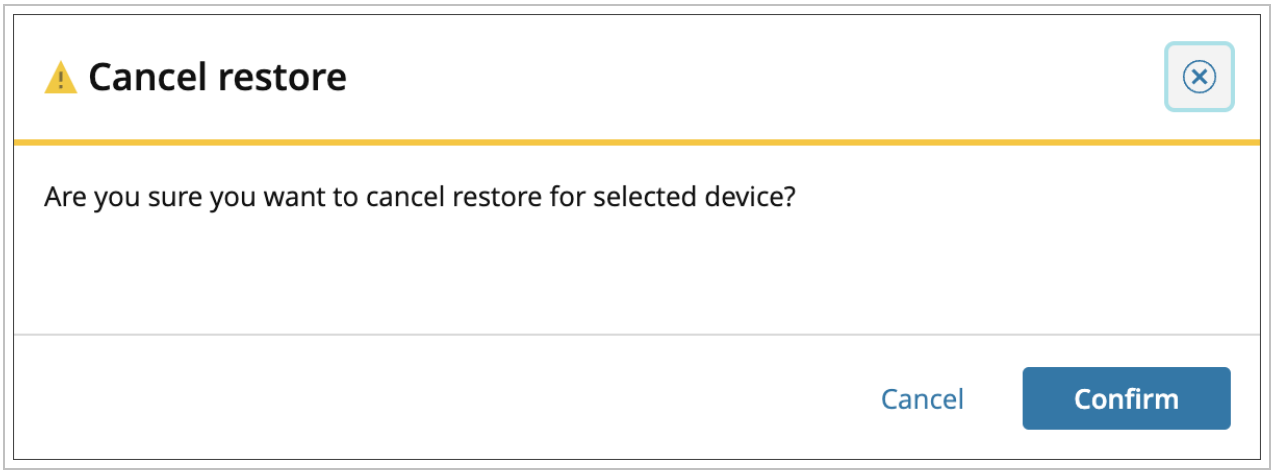
Cancel Restore

From the One-Time Restore overview, it is possible to cancel any recovery currently in progress:

1. Search for or use the filters to find the device in question where the recovery is currently running
2. Select the device
3. Click **Cancel restore** from the top bar



4. Confirm cancellation



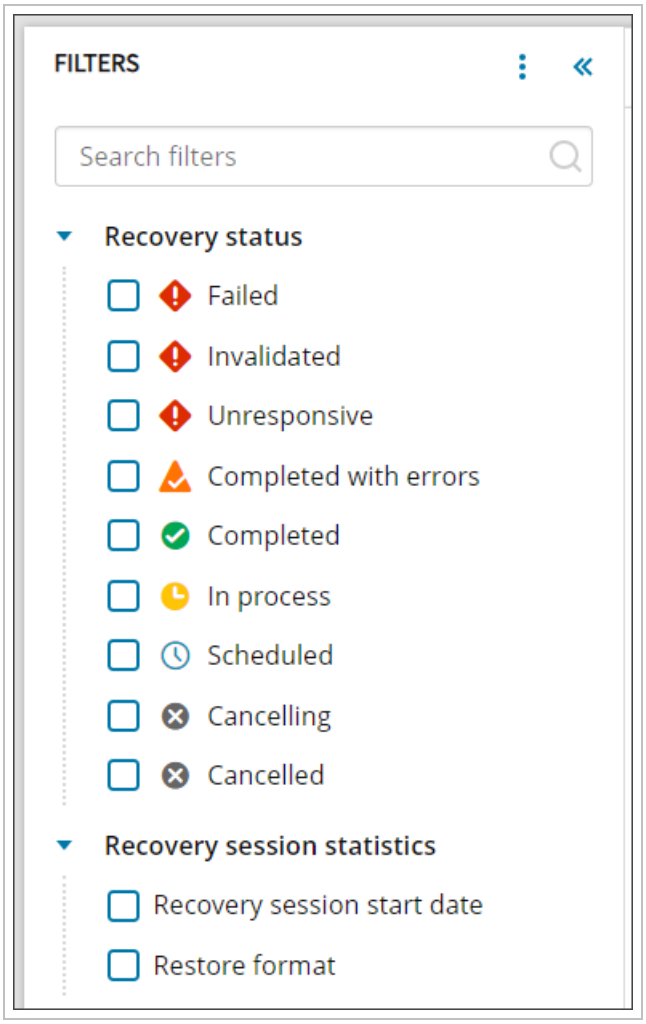
The device will now show in the list with a status of **Cancelled**

Searching

Searching within the One-Time Restore overview can be done by using the search box over to the right hand side of the page, just above the devices list. The search can be performed against any text field.

Filtering

The Standby Image overview also includes functionality to filter devices using the filter menu to the left of the device list and can be displayed or hidden by clicking the double arrows.



From this menu, you can filter by:

Recovery status

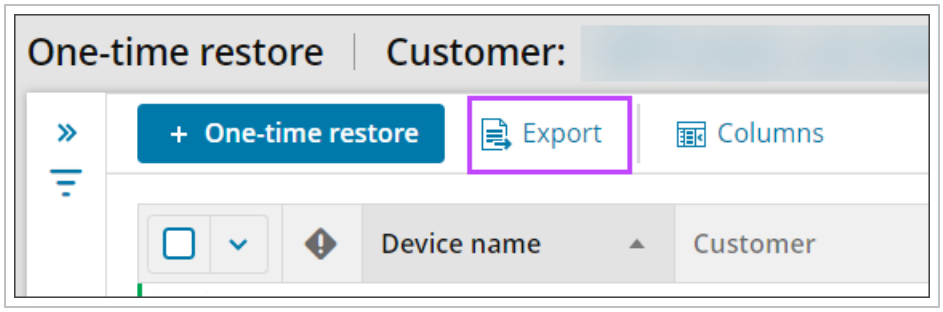
- **Failed** - The recovery session has failed
- **Invalidated** - Device was moved to an inappropriate partner and so the session has failed
- **Unresponsive** - The recovery session was initiated but did not receive updates for at least 30 minutes because the recovery location restarted or was offline.
- **Completed with errors** - The recovery session completed, but encountered errors
- **Completed** - The recovery session completed with no errors
- **In process** - The recovery is currently in progress
- **Scheduled** - Devices just added to a recovery plan and are waiting for their first recovery session or devices where restores were paused and have since been resumed will display as scheduled
- **Cancelling** - The recovery is in process of aborting
- **Cancelled** - The recovery has been cancelled

Recovery Session Statistics

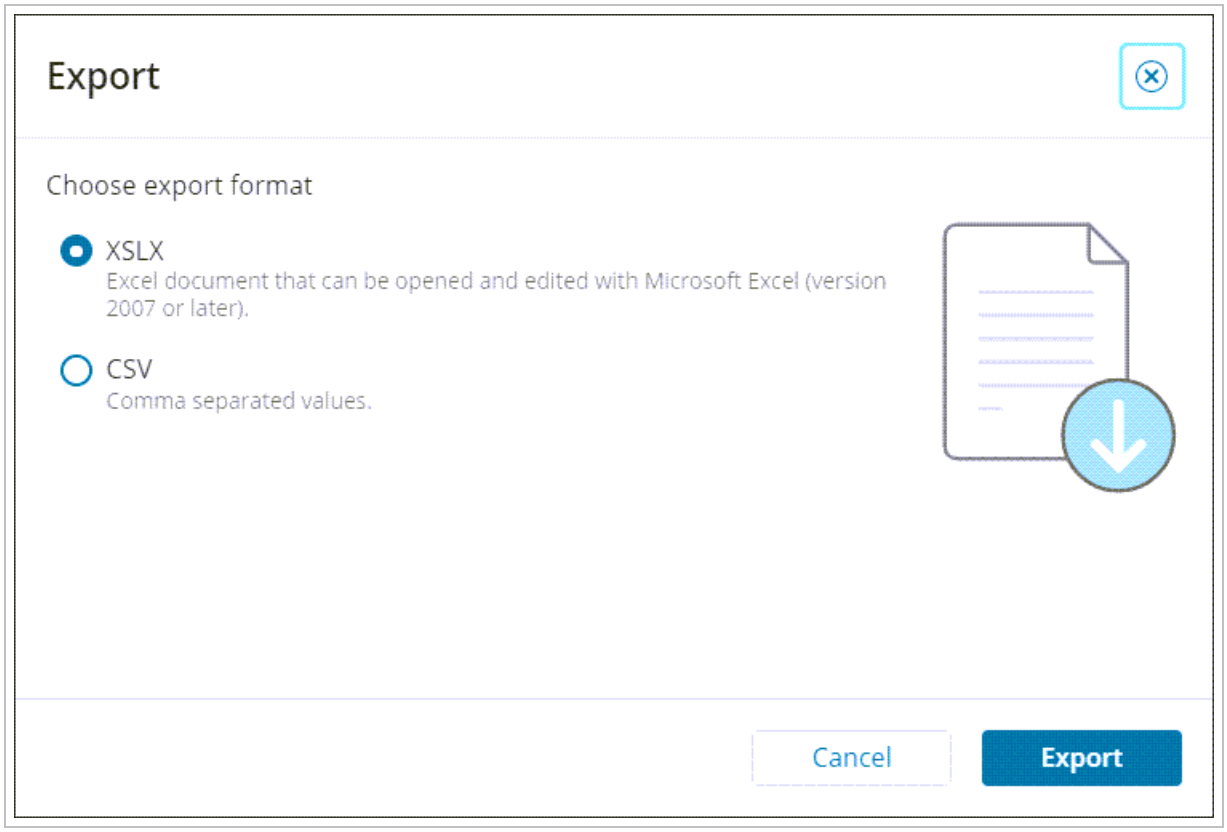
- Recovery session start date
- Restore format
  - Hyper-V VM
  - VHDX
  - Azure VM

Exporting

You may export a list of devices currently assigned a plan by clicking **Export**

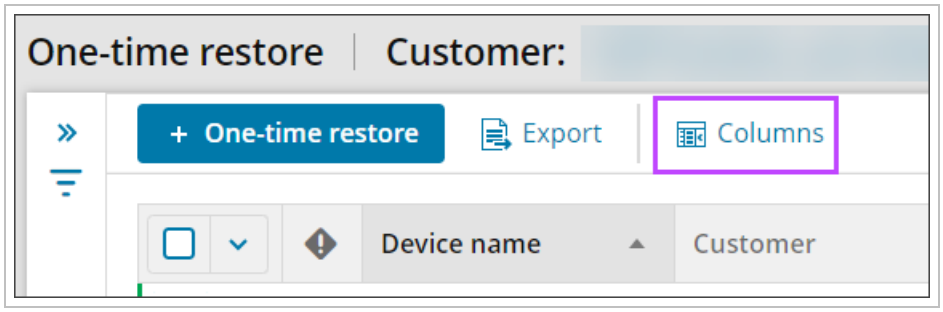


This will then provide a separate dialog where you can choose to export in either XSLX or CSV.

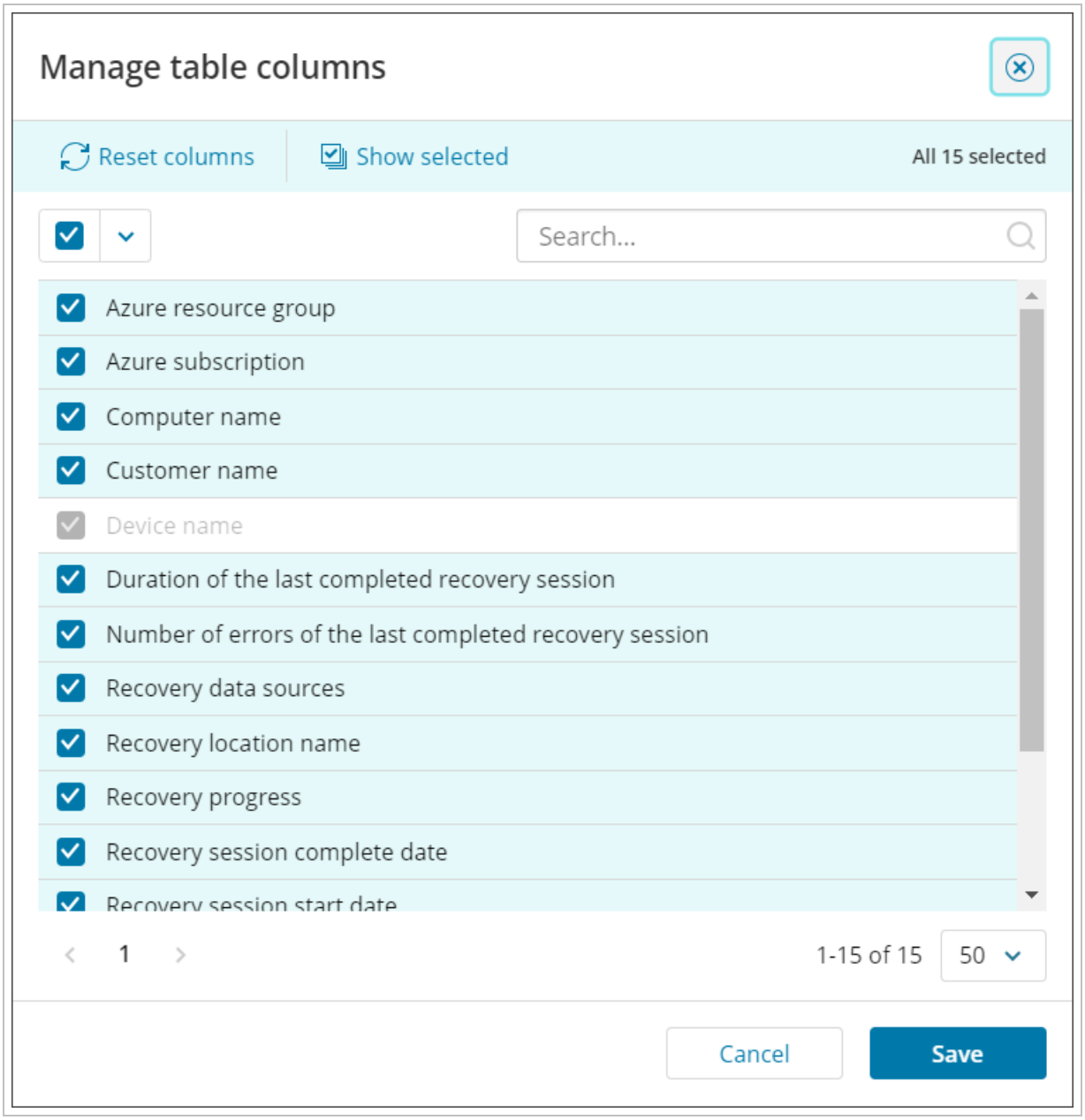


Manage Table Columns

Management Console allows you to manage the tables columns that can be seen within the One-Time Restore overview.



In the Manage table columns dialog, you can select and deselect columns based on the information you wish to view from the overview.



Accessing device properties

The Device Properties window displays several tabs detailing information on the Backup device. Full details of the contents of each tab can be found on the Device management in Management Console page.

This window can be accessed by clicking the **Device Name** from the One-Time Restore overview.

The two that are the most commonly used with One-Time Restore are the **Overview** tab and the **Settings** tab.

Remove Restore Record from Dashboard

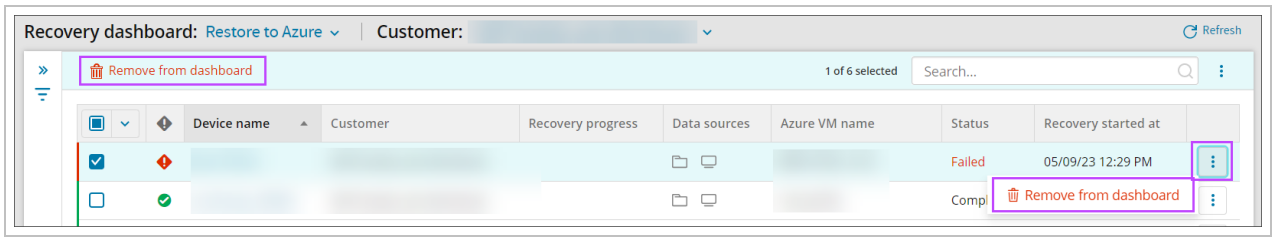
From the **One-Time Restore** overview, you may remove the record of a device's restore history.

This option is available for any restore status.

> This does **not** remove the device from any Standby Image plans or delete the device in Cove.

To remove a device's restore record:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity > One-Time Restore**
3. Using the search or filtering options, find the device(s) for which you need to delete the recovery record
4. Either:

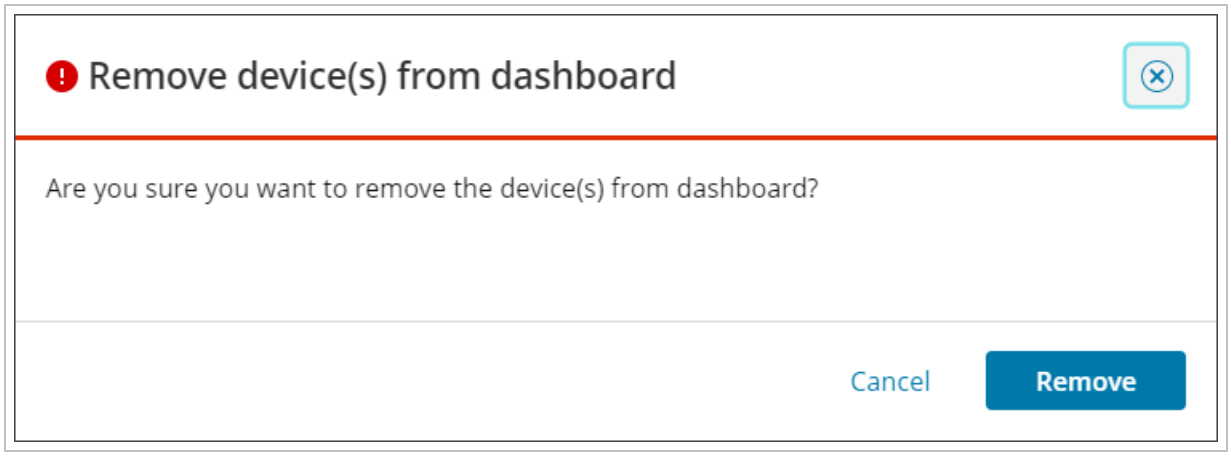


   a. Select the device(s) using the checkbox to the left of the Device Name and click **Remove from Dashboard** from the top bar

   or

   b. Using the action menu (three vertical dots) at the far right of the Device, select **Remove from Dashboard**

5. Confirm removal of the device's history



One-Time Restore to Azure

Cove Data Protection (Cove)'s **One-Time Restore** feature allows you to restore data to Microsoft Azure Virtual Machine as configured in Azure Recovery Locations on an on-demand basis.

Requirements

- An Azure Recovery Location
- Devices must be using Backup Manager version 17.4 or newer
- At minimum, you must have **Reader** role access to the subscription containing the Recovery Location VM
- An Application Administrator account for MS Azure or an account which has been granted permission to consent for apps
- A Cove Data Protection (Cove) SuperUser or Manager account
- The device to be restored must have `.NET Framework 4.0`

Limitations

- Available for Windows devices **only**
- **Files and Folders** and **System State** data sources must be included in the backup
- One-time restore is not available for devices where the 'Virtual disaster recovery' feature is disabled in an assigned Product
- 32-bit architecture is not supported
- Device should be In Agent Partner Tree
- Software-only devices are not supported
- Devices with operating system disks larger than **4TB** in size cannot be restored

What is restored?

The following data sources are supported and restored to the Azure recovery location given that they are selected for backup in the Product, or data source selection:

- Files and Folders
- System State
- MS SQL
- Exchange
- SharePoint

What's inside:

Configure One-Time Restore to Azure

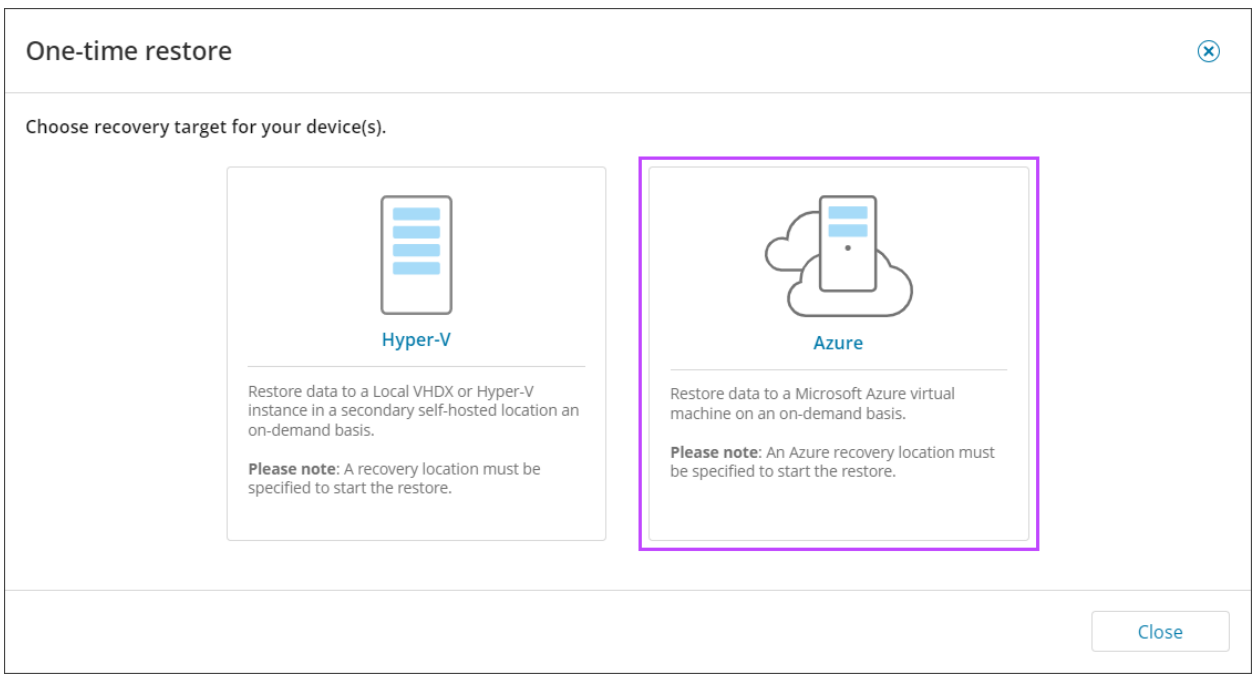
Before starting a One-Time Restore to Azure, ensure you have checked all requirements and limitations, including setting up an Azure recovery location.

From Backup Dashboard

1. Log in to the Management Console under a **SuperUser** account
2. In the Backup Dashboard, tick the checkbox to the left of the device(s) to restore

3. Click **One-Time Restore**

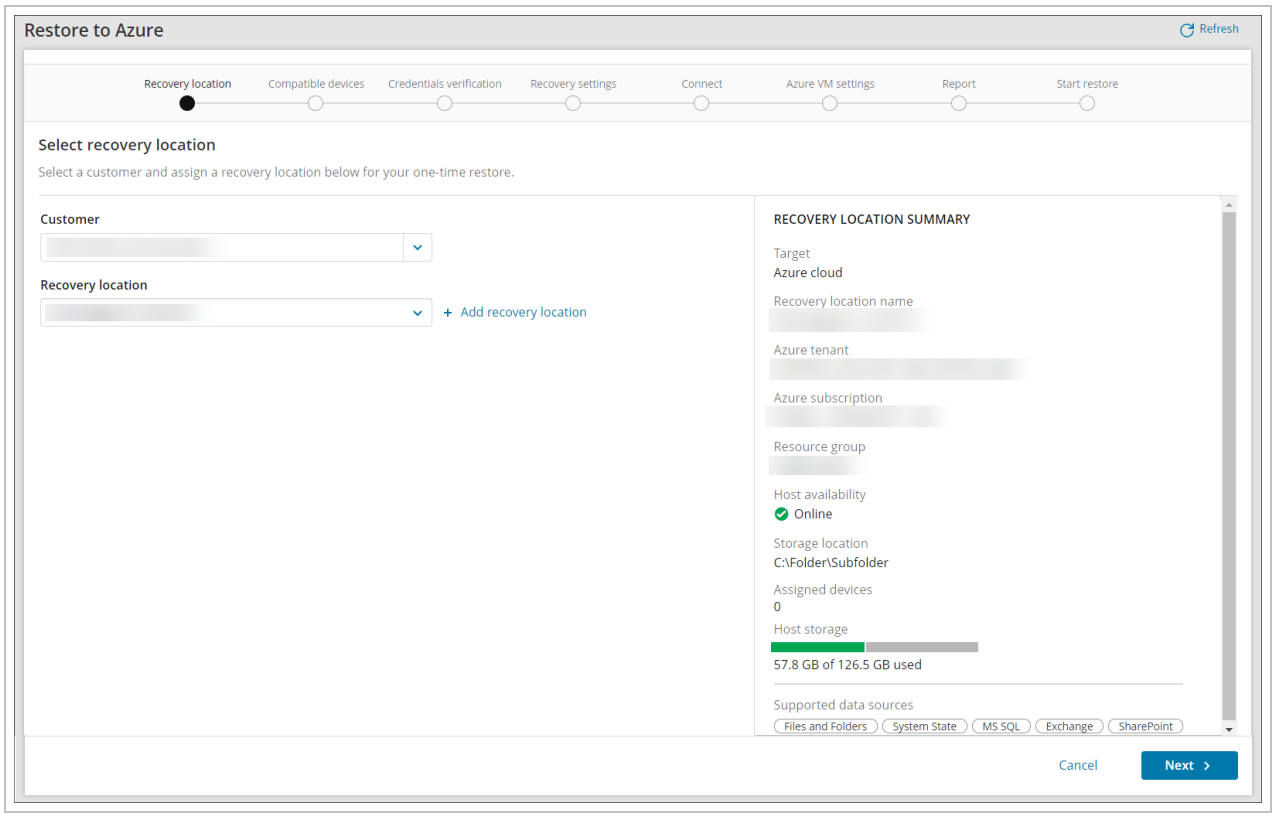
4. Select the **Azure** target



5. Select the Customer

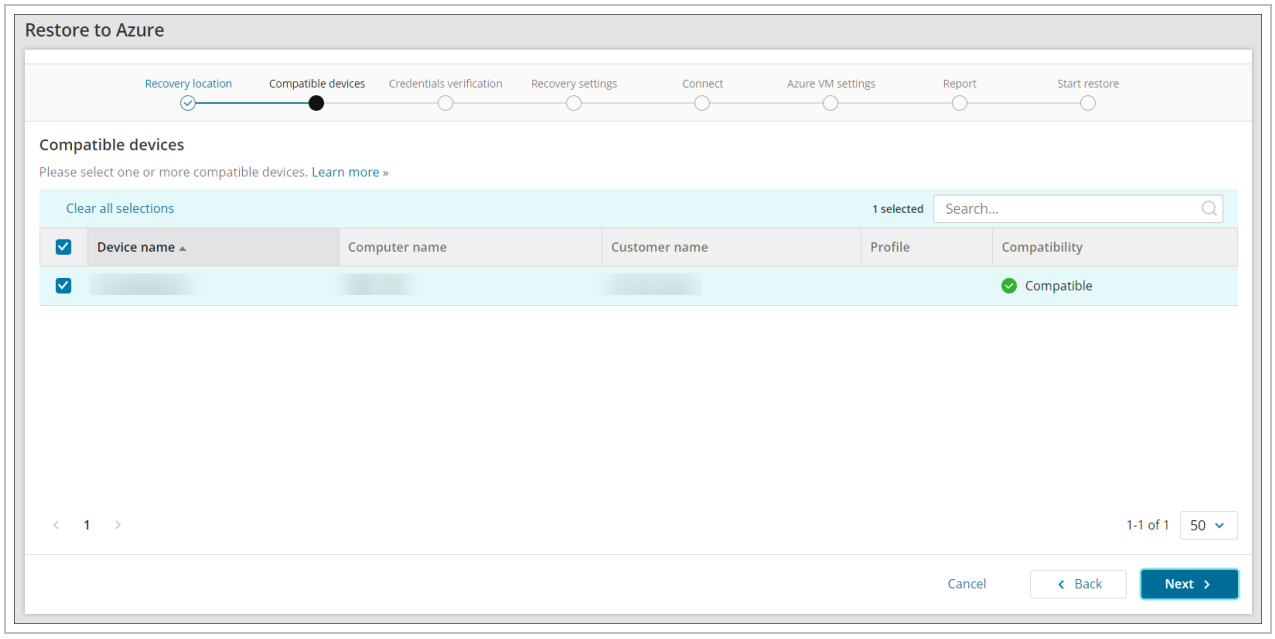
6. Select the Azure Recovery Location for the restore or click **+ Add recovery Location** to follow the steps to create a new Azure Recovery Location

> If adding a recovery location from here, you will be taken to the **Add Azure Recovery Location** wizard, where **Azure** will be automatically selected as the recovery type. Follow the Azure Recovery Location installation instructions from Step #4 onwards.



7. Click **Next**

8. Confirm compatibility of device(s) and click **Next**

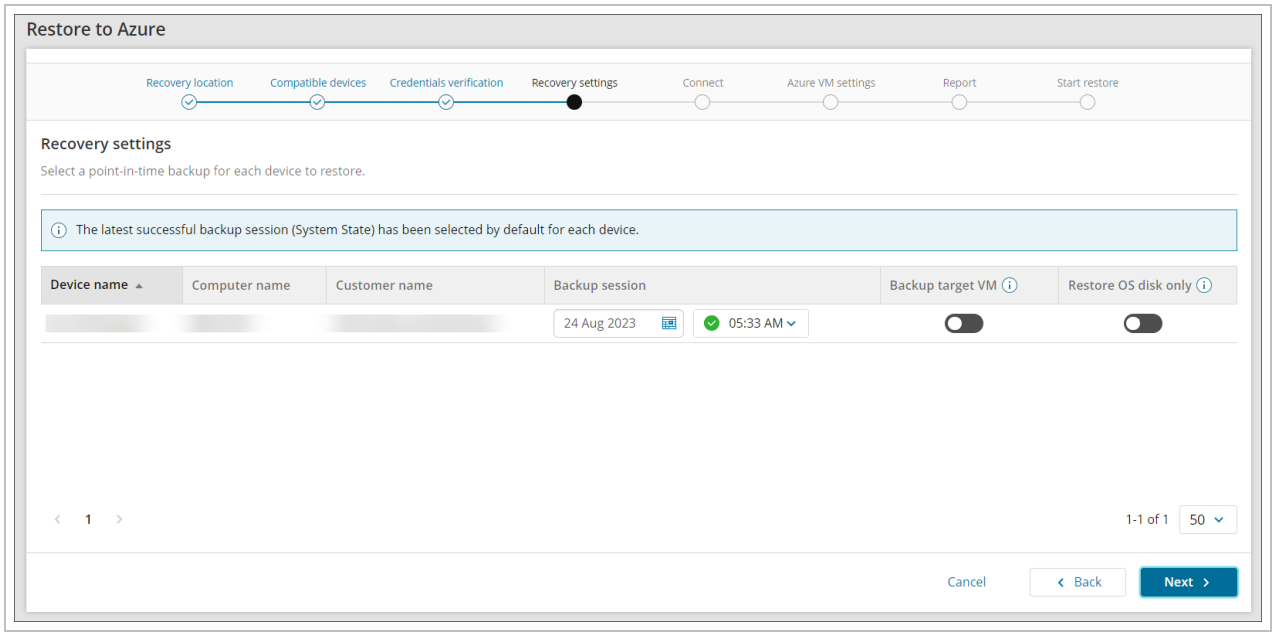


9. Enter the security code/encryption key or passphrase for the device(s). This can be either:
   - **Private encryption key** - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryption
   - **Passphrase encryption** - These are generated on demand for automatically installed devices. You can find information on this here

> If you are logged in as a security officer, this will be detected automatically.

10. Click **Next**

11. Select the date and time of the backup session to restore



> During this step, **all** available sessions for **all devices** listed will be loaded in the backup session column. **Please allow time for these to load**, if the load of sessions fails, a message stating so will be displayed with a refresh button to try again.

12. If you wish to protect the device according to its existing backup schedule, enable **Backup target VM**

> If the **Backup Target VM** option is enabled for one or more devices, be aware that if the backup agent is still running in backup mode on the source VM, this will lead to corrupted backup data for both the source and target VMs.

13. If you wish to skip all data drives, enable **Restore OS disk only**

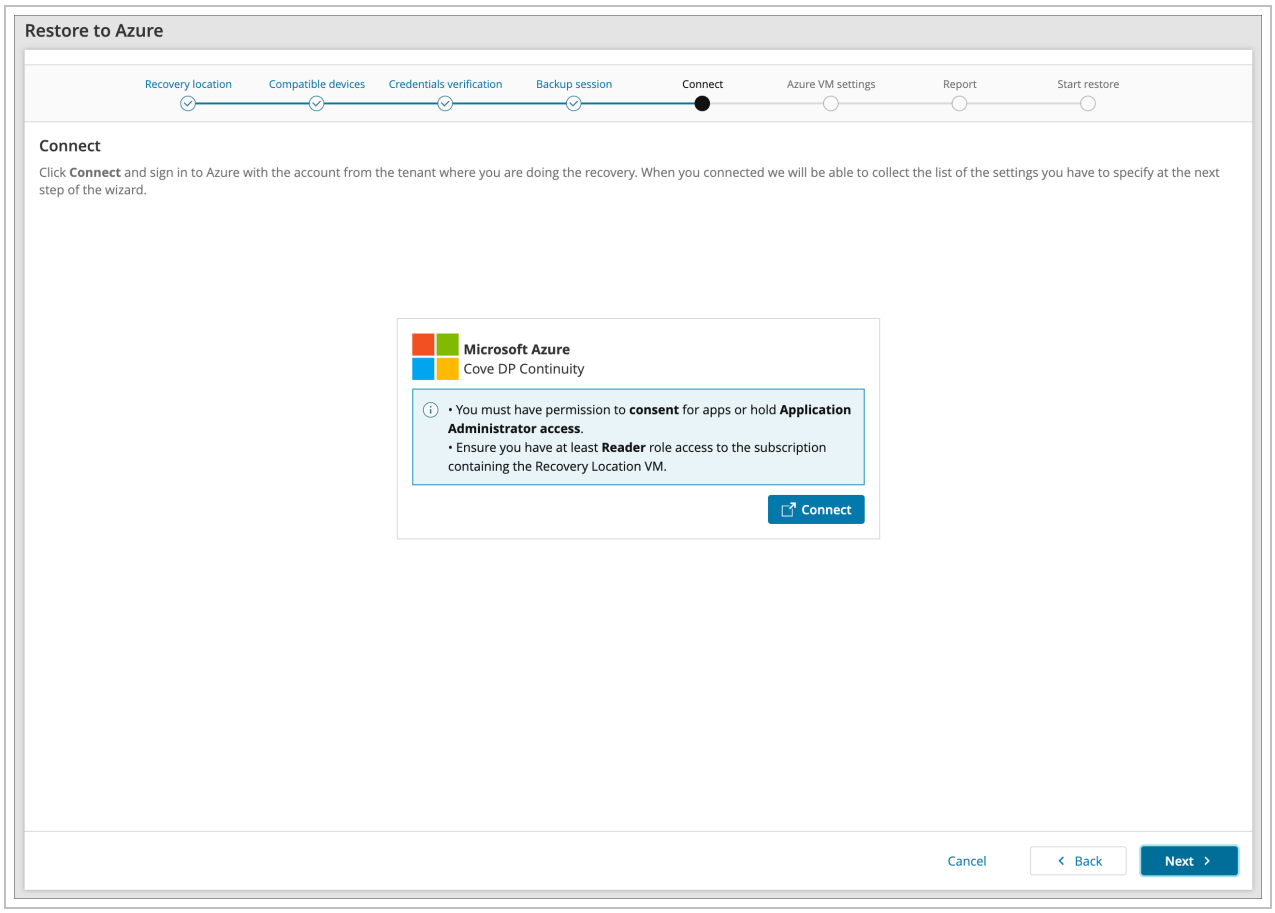
> Enabling **Restore OS disk only** will help to speed up restores as the only thing being restored is the Operating System

14. Click **Next**

15. Connect to Microsoft Azure by either:
    a. Allow permissions to the Azure user account to **consent for apps** access,

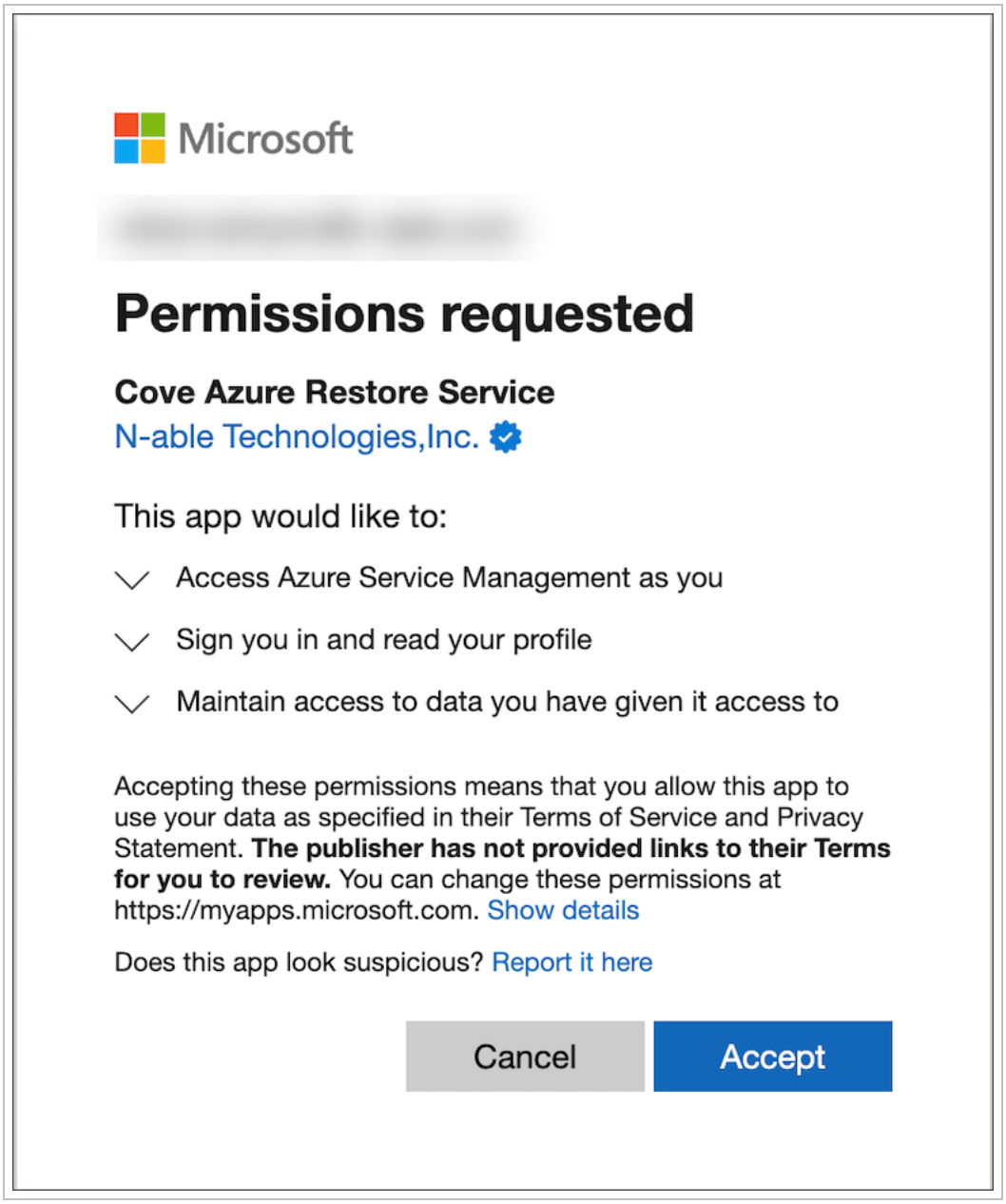
or;

    a. Login using Application Administrator access



> Ensure you have at minimum **Reader** role access to the subscription containing the Recovery Location VM

b. Accept the required permissions



If you do not see the authentication page, make sure your browser is not blocking pop-up windows.

16. Supply the **Azure VM settings**:

AZURE VM SETTINGS

Subscription

Resource group

Virtual machine name

BEN-0079

Region

West Europe

Availability options

VM size

OS disk type

Premium SSD

Data disk(s) type

Premium SSD

Virtual network

Subnet

default

Stop target VM after recovery

Assign NSG and public IP

- Subscription

  > This cannot be changed as the subscription is set in the **Recovery Location** configuration

- Resource Group
- Virtual Machine name
- Region

  > This cannot be changed as the subscription is set in the **Recovery Location** configuration

- Availability options
- VM size

  > If the **VM size** selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either **increase** the **regional vCPU quota** on the Subscription, or **decrease** the **VM size** selected in the Azure VM Settings.

- OS disk type

  > Set to **Premium SSD** to speed up the Azure restore. This can be changed in Azure later

- Data disk(s) type

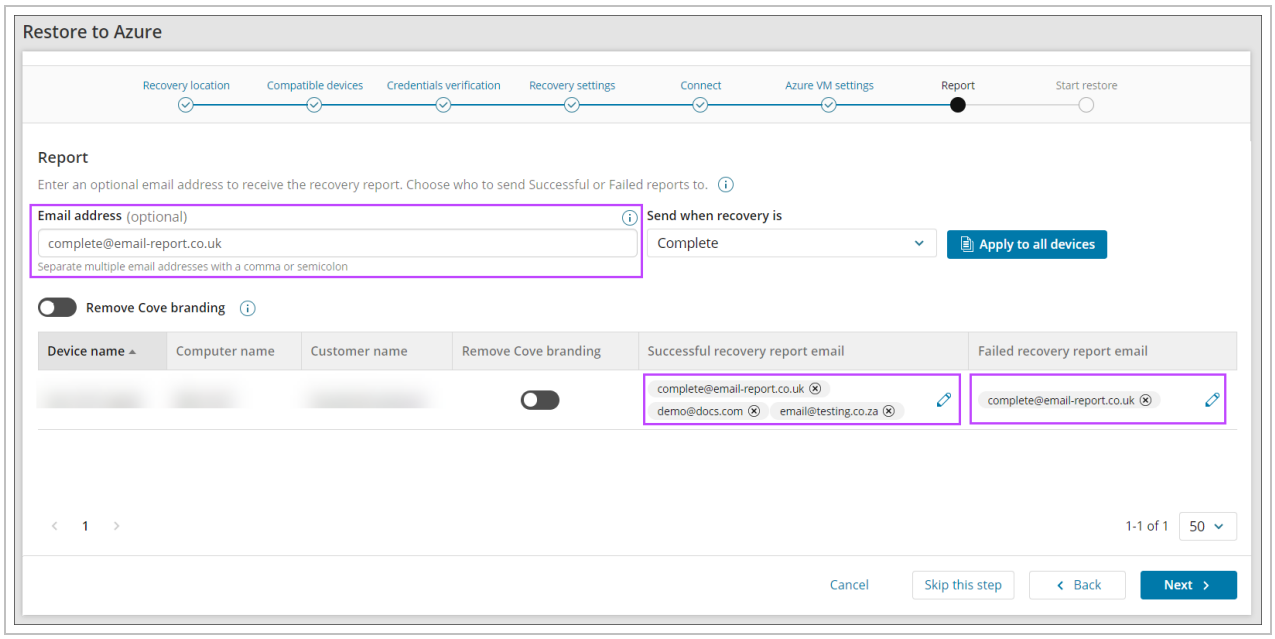
  > Set to **Premium SSD** to speed up the Azure restore. This can be changed in Azure later

- Virtual Network
- Subnet
- Stop target VM after recovery
- Assign NSG and public IP

17. Click **Next**

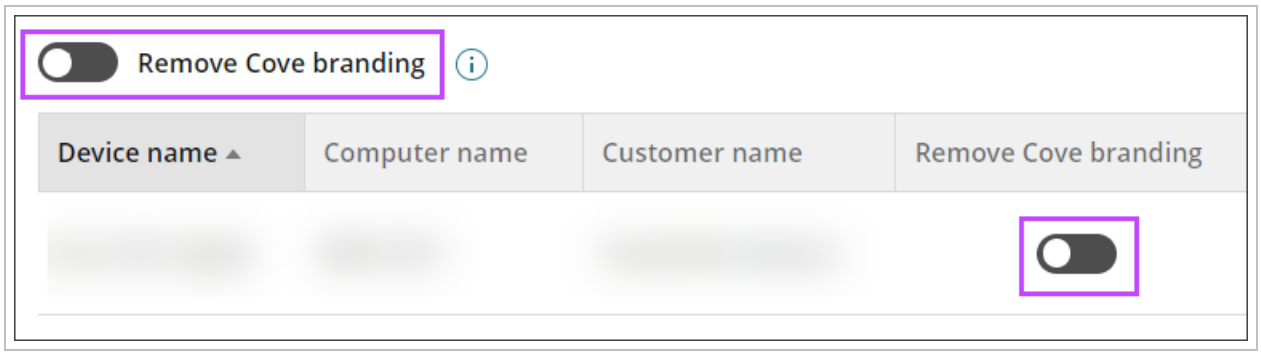
18. Click **Next** to progress to the **Report** window to enter one or more email addresses to receive a report when:
    a. The recovery is complete (Successful or Failed)
    b. The recovery was successful
    c. The recovery failed

> Multiple addresses should be separated using a comma or semi-colon



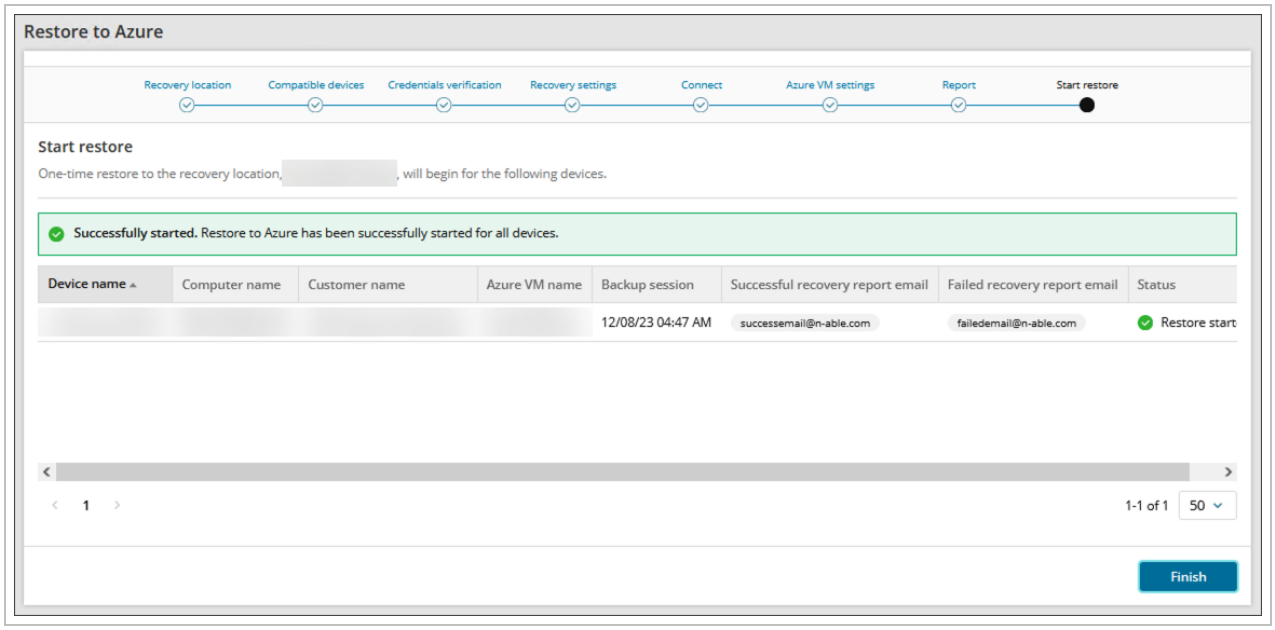
> If you do not want to add an email address to receive reports, click **Skip this step**

19. To remove all branding from the reports, use the **Remove Cove branding** toggle per device, or above the device list to apply the changes to all devices in this window



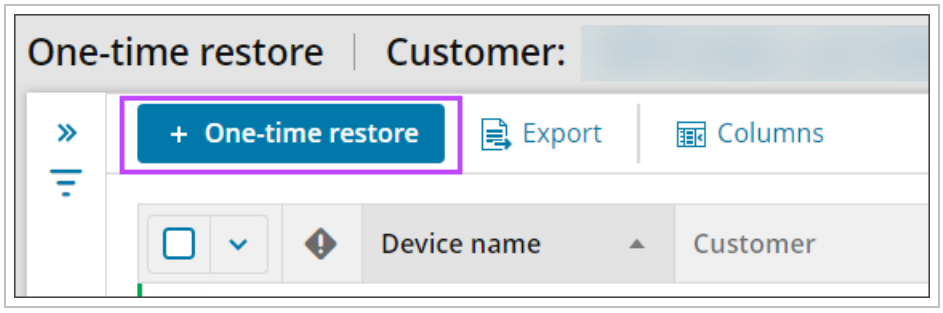
20. Review and confirm the restore details for each device and click **Confirm**

21. Once the restore has been started, a green banner will be displayed and a notification in the top right-hand corner of the screen to confirm. Click **Finish** to close the restore wizard and return to the Dashboard



From One-Time Restore Overview

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to the **One-Time Restore** overview by selecting **Continuity** > **One-time Restore** from the vertical menu on the left hand side
3. Click **One-time restore** from the top bar



4. The wizard will open to target selection window, follow the above steps from Step #4 onwards

Recovery Reports

When the device(s) assigned to the plan have **Successful recovery report email** or **Failed recovery report email** recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox.

Here is an example report **with** Cove branding:

Cove Data Protection

Recovery completed

On demand restore to Microsoft Azure

Last recovery session completed successfully: April 05 2023 7:12:10 PM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Restore to Azure dashboard.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Server
Operating system	Windows Server 2019 Standard Server (17763), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 05 2023 7:12:10 PM
Recovery status	Completed
Recovery duration	40 minutes and 58 seconds
Recovery location	

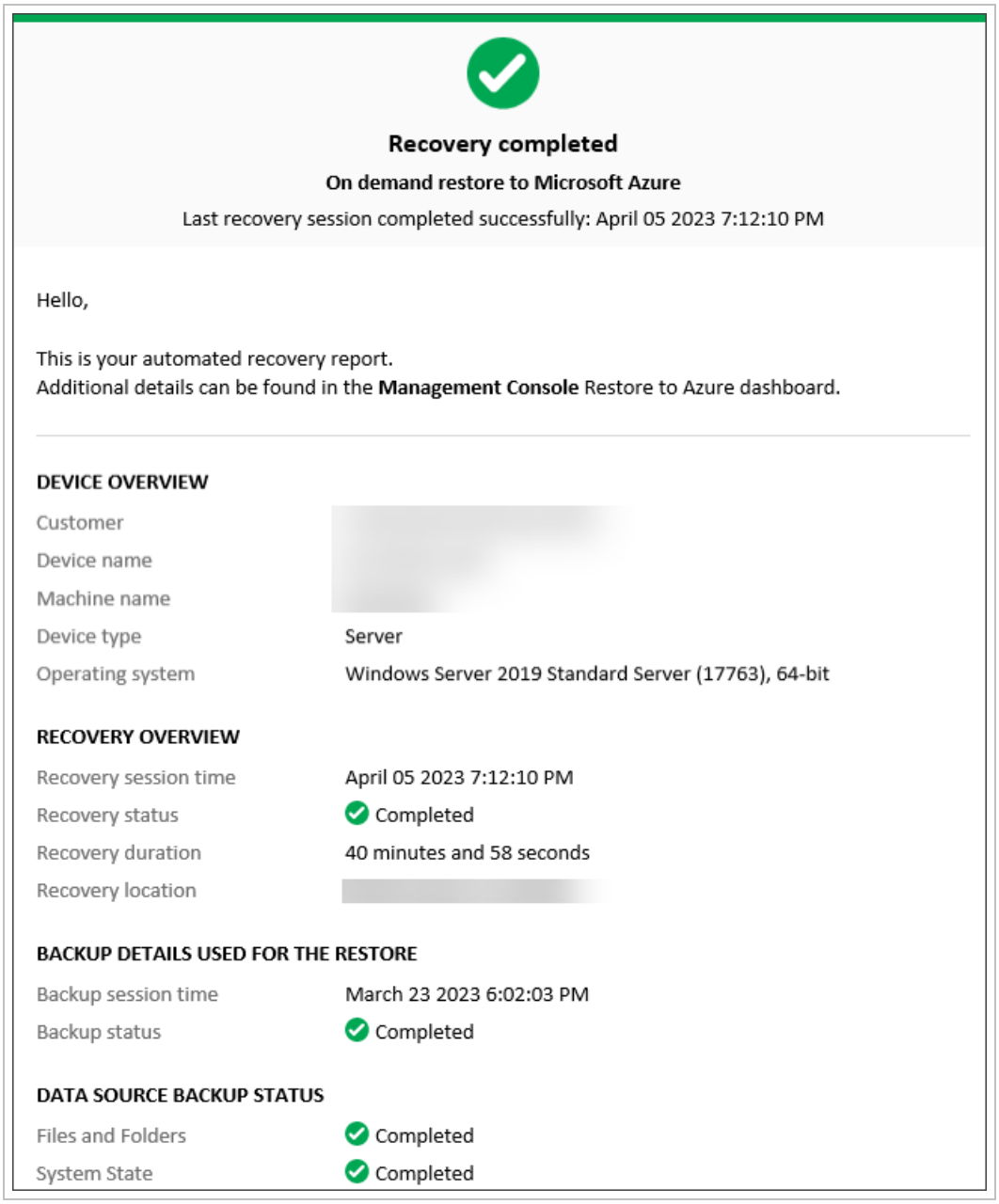
BACKUP DETAILS USED FOR THE RESTORE

Backup session time	March 23 2023 6:02:03 PM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

Here is an example **without** Cove branding:



Recovery completed

On demand restore to Microsoft Azure

Last recovery session completed successfully: April 05 2023 7:12:10 PM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Restore to Azure dashboard.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Server
Operating system	Windows Server 2019 Standard Server (17763), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 05 2023 7:12:10 PM
Recovery status	Completed
Recovery duration	40 minutes and 58 seconds
Recovery location	

BACKUP DETAILS USED FOR THE RESTORE

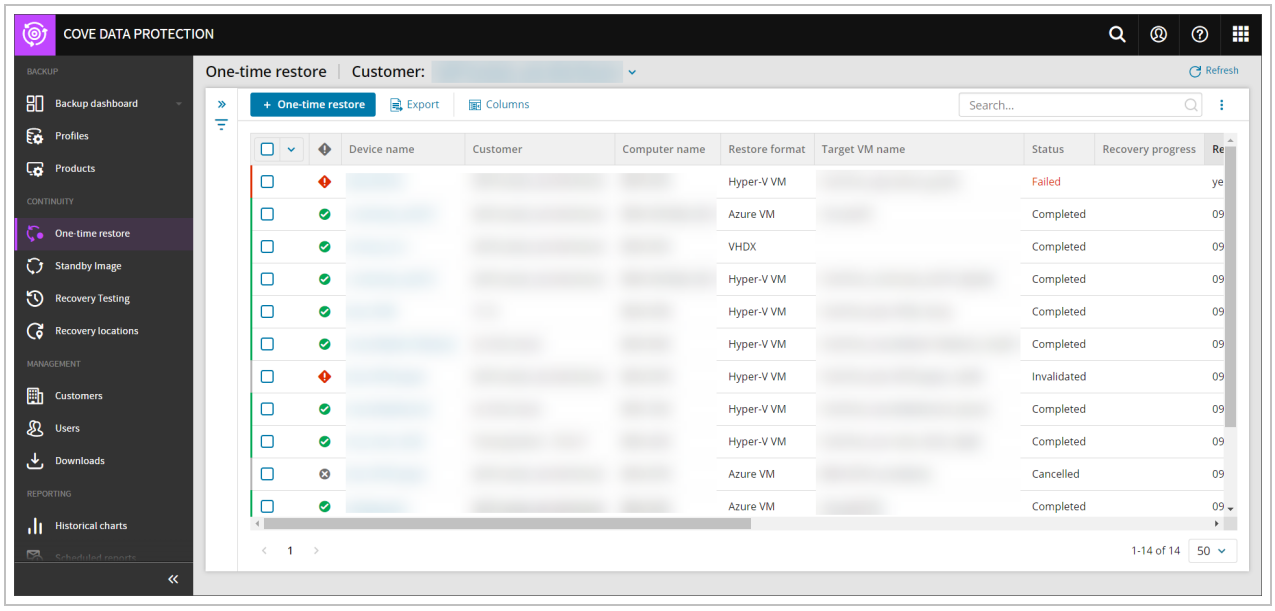
Backup session time	March 23 2023 6:02:03 PM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

Monitor Azure Restore Progress

From the Management Console, you can view the dedicated One-Time Restore overview by selecting **Continuity** > **One-time Restore** from the vertical menu on the left hand side.



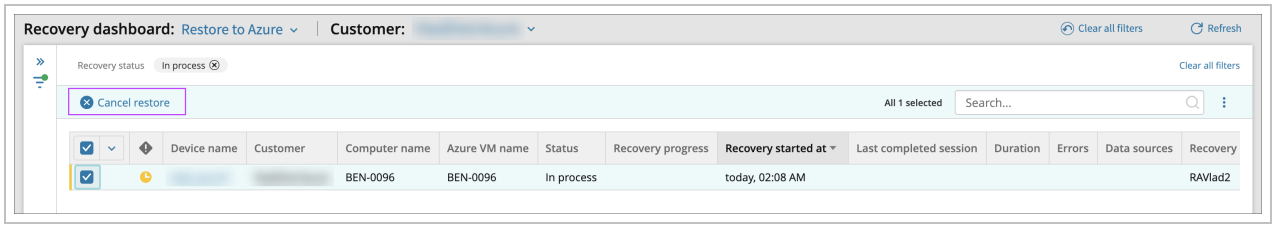
From this dashboard, you will see a specified set of columns detailing information relevant to devices using **One-time Restore**, including the status, restore format and data sources, along with other information relating to Azure and Hyper-V.

If no devices are active, the dashboard will display a message to advise.

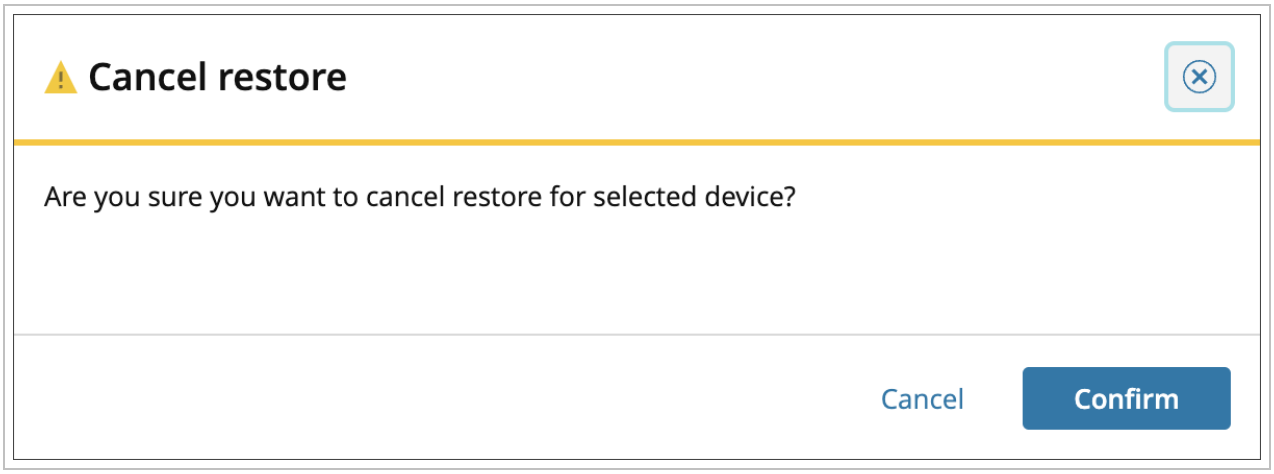
Cancel Restore

From the One-Time Restore overview, it is possible to cancel any recovery currently in progress:

1. Search for or use the filters to find the device in question where the recovery is currently running
2. Select the device
3. Click **Cancel restore** from the top bar



4. Confirm cancellation



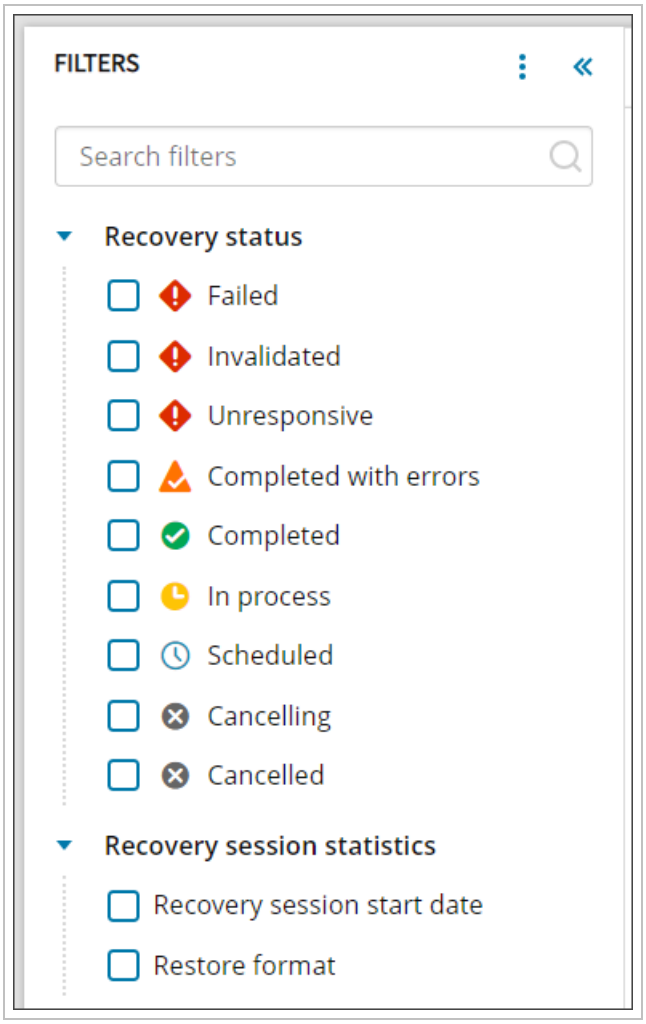
The device will now show in the list with a status of **Cancelled**

Searching

Searching within the One-Time Restore overview can be done by using the search box over to the right hand side of the page, just above the devices list. The search can be performed against any text field.

Filtering

The Standby Image overview also includes functionality to filter devices using the filter menu to the left of the device list and can be displayed or hidden by clicking the double arrows.



From this menu, you can filter by:

Recovery status

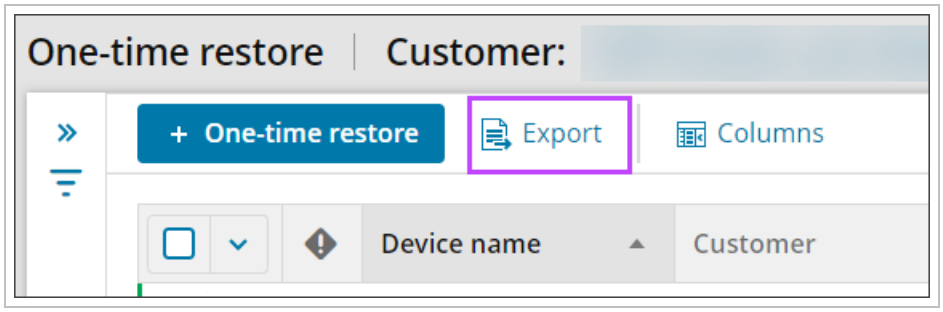
- **Failed** - The recovery session has failed
- **Invalidated** - Device was moved to an inappropriate partner and so the session has failed
- **Unresponsive** - The recovery session was initiated but did not receive updates for at least 30 minutes because the recovery location restarted or was offline.
- **Completed with errors** - The recovery session completed, but encountered errors
- **Completed** - The recovery session completed with no errors
- **In process** - The recovery is currently in progress
- **Scheduled** - Devices just added to a recovery plan and are waiting for their first recovery session or devices where restores were paused and have since been resumed will display as scheduled
- **Cancelling** - The recovery is in process of aborting
- **Cancelled** - The recovery has been cancelled

Recovery Session Statistics

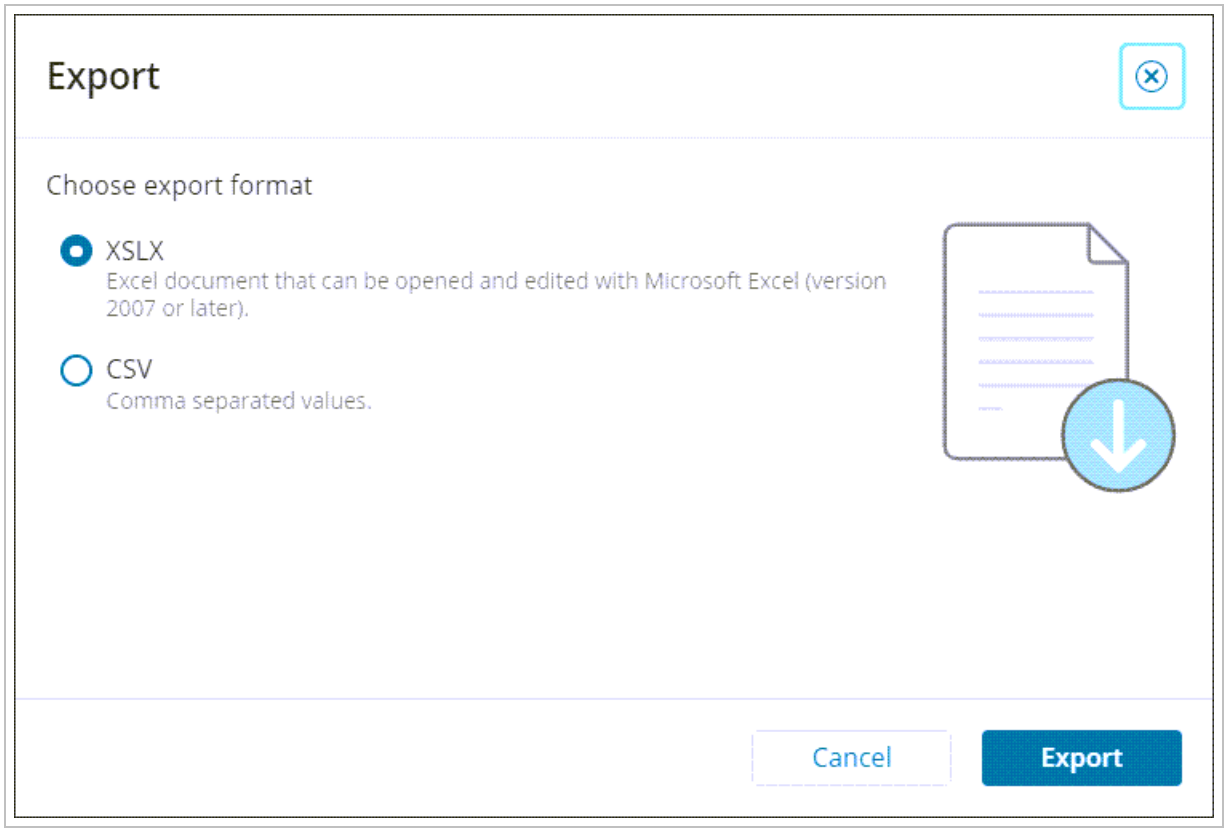
- Recovery session start date
- Restore format
  - Hyper-V VM
  - VHDX
  - Azure VM

Exporting

You may export a list of devices currently assigned a plan by clicking **Export**

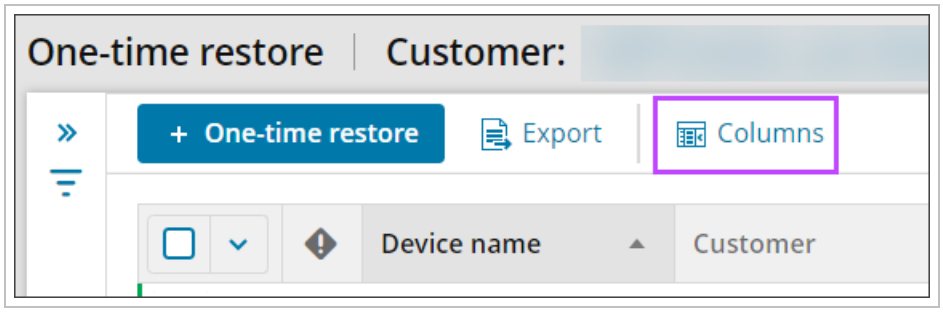


This will then provide a separate dialog where you can choose to export in either XSLX or CSV.

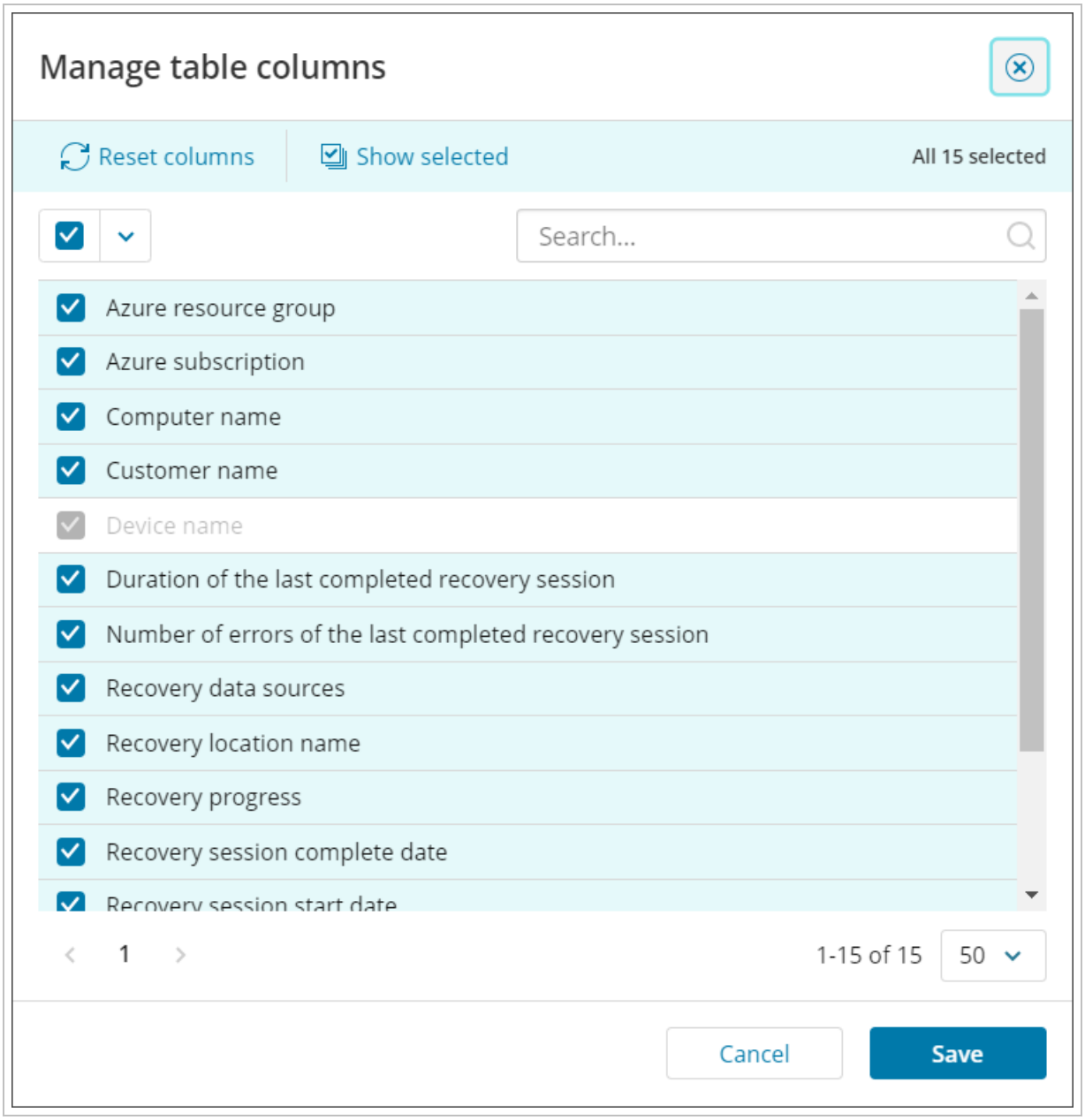


Manage Table Columns

Management Console allows you to manage the tables columns that can be seen within the One-Time Restore overview.



In the Manage table columns dialog, you can select and deselect columns based on the information you wish to view from the overview.



Accessing device properties

The Device Properties window displays several tabs detailing information on the Backup device. Full details of the contents of each tab can be found on the Device management in Management Console page.

This window can be accessed by clicking the **Device Name** from the One-Time Restore overview.

The two that are the most commonly used with One-Time Restore are the **Overview** tab and the **Settings** tab.

Remove Restore Record from Dashboard

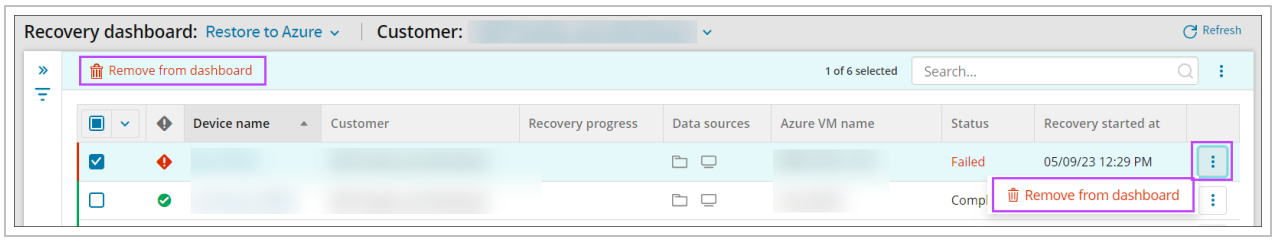
From the **One-Time Restore** overview, you may remove the record of a device's restore history.

This option is available for any restore status.

> This does **not** remove the device from any Standby Image plans or delete the device in Cove.

To remove a device's restore record:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity > One-Time Restore**
3. Using the search or filtering options, find the device(s) for which you need to delete the recovery record
4. Either:

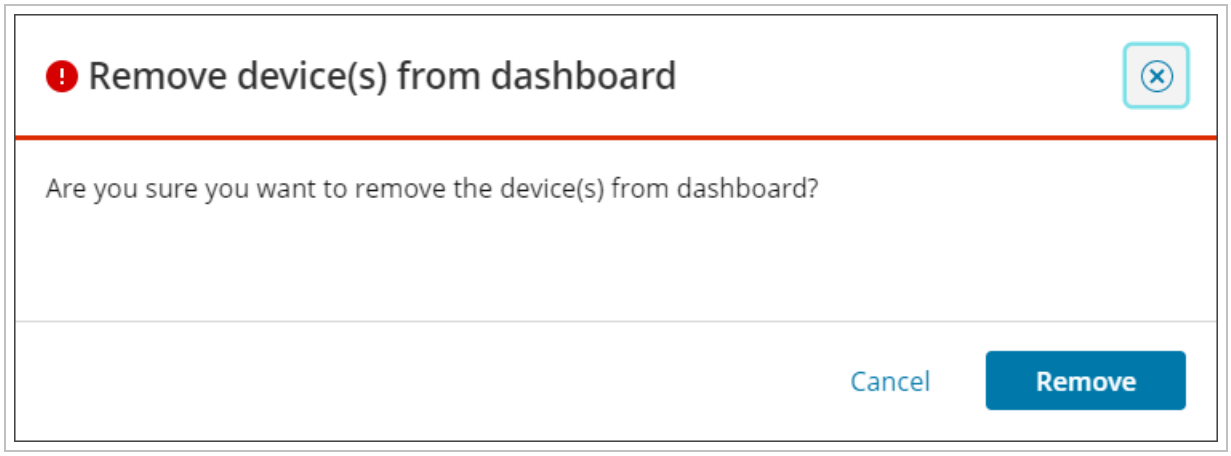


   a. Select the device(s) using the checkbox to the left of the Device Name and click **Remove from Dashboard** from the top bar

   or

   b. Using the action menu (three vertical dots) at the far right of the Device, select **Remove from Dashboard**

5. Confirm removal of the device's history



Standby Image

Cove has three separate methods of running a continuous restore of your data:

- Standby Image to Hyper-V - This service runs a continuous restore of a device to a Hyper-V or Local VHDX as configured in Add Recovery Locations

- Standby Image to Azure - This service runs a continuous restore of your data to Microsoft Azure and boots based on the frequency set during configuration of the plan to an Azure Virtual Machine as configured in Azure Recovery Locations
- Standby Image to ESXi- This service runs a continuous restore of a device to an ESXi server/host as configured in ESXi Recovery Locations

What's inside:

Standby Image to Hyper-V

Cove Data Protection (Cove) offers **self-hosted** Standby Image as a form of disaster recovery. It is a scheduled, automated service to recover critical devices.

> Devices **can** be assigned to **multiple Standby Image plans** at once, i.e. Standby Image to Hyper-V *and* Standby Image to Azure *and* Standby Image to ESXi.

Restores run after each backup session for System State, Files and Folders. After the first restore, a virtual machine is created and kept on the selected Recovery Location, then with each subsequent restore the virtual machine is updated with only new data.

> Restores can be performed to either a Hyper-V instance or to a Local VHDX file. Local VHDX files can be restored to either a Local Drive, or to a Network Share (NAS).

For a Virtual Machine restored to Hyper-V, there is an option to automatically boot it and create a screenshot to check that the Virtual Machine is bootable, then send this screenshot to the Management Console so that users can check it.

> There is no limit to the number of devices that can be added to a recovery location

Standby Image Data Restored:

The following data sources are supported and restored to the Hyper-V recovery location given that they are selected for backup in the Product, or data source selection:

- System State
- Files and Folders
- Exchange
- SharePoint
- MS SQL

Requirements:

- Backup Manager version 17.4 and newer
- Devices and Recovery Locations must belong to the same Customer
- A Cove Data Protection (Cove) SuperUser or Manager account

- Recovery Locations must be added to the Management Console and the Recovery service must be installed on the recovery location **before** Standby Image recovery can occur

> - Recovery Location is an environment where restores will be performed
> - Recovery service is a service which perform restores on that Recovery location

Limitations

- Standby Image cannot be used on the RMM integrated version of Backup (Managed Online Backup) or on the N-central integrated version of Backup (Backup and Recovery)
- Standby Image is **not** available for devices with disabled 'Virtual disaster recovery' feature in an assigned Product
- 32-bit architecture is not supported
- Due to a Microsoft limitation, Hyper-V **does not** support FAT/FAT32/ExFAT formatted drives. For this reason, please use NTFS formatted drives for Standby Image. More information can be found in the Microsoft Documentation for Hyper-V
- Maximum supported capacity for virtual hard disks is **64 TB** per disk
- Devices can only be assigned to **one** Recovery Location

What's inside:

Enable Standby Image to Hyper-V

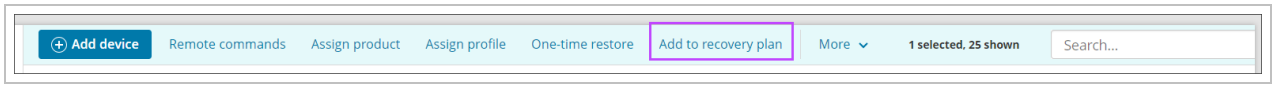
> Devices **cannot** be added to a **Standby Image plan** if already assigned to a **Recovery Testing plan**.

> Devices **can** be assigned to **multiple Standby Image plans** at once, i.e. Standby Image to Hyper-V *and* Standby Image to Azure.

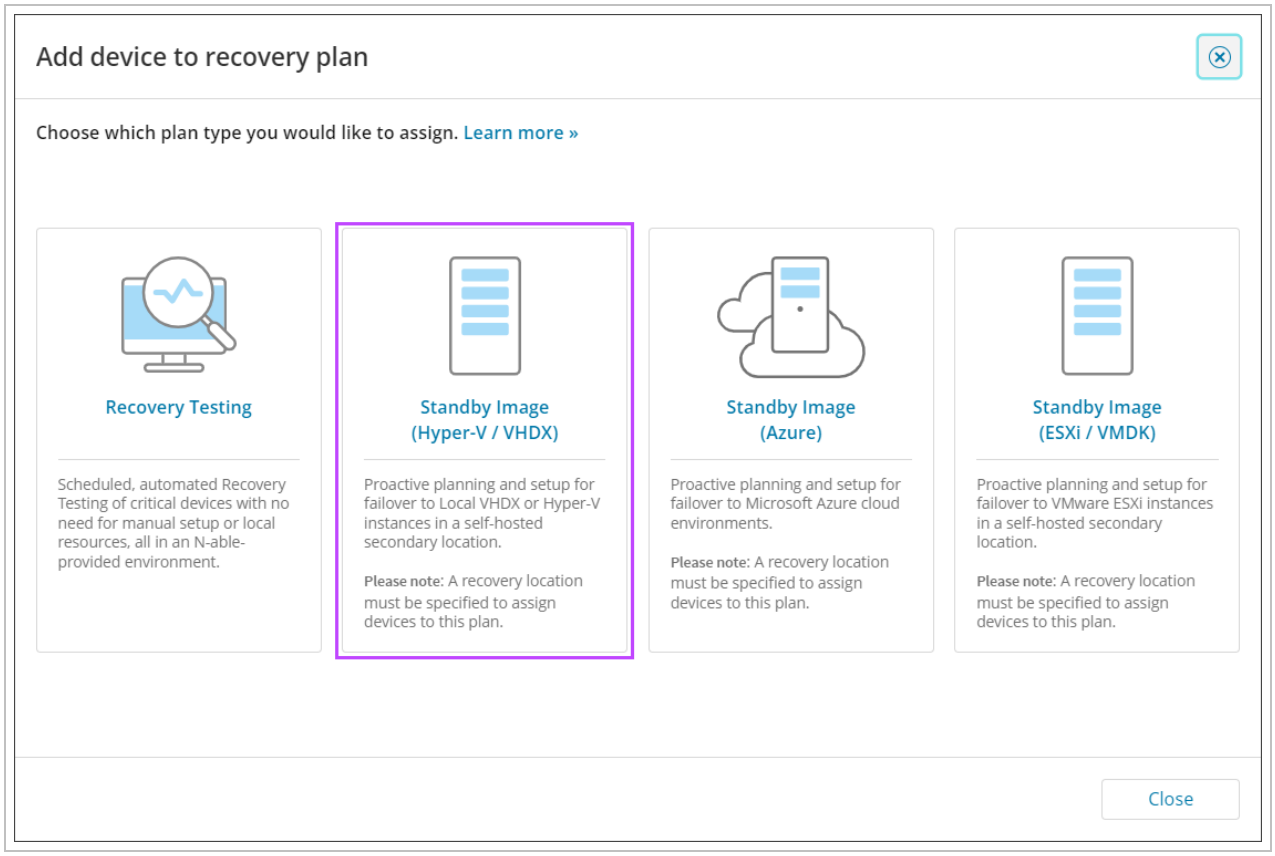
From Main Dashboard

To enable Standby Image to Hyper-V on a device from the Management Console's main Dashboard, follow the steps below:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan to
3. Click **Add to recovery plan** from the Toolbar



4. Select **Standby Image (Hyper-V)**

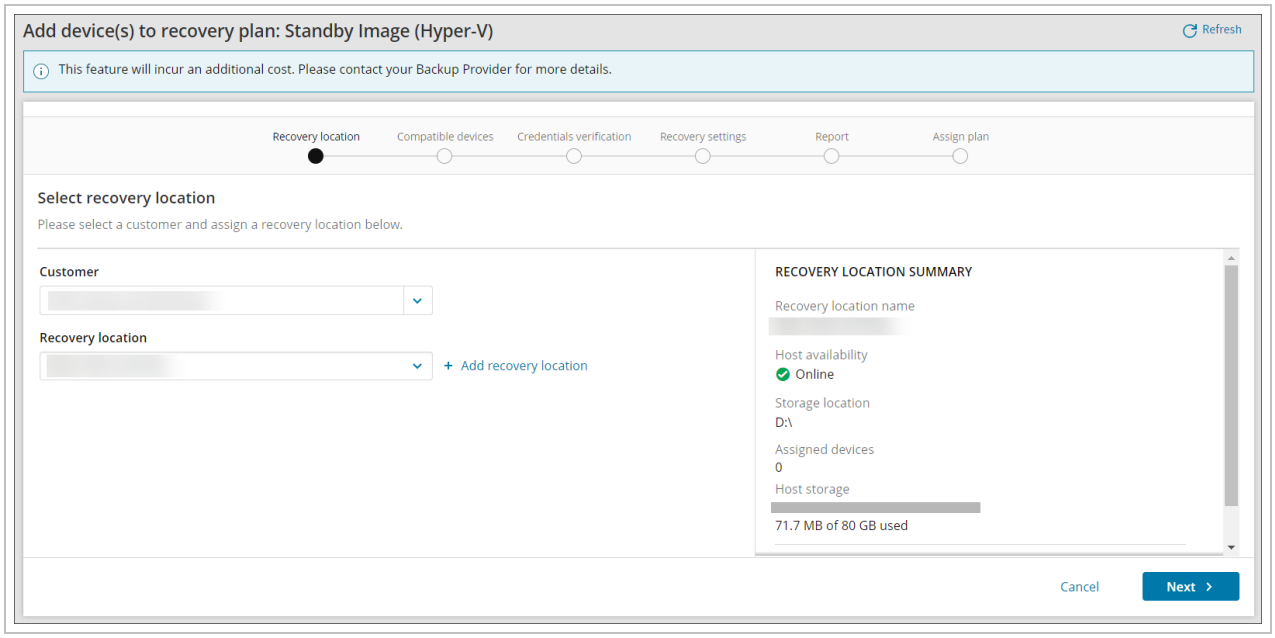


5. Select the customer the device(s) you wish to apply the Standby Image plan belong to

6. Choose the recovery location as was configured in Add Recovery Locations

> If the selected customer does not have any locations, you must add one before continuing by selecting **Add recovery location**. See Add Recovery Locations for full details of adding a location.

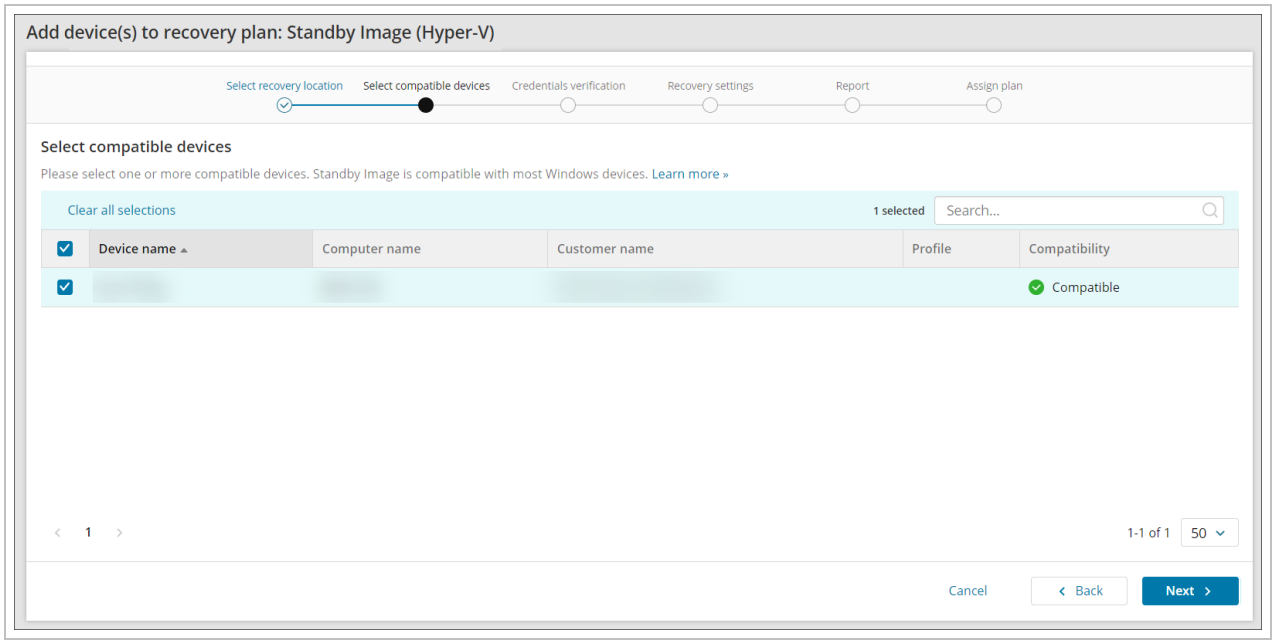
> If the Recovery Location does not have a drive letter, one must be provided before continuing



> It is not possible to assign a location for which the **Host availability** is "**Offline**"

7. Click **Next**

8. Confirm compatibility of the device(s) you want to apply the Standby Image plan on

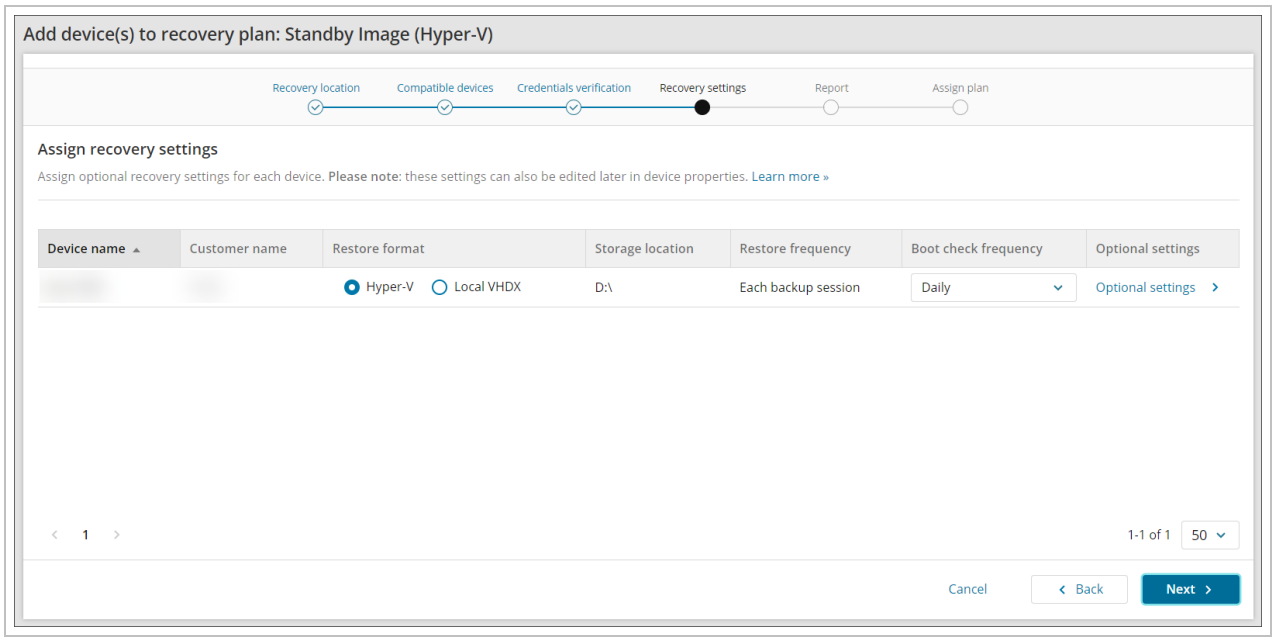


9. Click **Next**
10. Enter the security code/encryption key or passphrase for the device(s). This can be either:
    - **Private encryption key** - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryption
    - **Passphrase encryption** - These are generated on demand for automatically installed devices. You can find information on this here

    > If you are logged in as a security officer, this will be detected automatically.

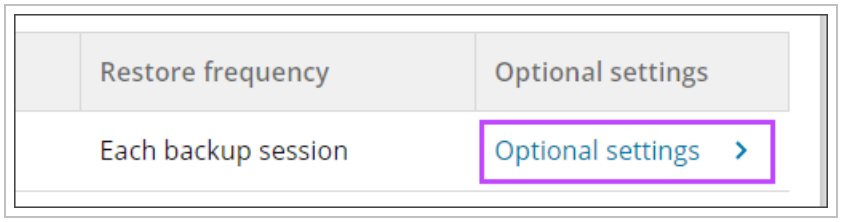
11. Click **Next** to continue

12. Choose the restore format:
    - Hyper-V
    - Local VHDX



13. Choose the boot check frequency:
    - Off
    - Every recovery session
    - Daily
    - Weekly
    - Biweekly
    - Monthly

14. Configure the **Optional Recovery Settings** for the restore format selected by clicking **Optional Settings** to the right of the storage location:



- Hyper-V optional settings:

OPTIONAL RECOVERY SETTINGS

Boot VM after restore and take a screenshot

Restore OS disk only

FRS and DFSR services

Local Speed Vault

CPU cores

4

RAM (GB)

4

Virtual switch

default switch

Enter a virtual switch to enable network settings

VM Subnet mask

255.255.255.0

VM gateway

10.16.10.1

VM DNS server

10.16.10.5.8.8.8.8

Separate multiple DNS servers with a comma or semicolon

VM IP address

10.16.10.24

IP addresses will increment by 1, if applied to all devices

- **Boot VM after restore and take a screenshot** - If this option is enabled, the new virtual machine is booted up after recovery and a confirmation screenshot is created. The results of recovery sessions together with screenshots of the booted systems come in email notifications if an email address was provided to receive a report

  The screenshots are also available in the Management Console see the "Screenshot" column in the Standby Image overview

  > Use the feature carefully if there is another virtual machines in the local network offering the same services (for example, the Active Directory) as it can result in a conflict with subsequent data loss.

- **Restore OS disk only** - Restoring the OS disk only will speed up restores
- **FRS and DFRS services** - If you are restoring Active Directory with multiple domain controllers, you should change the FRS and DFSR services to authoritative in the domain controller that will be started in the first place. Avoid marking several FRS/DFSR services as authoritative in the production environment as it can result in data loss. When the feature is on, the FRS and DFSR services are started on the target VM in the authoritative mode. The NETLOGON and SYSVOL shares become available, so the Active Directory and DNS services become functional again

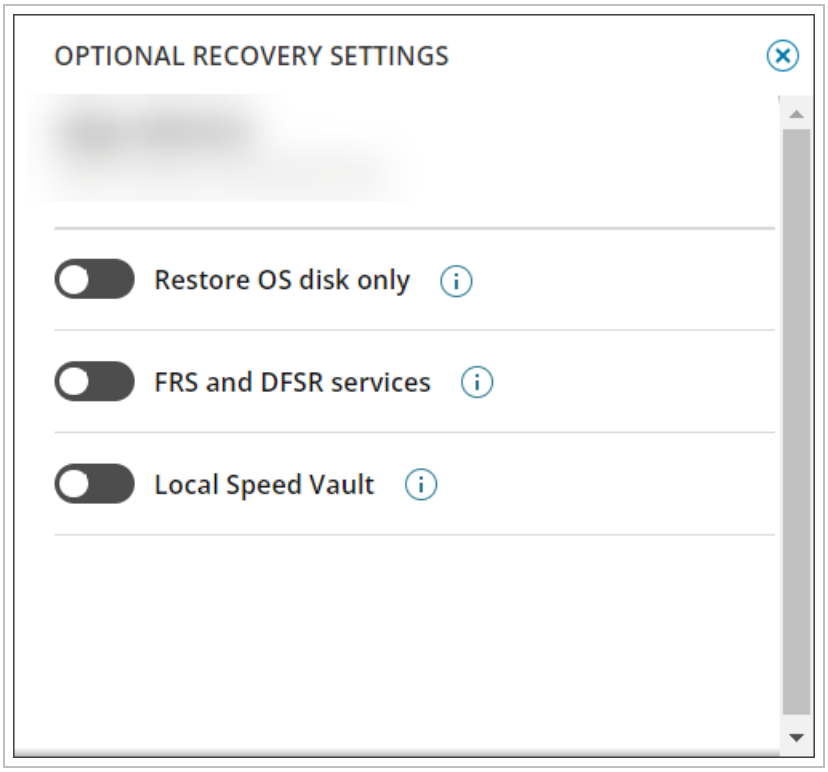
  > More information about FRS/DFSR is available in the Microsoft Knowledge Base. Article IDs: KB2218556 and KB290762

- **LocalSpeedVault** - If a LocalSpeedVault (LSV) is enabled on a backup device, the data is sent to both the LSV and the cloud or private storage location. During a restore, data is automatically downloaded from the LSV first to the local device which makes restore faster. If the LSV is not available or not synchronized, the restore data will be pulled from the cloud or private storage location. This takes place automatically and cannot be reconfigured
- **CPU Cores** - Select the number of CPU Cores to be allocated to the new virtual machine
- **RAM (GB)** - Select the amount of RAM in Gigabytes to be allocated to the new virtual machine
- **Virtual switch** - Enter the Hyper-V network adapter that will be used by your new virtual machine
- **VM subnet mask** - Assign a custom subnet mask to the virtual machine
- **VM gateway** - Assign a custom gateway to the virtual machine
- **VM DNS servers** - Assign the list of custom DNS servers (separated by comma), Example:

  ```
  8.8.8.8 or 8.8.8.8,7.7.7.7
  ```

- **VM IP address** - Assign a custom IP address to the virtual machine

- Local VHDX optional settings:



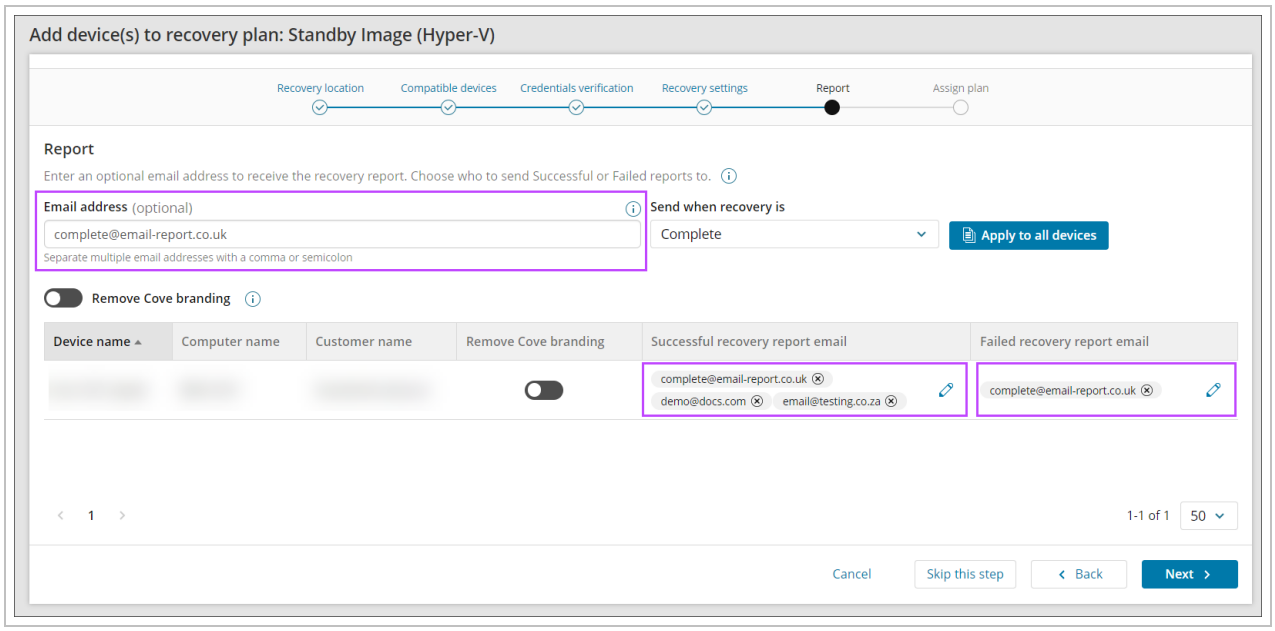
  - **Restore OS disk only** - Restoring the OS disk only will speed up restores
  - **FRS and DFRS services** - If you are restoring Active Directory with multiple domain controllers, you should change the FRS and DFSR services to authoritative in the domain controller that will be started in the first place. Avoid marking several FRS/DFSR services as authoritative in the production environment as it can result in data loss. When the feature is on, the FRS and DFSR services are started on the target VM in the authoritative mode. The NETLOGON and SYSVOL shares become available, so the Active Directory and DNS services become functional again

    > More information about FRS/DFSR is available in the Microsoft Knowledge Base. Article IDs: KB2218556 and KB290762

  - **LocalSpeedVault** - If a LocalSpeedVault (LSV) is enabled on a backup device, the data is sent to both the LSV and the cloud or private storage location. During a restore, data is automatically downloaded from the LSV first to the local device which makes restore faster. If the LSV is not available or not synchronized, the restore data will be pulled from the cloud or private storage location. This takes place automatically and cannot be reconfigured

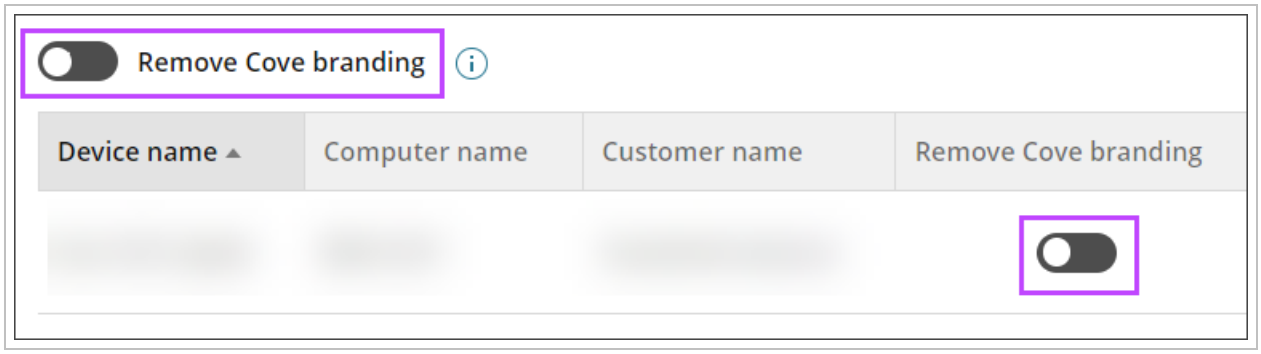
15. Click **Next** to progress to the **Report** window to enter one or more email addresses to receive a report when:
    a. The recovery is complete (Successful or Failed)
    b. The recovery was successful
    c. The recovery failed

> Multiple addresses should be separated using a comma or semi-colon



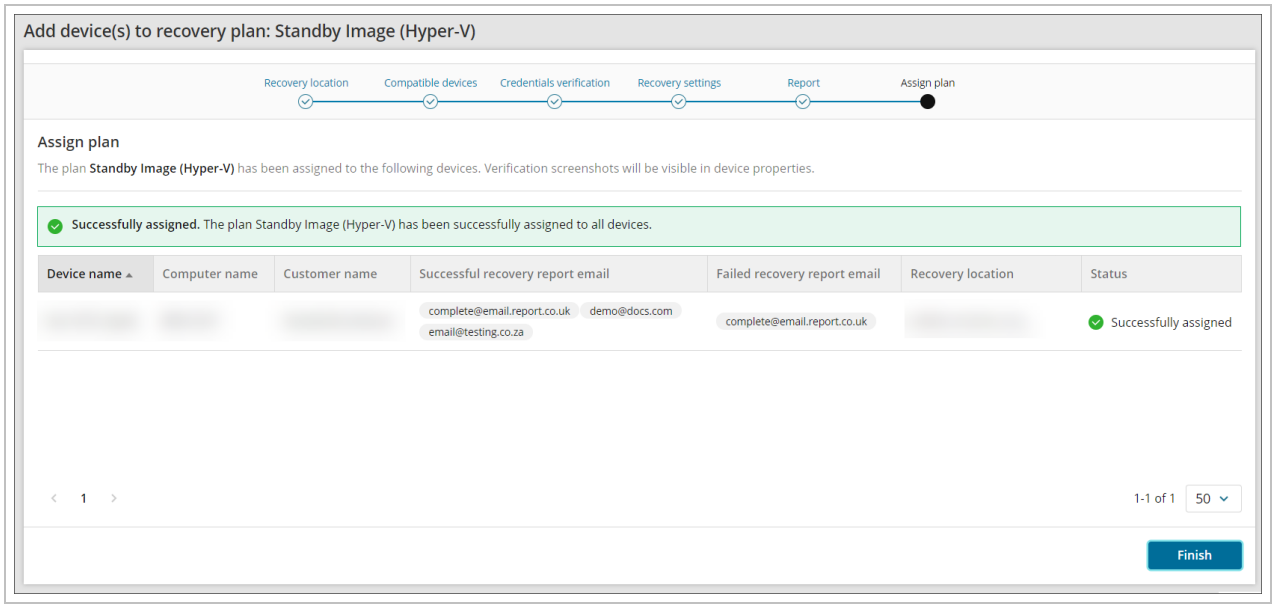
> If you do not want to add an email address to receive reports, click **Skip this step**

16. To remove all branding from the reports, use the **Remove Cove branding** toggle per device, or above the device list to apply the changes to all devices in this window



17. Confirm assigning the plan to the device(s)

18. Wait for the plan to be assigned until you see a confirmation banner on the page

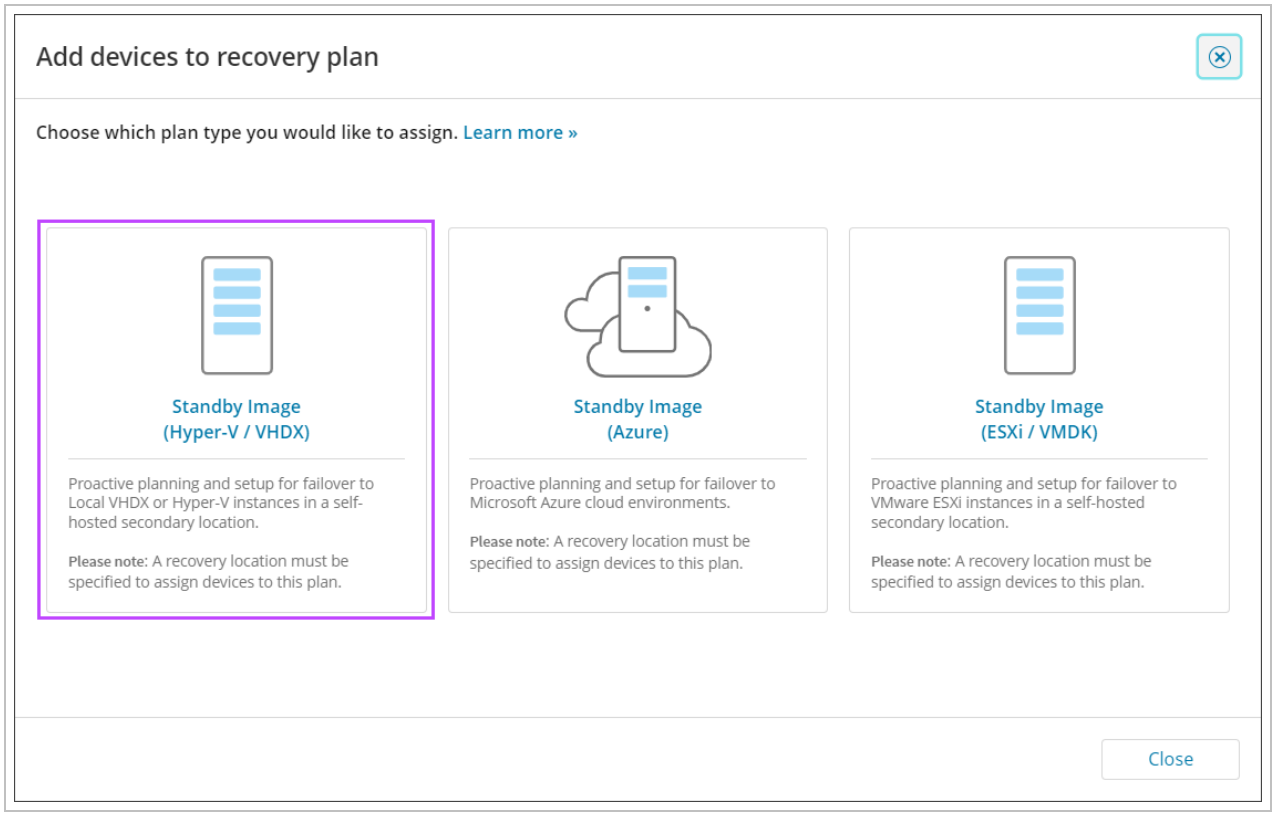


19. Click **Finish**

From Standby Image Overview

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Click **Add to Plan**

4. Select **Standby Image (Hyper-V)**



5. You will now be taken to the **add devices to recovery plan** wizard. Follow the steps from select the customer from the dropdown onwards

From Recovery Locations dashboard

Devices can be added to a Recovery Location from the **Continuity** > **Recovery Locations** page, thereby enabling the Standby Image Plan, using one of three methods:

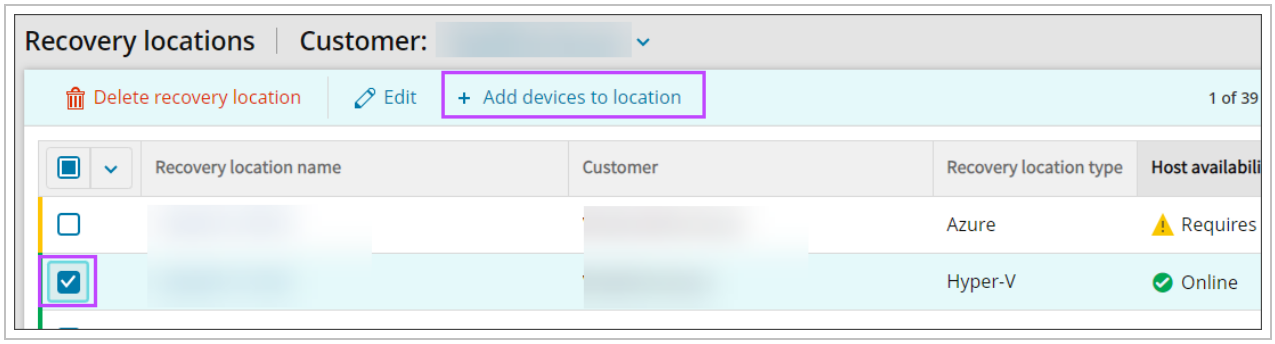
- Top bar menu
- Location context menu
- Right-hand menu

> These will only be available if the Recovery Location is **Online**.

Top bar menu

Available for Hyper-V and ESXi Locations **only**.

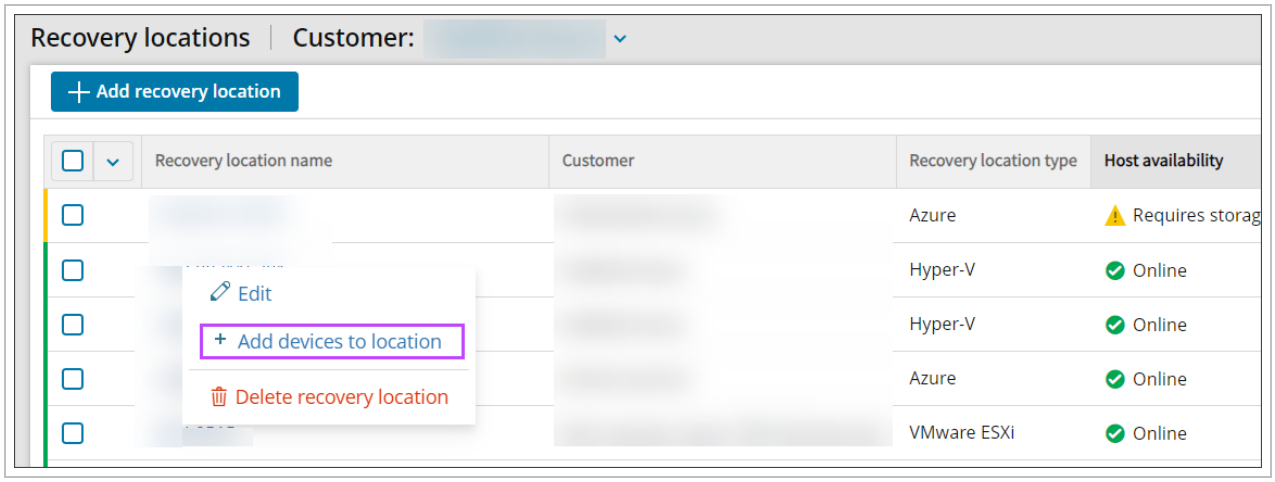
1. Select the checkbox for the Recovery Location to add the device to
2. At the top of the Recovery Locations page, select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
   a. Top bar menu
   b. Top bar menu

Location context menu

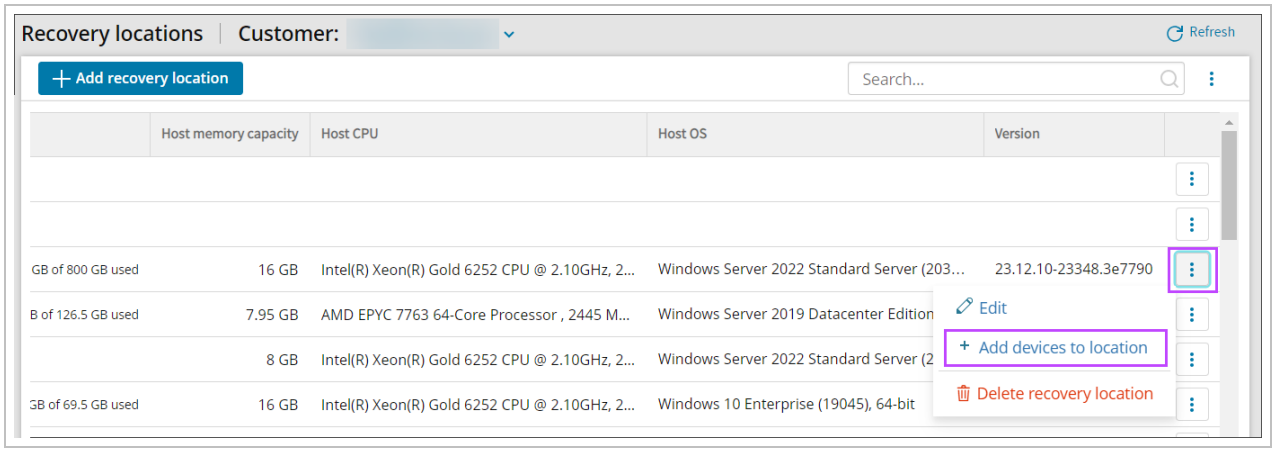
1. Right-click on the Recovery Location to add the device to
2. Select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
    a. Enable Standby Image to AzureDevices cannot be added to a Standby Image plan if already assigned to a Recovery Testing plan.Devices can be assigned to multiple Standby Image plans at once, i.e. Standby Image to Hyper-V and Standby Image to Azure. From Main DashboardTo enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:Log in to the Management Console under a SuperUser or Manager account In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan toClick Add to recovery plan from the Toolbar Select Standby Image (Azure)Select the customer the device(s) you wish to apply the Standby Image plan belong toChoose the recovery location as was configured in Add Recovery LocationsIf the selected customer does not have any locations, you must add one before continuing by selecting Add recovery location. See Add Recovery Locations for full details of adding a location.It is not possible to assign a location for which the Host availability is "Offline"Click NextConfirm the device selected from the Dashboard is compatible and click Next Enter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereClick Next to continueChoose the boot check frequency:OffEvery recovery sessionDailyWeeklyBiweeklyMonthlyIf you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Once connected, click NextClick Azure VM settings towards the right-hand side of the screen to open the settings configuration window:Configure the Azure VM Settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk typeData disk(s) typeVirtual NetworkSubnetAssign NSG and public IPDuring the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend blocking internet access for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.Click Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowConfirm assigning the plan to the device(s)Wait for the plan to be assigned until you see a confirmation banner on the pageClick FinishFrom Standby Image OverviewLog in to the Management Console under a SuperUser or Manager accountNavigate to Continuity > Standby ImageClick Add to PlanSelect Standby Image (Azure)You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the planRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding:
    b. Top bar menu
    c. Top bar menu

Right-hand menu

1. Click the action menu button for the Recovery Location, seen as three dots in a vertical line to the right of the location's version
2. Select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
    a. Enable Standby Image to AzureDevices cannot be added to a Standby Image plan if already assigned to a Recovery Testing plan.Devices can be assigned to multiple Standby Image plans at once, i.e. Standby Image to Hyper-V and Standby Image to Azure. From Main DashboardTo enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:Log in to the Management Console under a SuperUser or Manager account In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan toClick Add to recovery plan from the Toolbar Select Standby Image (Azure)Select the customer the device(s) you wish to apply the Standby Image plan belong toChoose the recovery location as was configured in Add Recovery LocationsIf the selected customer does not have any locations, you must add one before continuing by selecting Add recovery location. See Add Recovery Locations for full details of adding a location.It is not possible to assign a location for which the Host availability is "Offline"Click NextConfirm the device selected from the Dashboard is compatible and click Next Enter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereClick Next to continueChoose the boot check frequency:OffEvery recovery sessionDailyWeeklyBiweeklyMonthlyIf you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Once connected, click NextClick Azure VM settings towards the right-hand side of the screen to open the settings configuration window:Configure the Azure VM Settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk typeData disk(s) typeVirtual NetworkSubnetAssign NSG and public IPDuring the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend blocking internet access for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.Click Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowConfirm assigning the plan to the device(s)Wait for the plan to be assigned until you see a confirmation banner on the pageClick FinishFrom Standby Image OverviewLog in to the Management Console under a SuperUser or Manager accountNavigate to Continuity > Standby ImageClick Add to PlanSelect Standby Image (Azure)You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the planRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding:
    b. Top bar menu
    c. Top bar menu

Recovery Reports

When the device(s) assigned to the plan have **Successful recovery report email** or **Failed recovery report email** recipient

address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox.

Here is an example report with Cove branding:

Cove Data Protection

Recovery completed

Recovery plan: **Standby Image (Hyper-V)**

Last recovery session completed successfully: April 13 2024 9:15:32 PM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Workstation
Operating system	Windows 10 Enterprise (19045), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 13 2024 9:15:32 PM
Recovery status	Completed
Recovery duration	1 hour, 2 minutes and 11 seconds
Recovery location	
Storage location	D:\
Restore frequency	Each backup session
Recovery plan	Standby Image (Hyper-V)

BACKUP DETAILS USED FOR THE RESTORE

Backup session time	April 13 2024 8:45:28 PM
Backup status	Completed

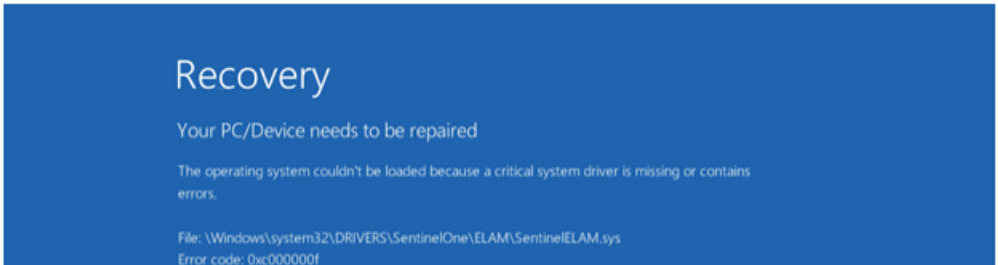
DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

BOOT TEST OVERVIEW

Screenshot verification	Completed
Boot time	April 13 2024 9:15:32 PM
Backup session time	April 13 2024 8:45:28 PM
Boot check frequency	Each recovery session

Below is a screenshot of the virtual machine created during the boot phase of recovery.



Here is an example **without** Cove branding:

Recovery completed

Recovery plan: **Standby Image (Hyper-V)**

Last recovery session completed successfully: April 16 2024 3:45:28 AM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Workstation
Operating system	Windows 10 Enterprise (19045), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 16 2024 3:45:28 AM
Recovery status	Completed
Recovery duration	1 hour, 13 minutes and 6 seconds
Recovery location	Hyper-V.OaNaB
Storage location	D:\
Restore frequency	Each backup session
Recovery plan	Standby Image (Hyper-V)

BACKUP DETAILS USED FOR THE RESTORE

Backup session time	April 16 2024 3:35:44 AM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

BOOT TEST OVERVIEW

Screenshot verification	Not applicable
Boot check frequency	Off

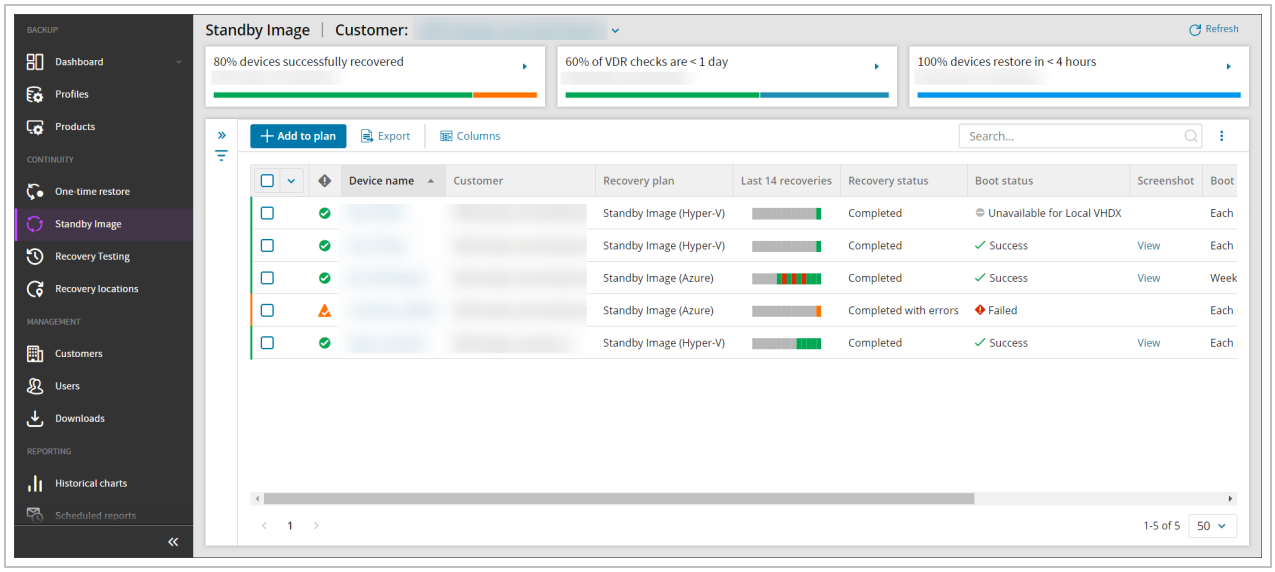
Screenshot verification is not applicable

Monitor Standby Image Devices

From the Management Console, you can view the dedicated Standby Image Overview by selecting **Continuity** > **Standby Image** from the vertical menu on the left hand side.

This page will list devices assigned to the Standby Image plans:

- Standby Image to Hyper-V
- Standby Image to Azure
- Standby Image to ESXi



From this dashboard, you will see a specified set of columns detailing information relevant to devices using the Standby Image plan, including the continuity history of the last 14 recoveries, the recovery status, boot status, and plan assigned, along with some other information.

If no devices are assigned to either Standby Image plan, the dashboard will display a message to advise, along with a button to add devices to a plan.

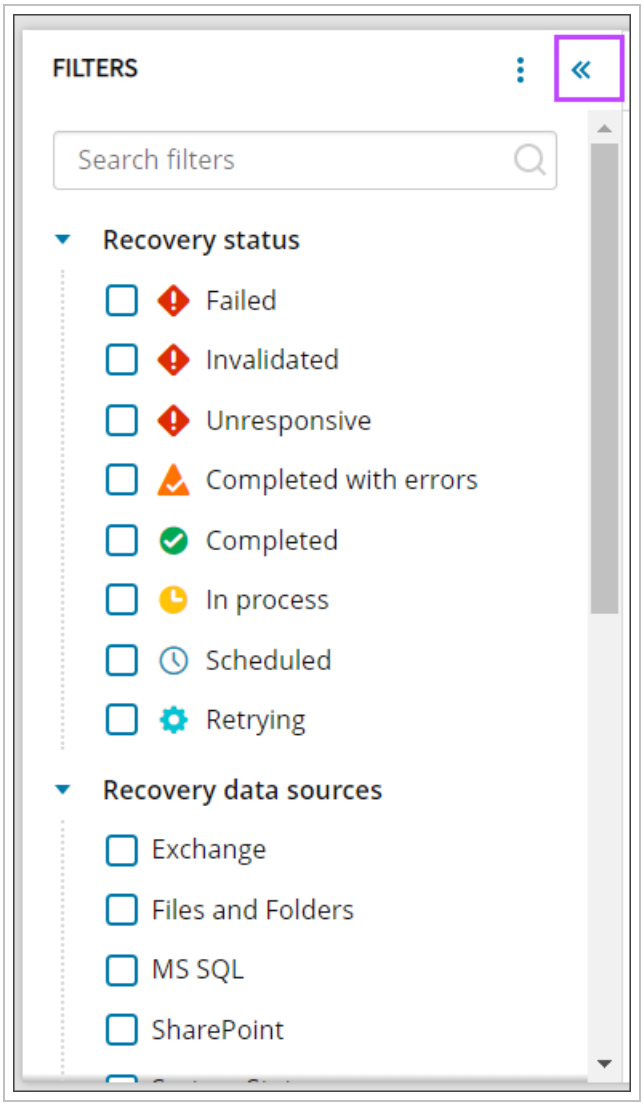
> If a device is assigned to **multiple** plans (i.e. **Standby Image to Hyper-V**, **Standby Image to Azure** and **Standby Image to ESXi**), the device will be listed for each instance of a plan and can be told apart by the **Recovery Plan** column.

Searching

Searching within the Standby Image overview can be done by using the search box over to the right hand side of the page, just above the devices list. The search can be performed by any text field.

Filtering

The Standby Image overview also includes functionality to filter devices using the filter menu to the left of the device list and can be displayed or hidden by clicking the double arrows.



From this menu, you can filter by:

Recovery status

- **Failed** - The recovery session has failed
- **Invalidated** - Device was moved to an inappropriate partner and so the session has failed
- **Unresponsive** - The recovery session was initiated but did not receive updates for at least 30 minutes because the recovery location restarted or was offline.
- **Completed with errors** - The recovery session completed, but encountered errors
- **Completed** - The recovery session completed with no errors
- **In process** - The recovery is currently in progress
- **Scheduled** - Devices just added to a recovery plan and are waiting for their first recovery session or devices where restores were paused and have since been resumed will display as scheduled
- **Retrying** - A restore session was not finished so the system is trying the restore again

Recovery data sources

- Exchange
- Files and Folders
- MS SQL
- SharePoint
- System State

Recovery session statistics

- Boot check frequency
  - Off
  - Every recovery session
  - Daily
  - Weekly
  - Biweekly
  - Monthly
- Boot Check Status
  - Success
  - Failed
  - Off
  - Unavailable for Local VHDX
- Continuous restores
  - Running
  - Paused
- Duration of the last completed recovery session
  - Sliding scale from 0 to unlimited

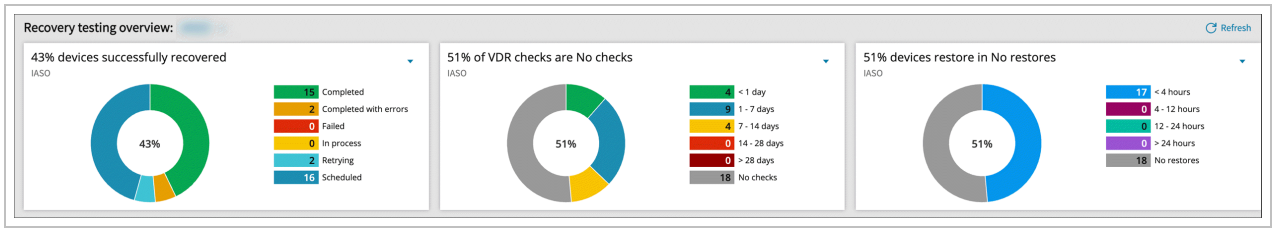
  in minutes
- Number of errors of the last completed recovery session
  - Sliding scale from 0 to unlimited
- Number of restored files
  - Sliding scale from 0 to unlimited
- Number of selected files
  - Sliding scale from 0 to unlimited
- Recovery Location name
  - Select the recovery location from a dropdown
- Recovery Plan
  - Standby Image (Hyper-V)
  - Standby Image (ESXi)
  - Standby Image (Azure)
- Restored size
  - Sliding scale from 0 to unlimited

  in KB and GB

- Recovery testing status of the last completed recovery session
  - Failed
  - Completed with errors
  - Completed
- Screenshot
  - Available
  - Not Available
- Selected size
  - Sliding scale from 0 to unlimited
  in KB and GB
- Timestamp of the last completed recovery session
  - Quick Picks of:
    - Last day
    - 1 - 7 days
    - 7 - 14 days
    - 14 - 28 days
    - > 28 days
  - Custom range, select a stat date and time and an end date and time

Widgets

Three widgets can be maximized at the top of the page, which allow for further filtering:



Device recovery status

This widget allows you to filter the devices by recovery status:

- Completed
- Completed with errors
- Failed
- In process
- Retrying
- Scheduled

VDR checks time frame

This widget allows you to see the percentage of devices whose recovery check completed within the following day ranges:

- < 1 day
- 1 - 7 days
- 7 - 14 days
- 14 - 28 days
- > 28 days
- No checks

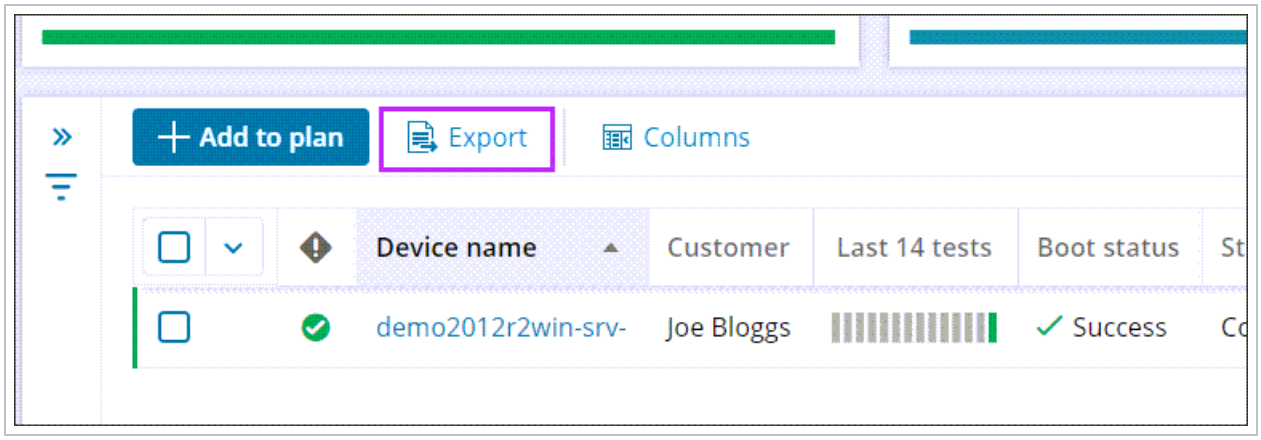
Device restore time frame

From this widget, you can filter devices by the how recent restores are done by the following time frames:

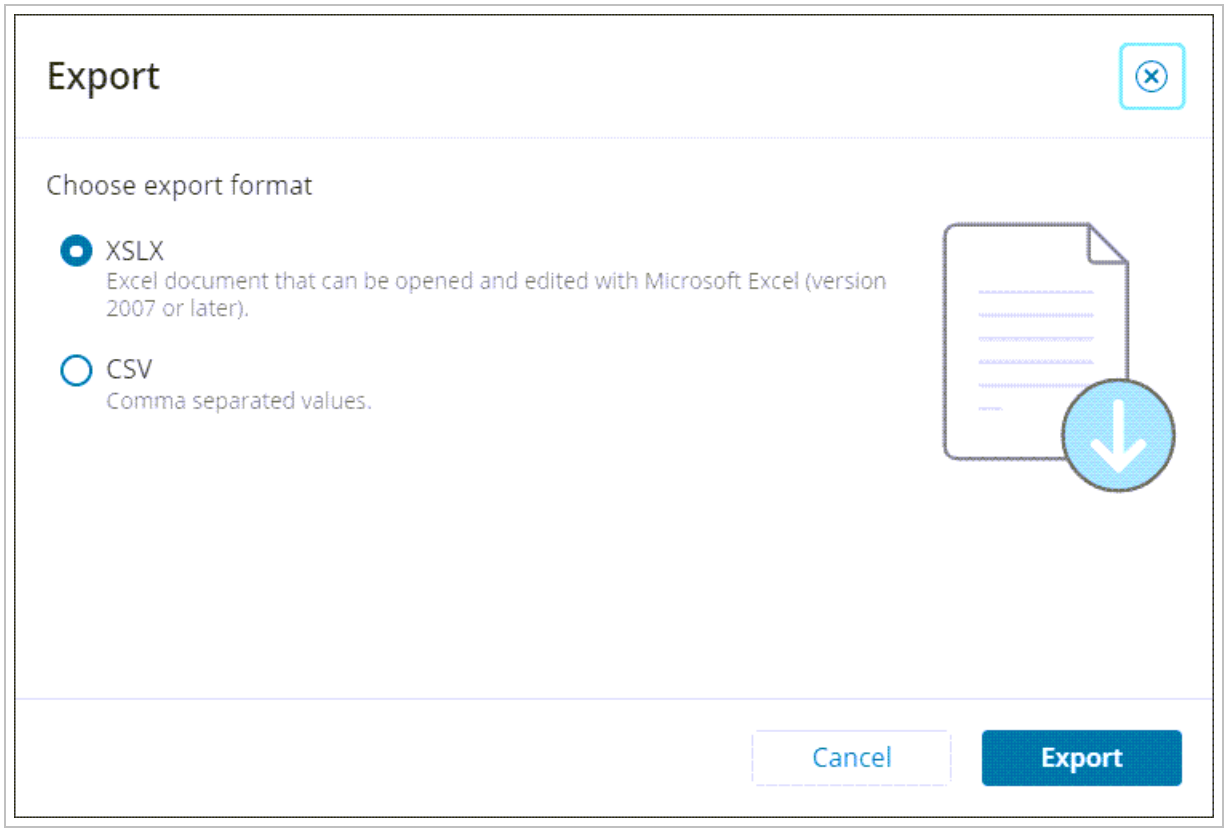
- < 4 hours
- 4 - 12 hours
- 12 - 24 hours
- > 24 hours
- No restores

Exporting

You may export a list of devices currently assigned a plan by clicking **Export**

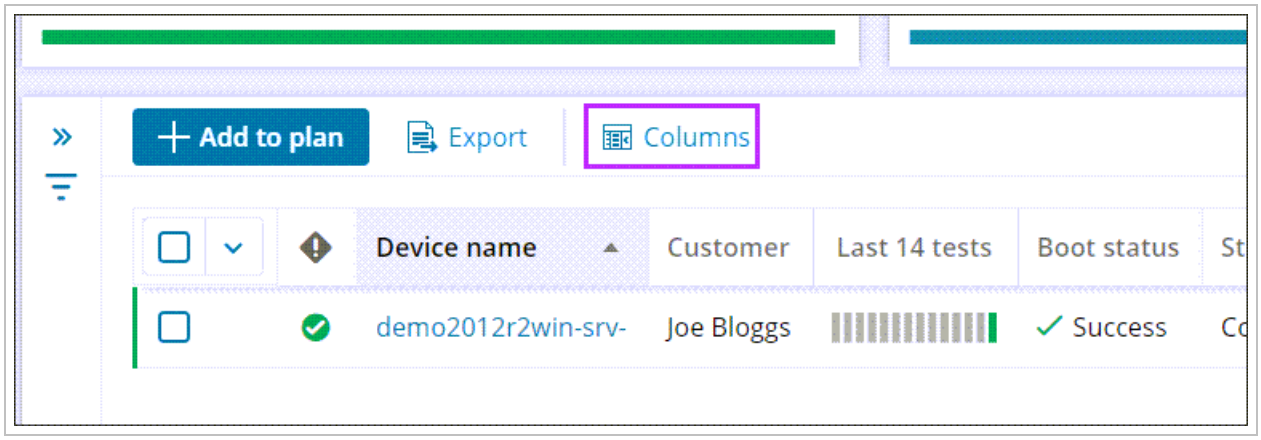


This will then provide a separate dialog where you can choose to export in either XSLX or CSV.

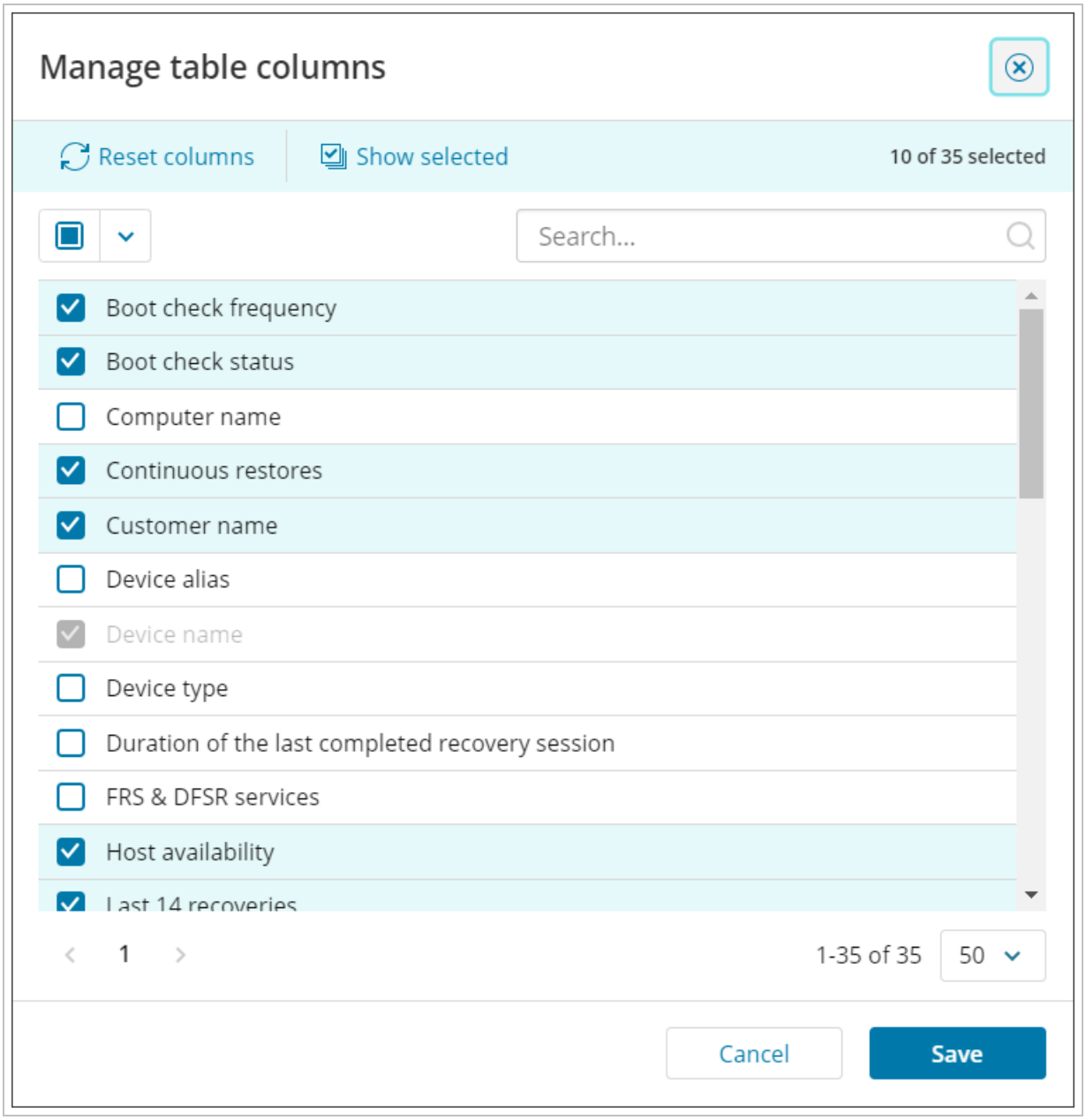


Manage Table Columns

Management Console allows you to manage the tables columns that can be seen within the Standby Image overview.



In the Manage table columns dialog, you can select and deselect columns based on the information you wish to view from the overview.

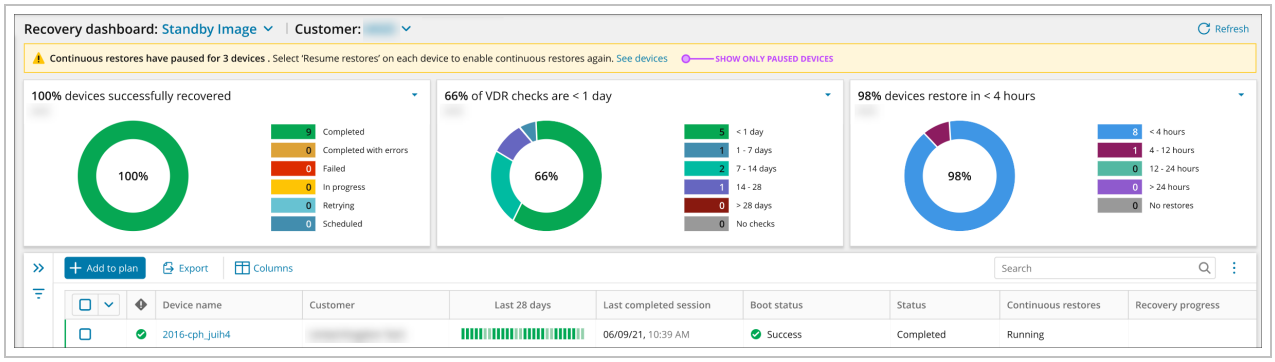


Pause Standby Image recovery

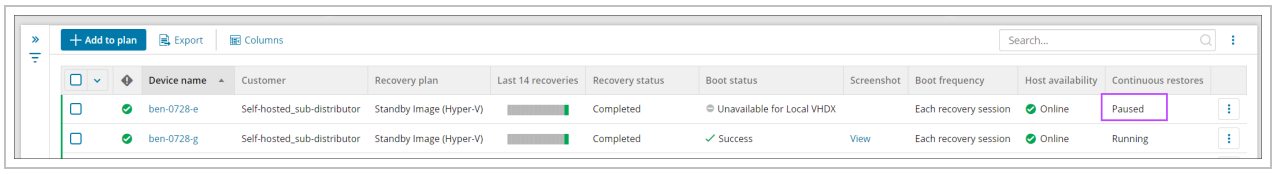
Once a Standby plan has been assigned to a device, the continuous restores can be paused and restarted. Pause or resume restores functionality there to provide a possibility to use the restored machine for failover in case of disaster.

> If a restored Virtual Machine is turned on manually, the Standby Image restore will automatically pause.

Pausing and restarting continuous restores can done be for single or multiple devices at a time. Once devices have been paused, a banner will be displayed at the top of the page to advise.

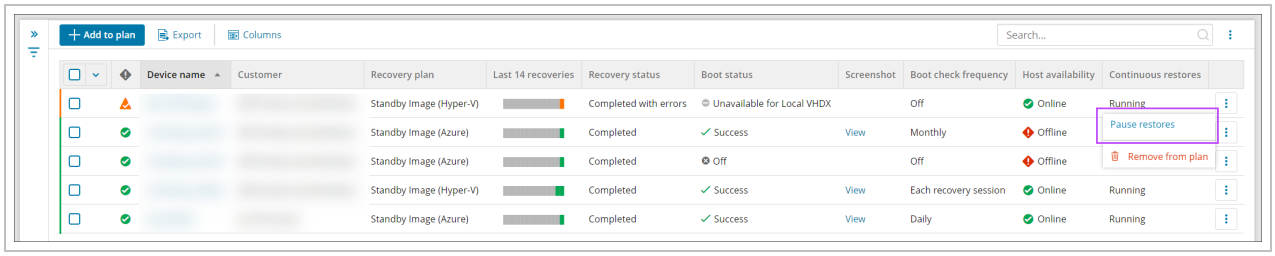


Click **See devices** to filter the devices list by **Continuous Restore: Paused** to only devices which are currently paused.



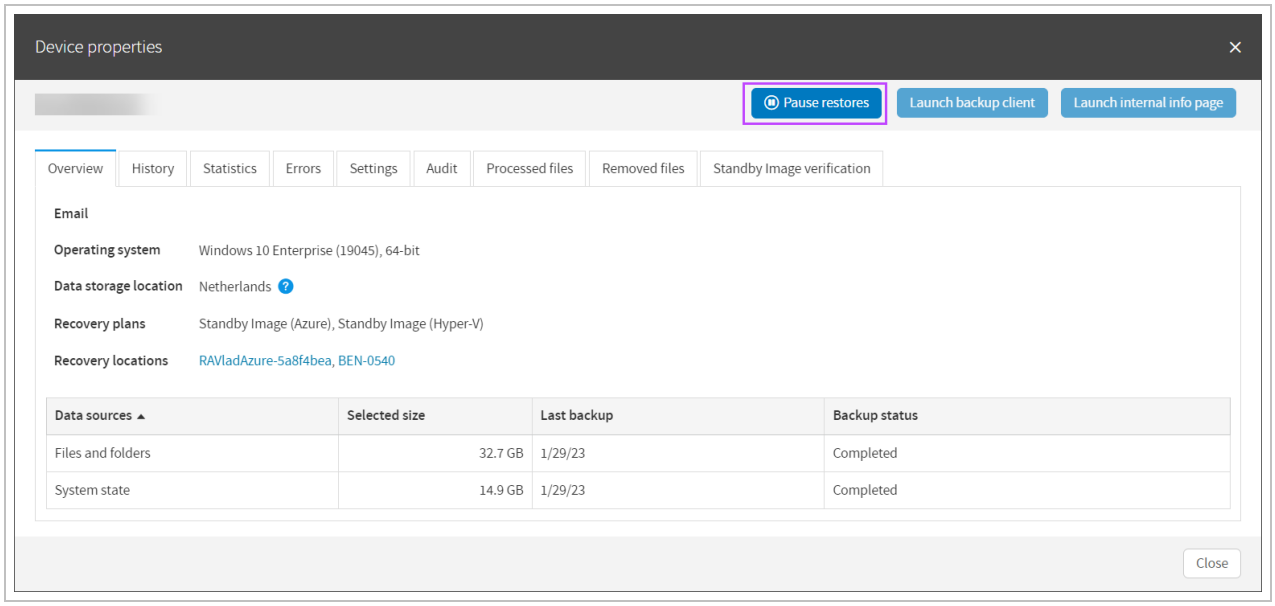
For single devices

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Click the menu action button to the right of the device (Three vertical dots)
4. Select **Pause Restores** or **Resume Restores**



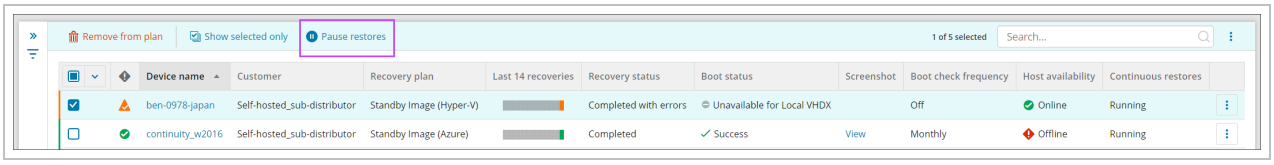
> This will differ depending on whether the plan is currently active, or has been paused already

It is also possible to pause restores from the Device Properties window:



For single or multiple devices

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Tick the checkbox for any devices that need paused from the list
4. In the top panel, select **Pause Restores** or **Resume Restores**



> This will differ depending on whether the plan is currently active, or has been paused already

Accessing device properties

The Device Properties window displays several tabs detailing information on the Backup device. Full details of the contents of each tab can be found on the Device management in Management Console page.

The two that are the most commonly used with Standby Image are the **Settings** tab and the **Standby Image Verification** tab.

Settings Tab

Broken into several sections, this tab contains:

General

This section provides the main device details:

- **customer** - Who device belongs to, can be changed to move the device to a different customer
- **Device name** - Cannot be changed

- **Installation key** - Cannot be changed
- **Creation date** - Cannot be changed
- **Expires on** - Can be amended to a date in the future, or set to **'no expiration'** if required

> You may also see the Request Passphrase button here if the device is set up to use this instead of its own security code/encryption key

Backup

This section contains:

- **Backup product** - Use the dropdown to change the Product used by the device
- **Profile** - Use the dropdown to change the Profile applied to the device

Recovery

On a device assigned to the Standby Image plan, this section will allow you to see plan in use and amend some details of this:

- **Recovery Plan** - Standby Image (Each backup session)
- **Recovery Location** - Cannot be changed from this panel. To change this, see Add Device to Recovery Location
- **Successful recovery report email** - Specify the email address(es) that will receive reports when the most recent Recovery as per the assigned plan has been successful
- **Failed recovery report email** - Specify the email address(es) that will receive reports when the most recent Recovery as per the assigned plan has failed
- **Remove Cove branding** - toggle branding of the email reports on or off
- **Restore format** - This option will not be available for Standby Image to Azure.
  - For **Standby Image to Hyper-V**, this is a choice between **Hyper-V** or **Local VHDX**
  - For **Standby Image to ESXi**, this is a choice between **ESXi** and Local **VHDX**

    > Further settings displayed are dependent on the Restore Format selected for the device. These settings can be changed as required.

> All Recovery Plans associate to the device will be included here, and can be minimized or expanded by clicking the arrow to the left of the plan name.

Device properties

Launch backup client | Launch internal info page

Overview | History | Statistics | Errors | Settings | Audit | Processed files | Removed files | Standby Image verification

General

Customer

Device name

Installation key

Creation date 2/21/23

Expires on 04/18/24 No expiration

Backup

Product _test

Profile -servers

Recovery

Standby Image (ESXi)

Recovery plan Standby Image (ESXi)

Recovery location ESXiRA

Successful recovery report email e.g email@email.com

Failed recovery report email e.g email@email.com

Remove Cove branding OFF

Restore format ESXi VMDK

Boot check frequency Daily

FRS and DFSR services OFF

Local Speed Vault OFF

CPU cores 4

RAM (GB) 4

VM Subnet mask Enter a custom subnet mask to the new virtual mac

VM gateway Enter a custom gateway to the new virtual machine

VM DNS server Enter a DNS server to be used on the restored mach

Separate multiple DNS servers with a comma or semicolon

VM IP address Enter a custom IP address to the new virtual machir

Standby Image (Hyper-V)

Recovery plan Standby Image (Hyper-V)

Recovery location BEN-6478

Successful recovery report email e.g email@email.com

Failed recovery report email e.g email@email.com

Remove Cove branding OFF

Restore format Hyper-V Local VHDX

Boot check frequency Daily

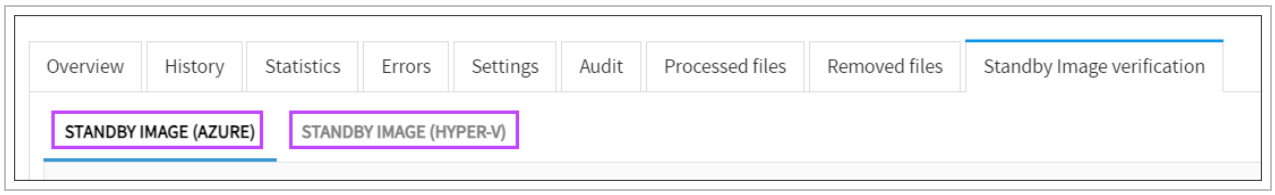
FRS and DFSR services OFF

Local Speed Vault OFF

Standby Image Verification Tab

To view statistics of the Standby Image and check the screenshots to ensure this has been successful, you can view this by following one of the below methods.

All plans associated to the device will have their own sub-tabs that can be selected to view the appropriate screenshot:



From Device Properties

1. Log in to the Management Console
2. Click the device name on either the Backup Dashboard or the Standby Image overview to open the Device Properties
3. Navigate to the **Standby Image Verification** tab

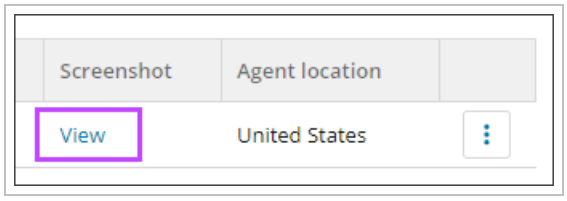
From Standby Image Overview

The Standby Image Verification tab can be viewed from the Standby Image overview in one of two ways:

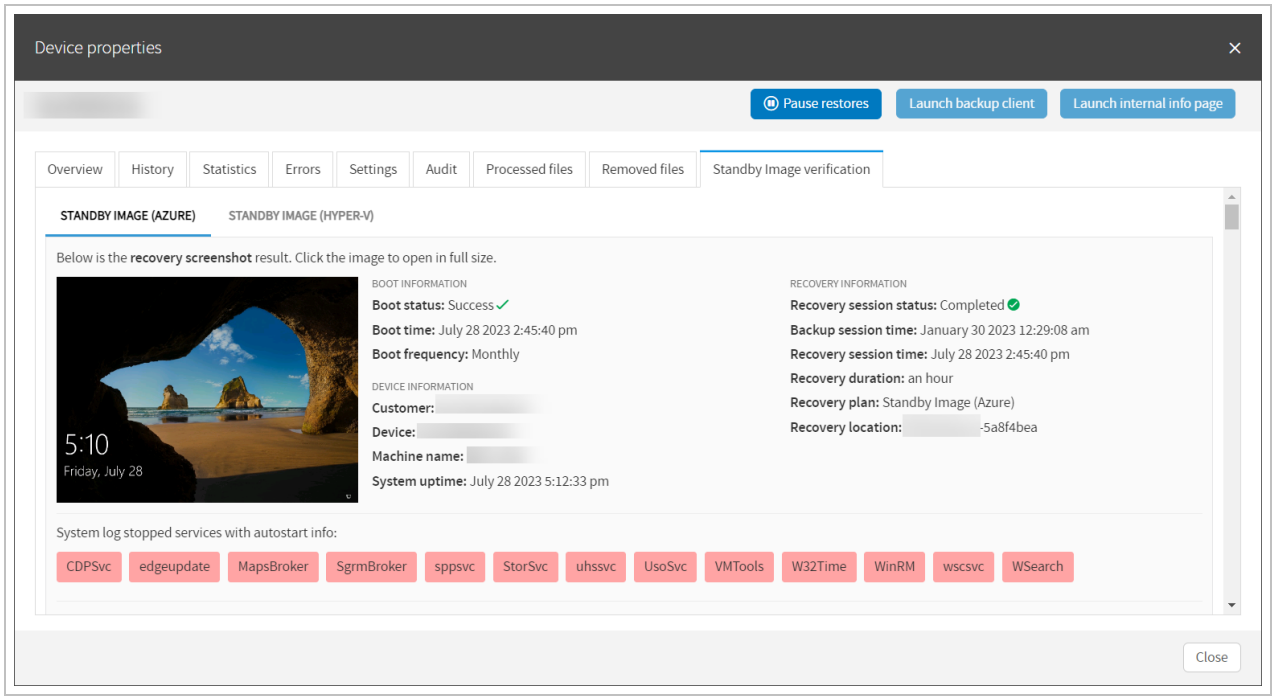
- Via theScreenshot column
- Via the Last 14 recoveries column

Screenshot column

1. Log in to the Management Console
2. Navigate to **Continuity** > **Standby Image**
3. Click **View** under the Screenshot column

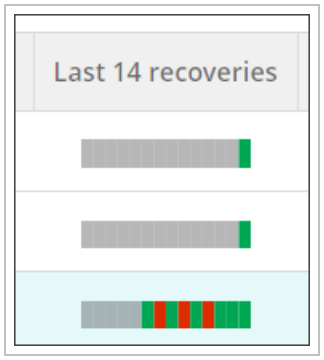


4. This will take you in to the Device Properties dialogue, where you will now see the **Standby Image Verification** tab:

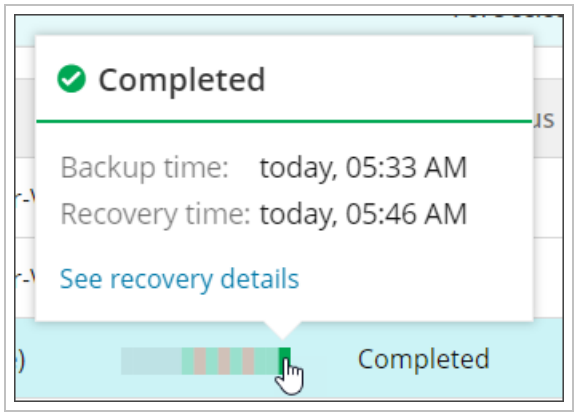


Last 14 recoveries column

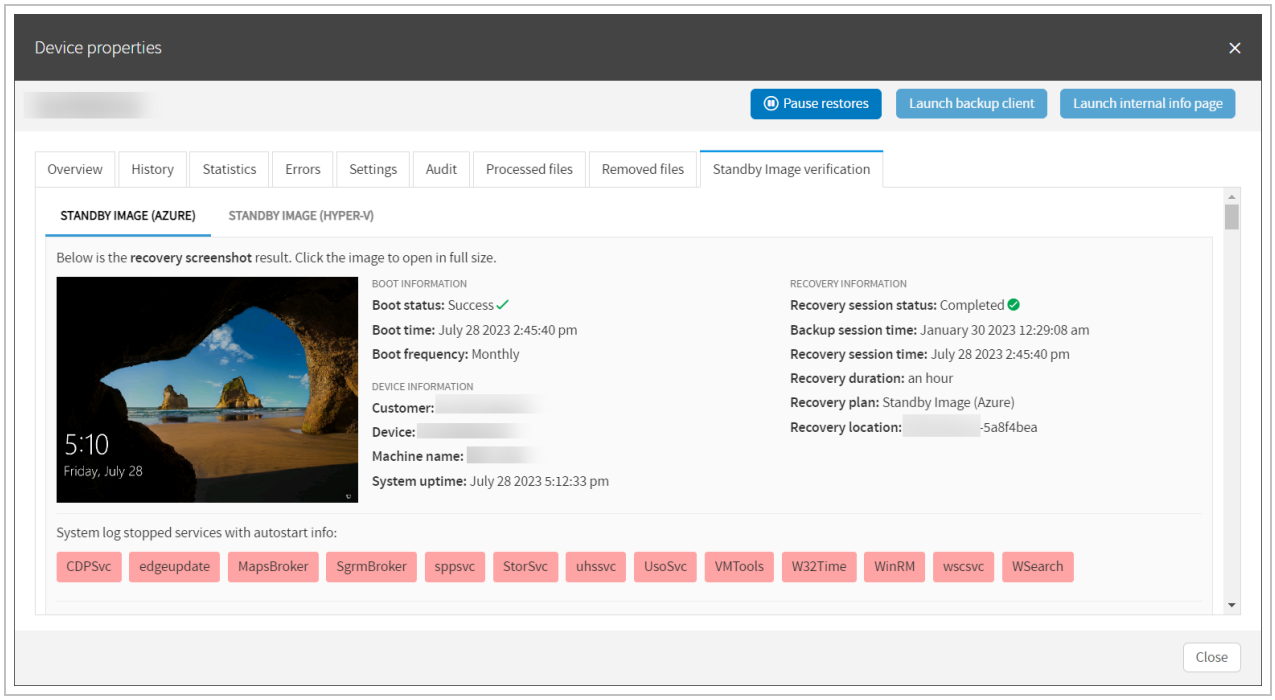
1. Log in to the Management Console
2. Navigate to **Continuity** > **Standby Image**
3. Hover your mouse over the most recent colored bar in the Last 14 recoveries column



4. Click **See recovery details** in the popup box that appears



5. This will take you in to the Device Properties dialogue, where you will now see the **Standby Image Verification** tab:



Standby Image to Azure

Cove Data Protection (Cove)'s Standby Image to Azure service runs a continuous restore of your data to Microsoft Azure and boots based on the frequency set during configuration of the plan.

> Devices **can** be assigned to **multiple Standby Image plans** at once, i.e. Standby Image to Hyper-V *and* Standby Image to Azure *and* Standby Image to ESXi.

Standby Image Data Restored:

Standby Image restores the following data sources:

- System State
- Files and Folders
- Exchange
- SharePoint
- MS SQL

Requirements

- Backup Manager version 17.4 and above
- The target VM **must** have access to Azure storage in order to successfully perform boot test
- A pre-created virtual network and subnet in the Azure resource group where you plan to do the restore
- The Recovery Location VM **must** be assigned the **Owner role** in the **Azure resource group** where you are placing standby image
- The Recovery Location VM **must** be assigned the **Owner role** for the **resource group of the Virtual Network** being used for the restore

What's inside:

Enable Standby Image to Azure

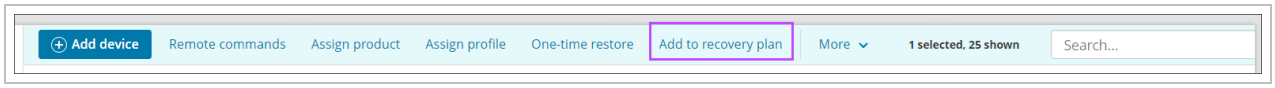
> Devices **cannot** be added to a **Standby Image plan** if already assigned to a **Recovery Testing plan**.

> Devices **can** be assigned to **multiple Standby Image plans** at once, i.e. Standby Image to Hyper-V *and* Standby Image to Azure.

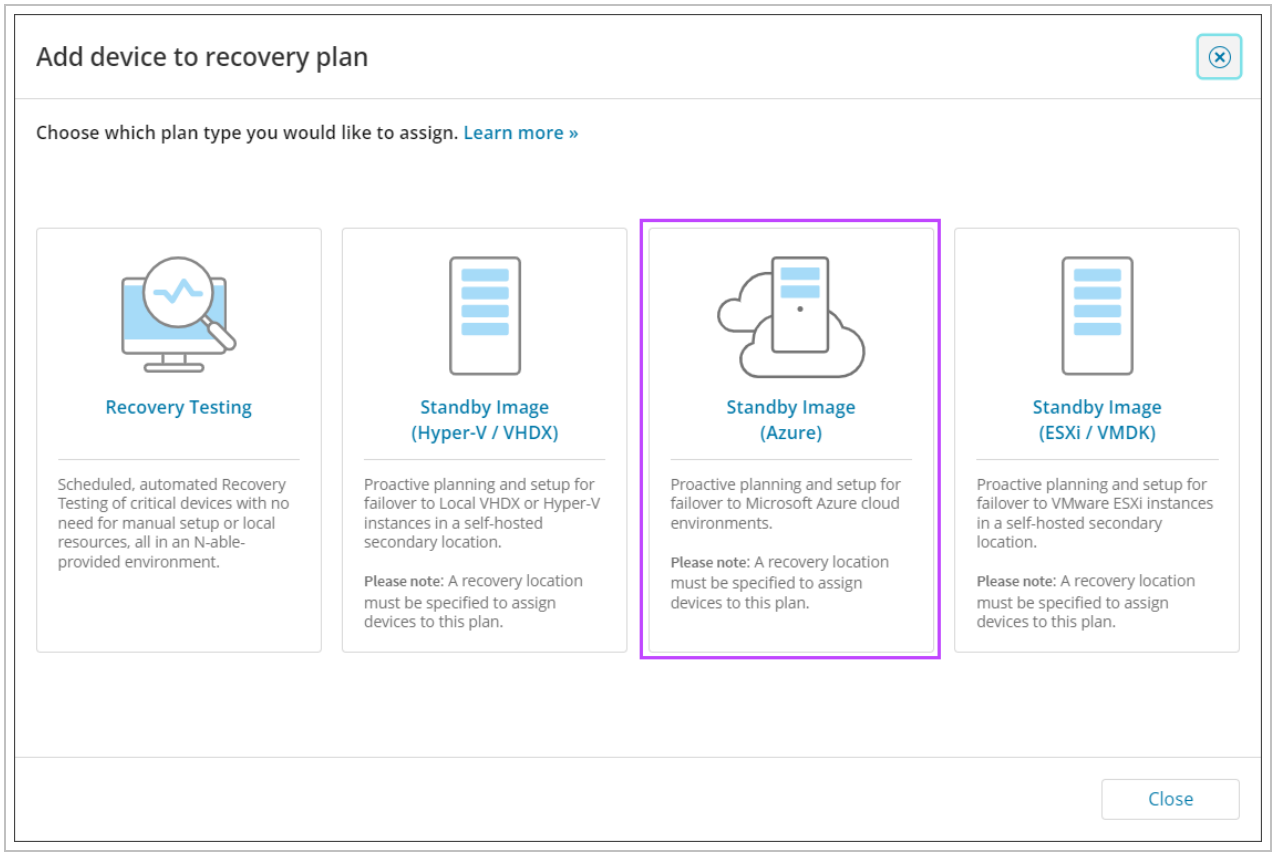
From Main Dashboard

To enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan to
3. Click **Add to recovery plan** from the Toolbar



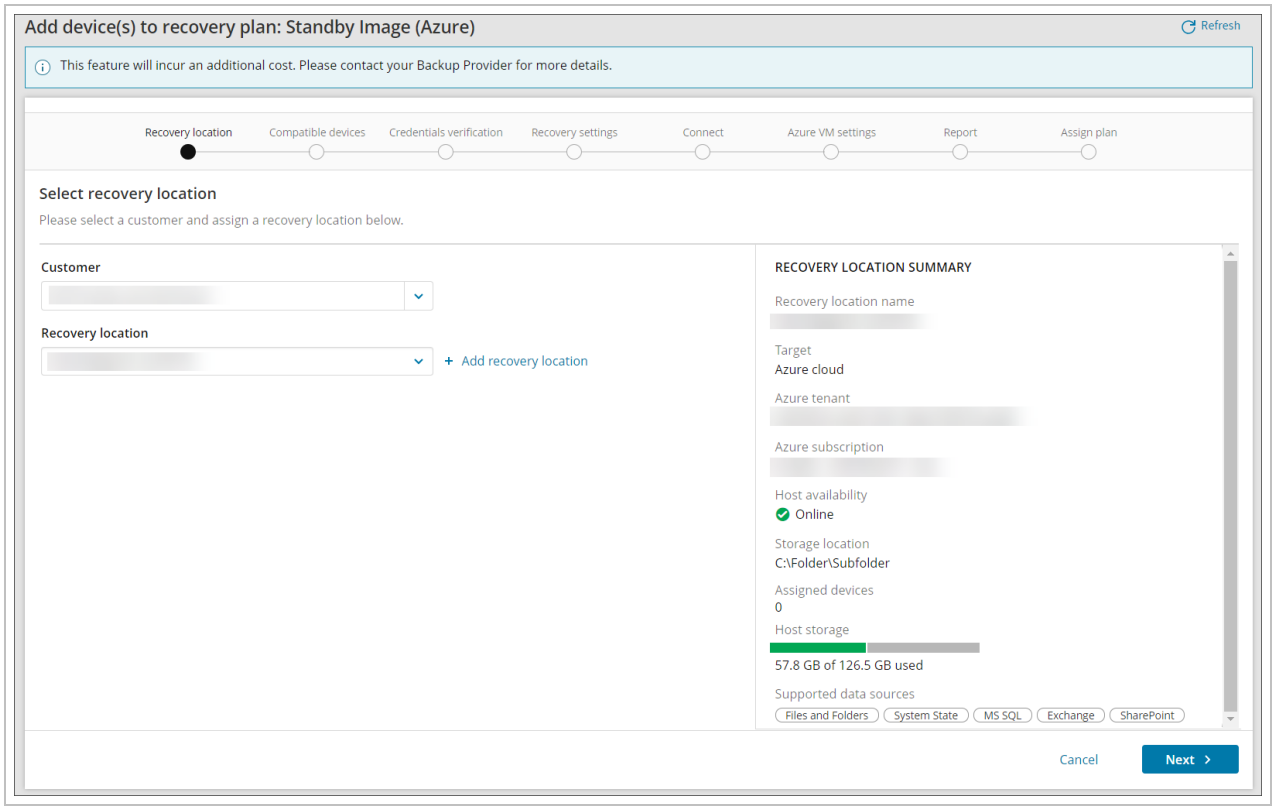
4. Select **Standby Image (Azure)**



5. Select the customer the device(s) you wish to apply the Standby Image plan belong to

6. Choose the recovery location as was configured in Add Recovery Locations

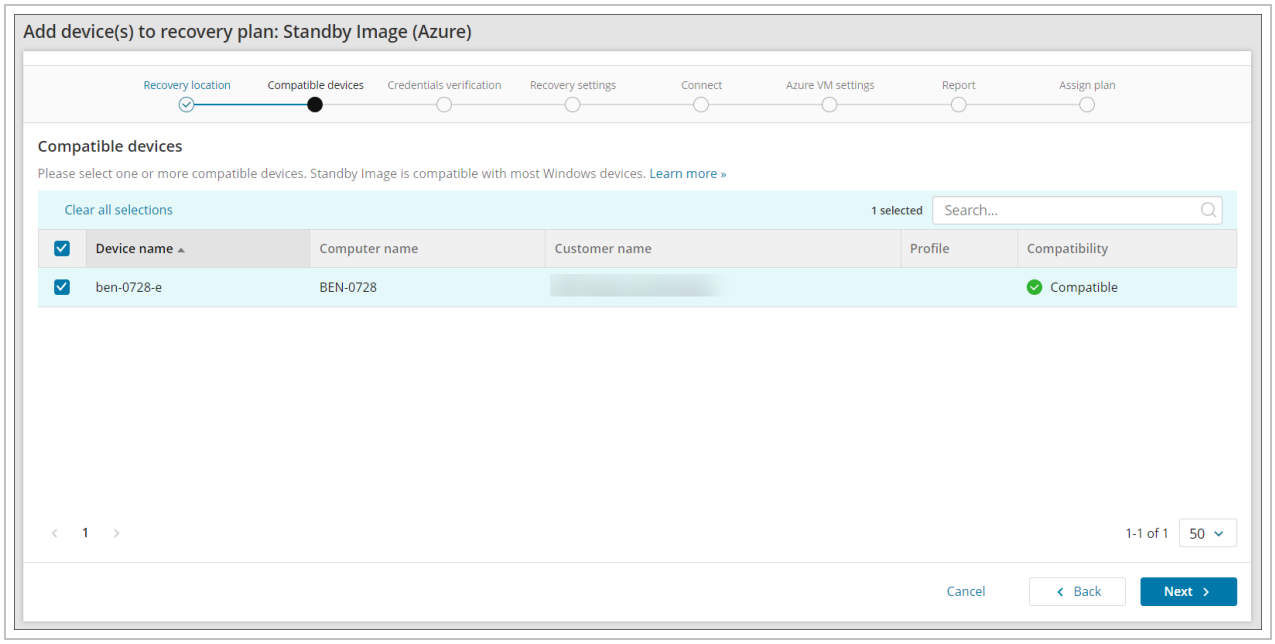
> If the selected customer does not have any locations, you must add one before continuing by selecting **Add recovery location**. See Add Recovery Locations for full details of adding a location.



> It is not possible to assign a location for which the **Host availability** is "**Offline**"

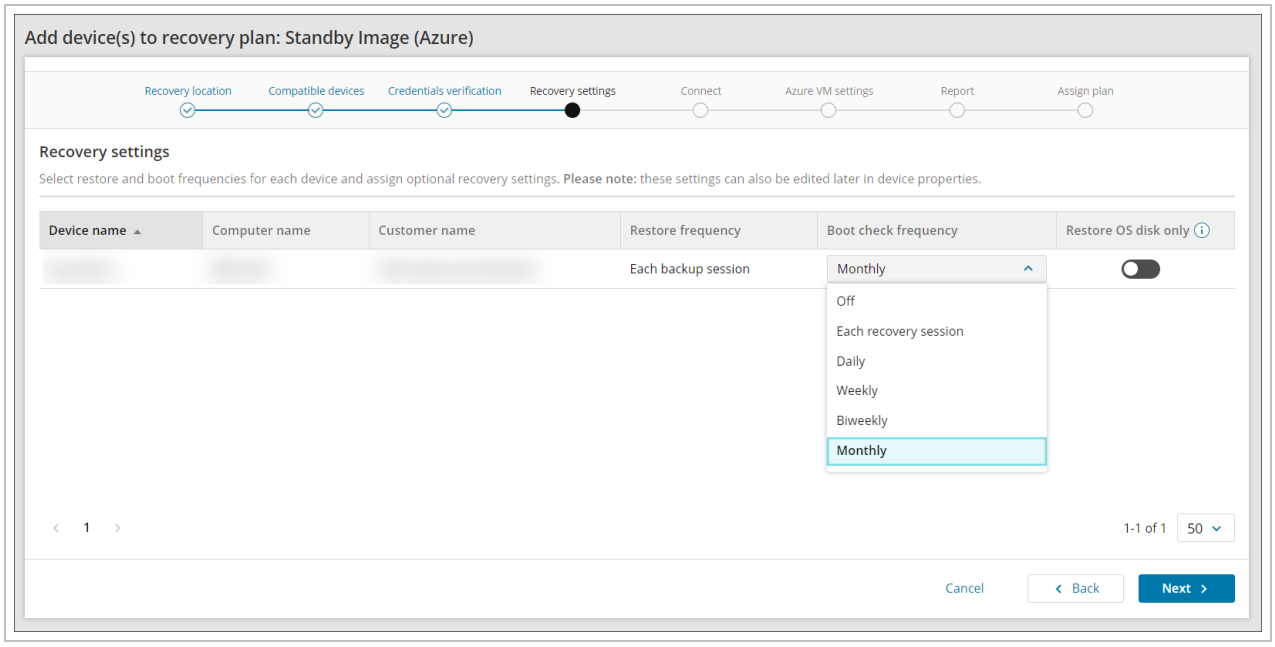
7. Click **Next**

8. Confirm the device selected from the Dashboard is compatible and click **Next**

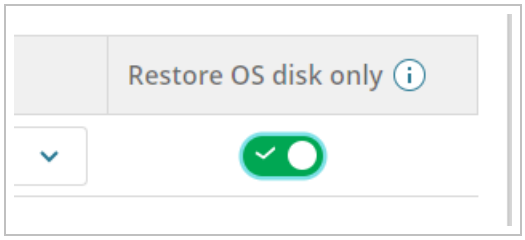


9. Enter the security code/encryption key or passphrase for the device(s). This can be either:
   - **Private encryption key** - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryption
   - **Passphrase encryption** - These are generated on demand for automatically installed devices. You can find information on this here
10. Click **Next** to continue

11. Choose the boot check frequency:
    - Off
    - Every recovery session
    - Daily
    - Weekly
    - Biweekly
    - Monthly



12. If you wish to skip all data drives, enable **Restore OS disk only**



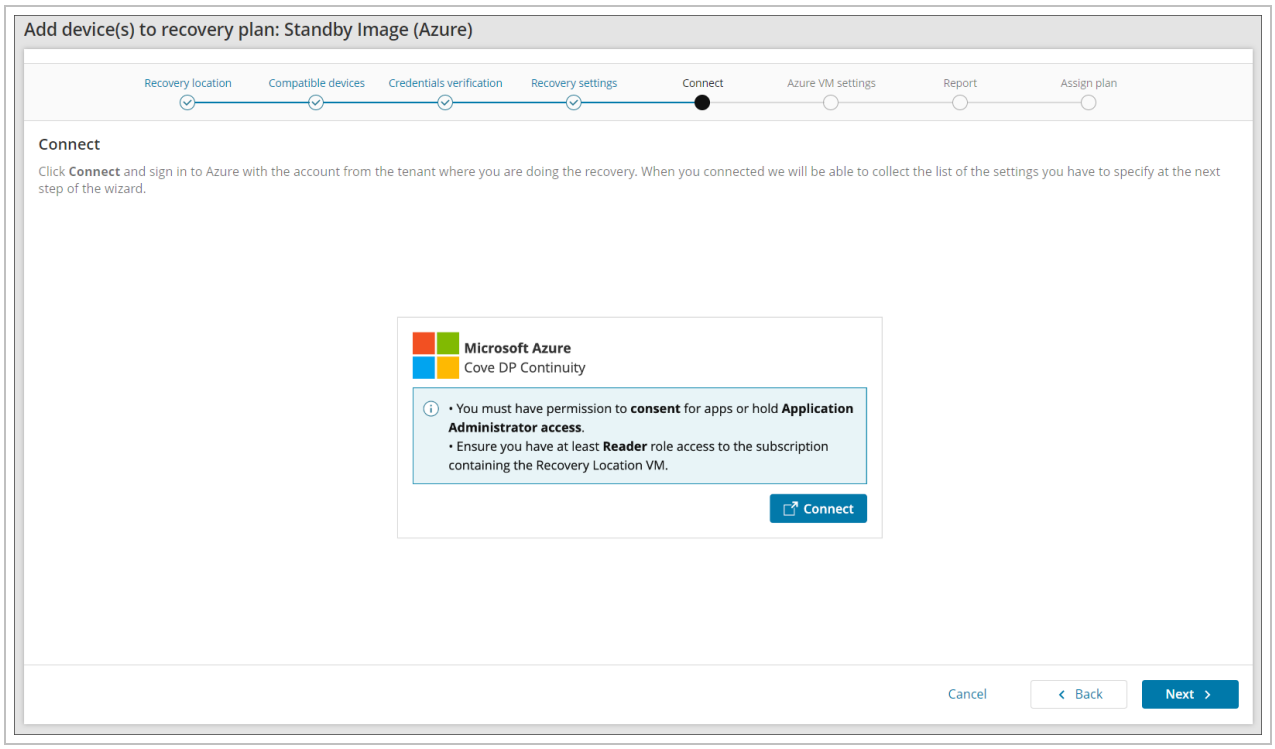
> Enabling **Restore OS disk only** will help to speed up restores as the only thing being restored is the Operating System

13. Click **Next**

14. Connect to Microsoft Azure by either:
    a. Allow permissions to the Azure user account to **consent for apps** access,

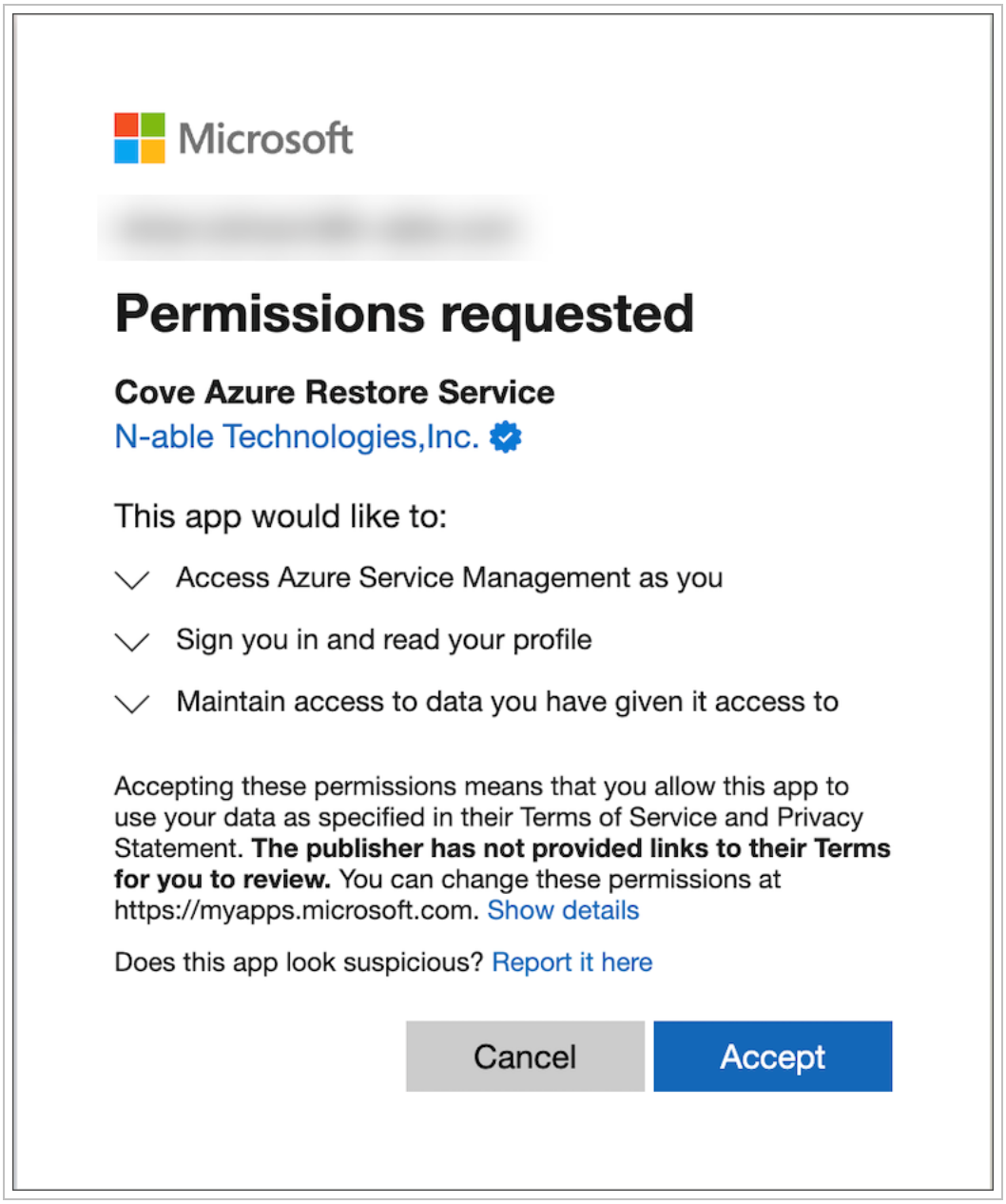
or;

    a. Login using Application Administrator access



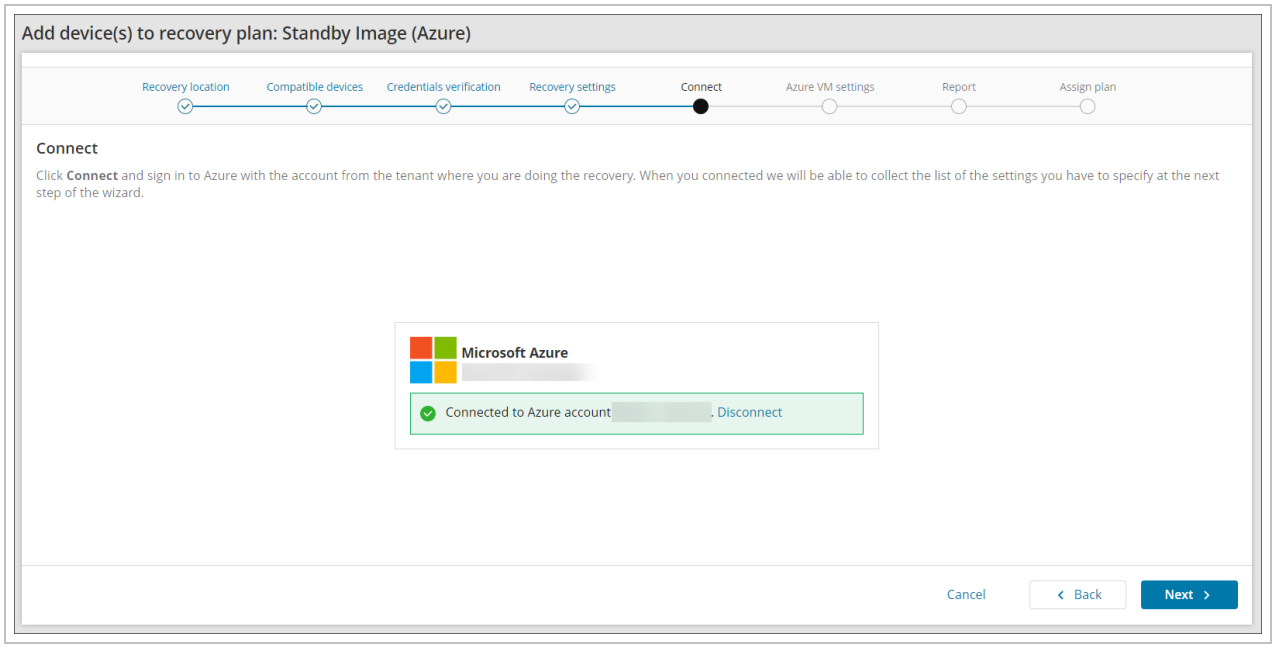
> Ensure you have at minimum **Reader** role access to the subscription containing the Recovery Location VM

b. Accept the required permissions



If you do not see the authentication page, make sure your browser is not blocking pop-up windows.

15. Once connected, click **Next**



16. Click **Azure VM settings** towards the right-hand side of the screen to open the settings configuration window:

17. Configure the **Azure VM Settings:**

AZURE VM SETTINGS

Subscription

Resource group

Virtual machine name

Region

West Europe

Availability options

VM size

OS disk type

Premium SSD

Data disk(s) type

Premium SSD

Virtual network

Subnet

default

Assign NSG and public IP

- Subscription

  > This cannot be changed as the subscription is set in the **Recovery Location** configuration

- Resource Group
- Virtual Machine name
- Region

  > This cannot be changed as the subscription is set in the **Recovery Location** configuration

- Availability options
- VM size

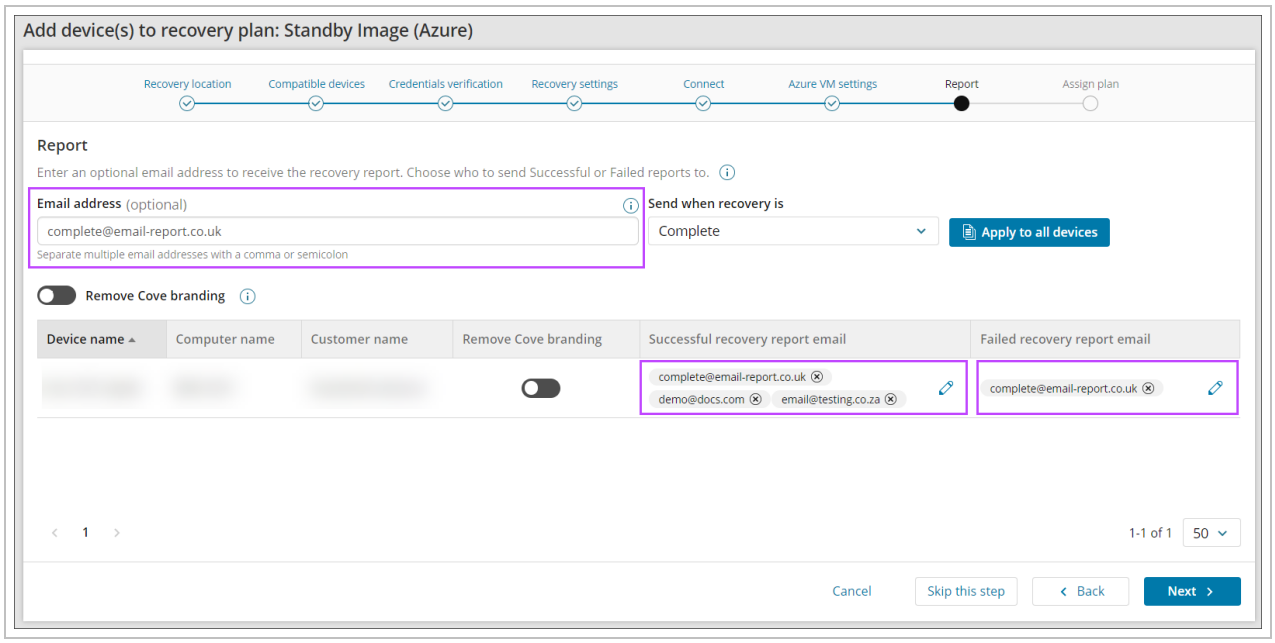
  > If the **VM size** selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either **increase** the **regional vCPU quota** on the Subscription, or **decrease** the **VM size** selected in the Azure VM Settings.

- OS disk type
- Data disk(s) type
- Virtual Network
- Subnet
- Assign NSG and public IP

> During the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend **blocking internet access** for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.

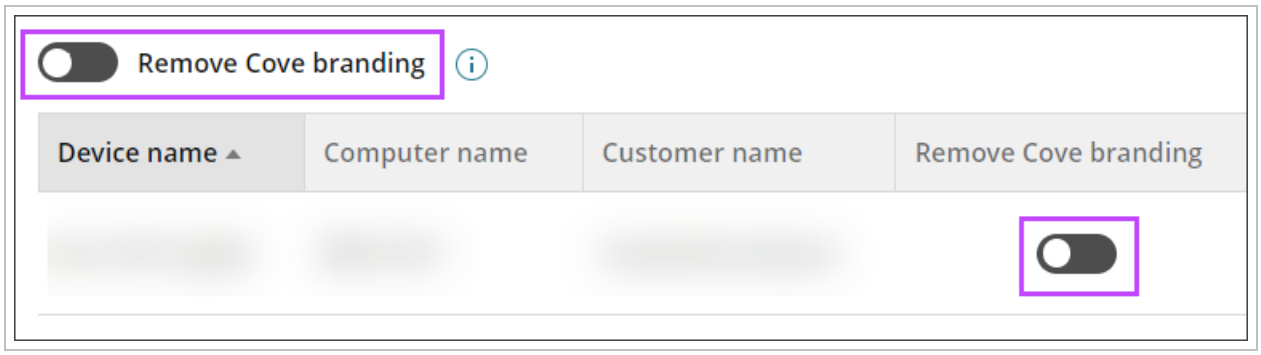
18. Click **Next** to progress to the **Report** window to enter one or more email addresses to receive a report when:
    a. The recovery is complete (Successful or Failed)
    b. The recovery was successful
    c. The recovery failed

> Multiple addresses should be separated using a comma or semi-colon



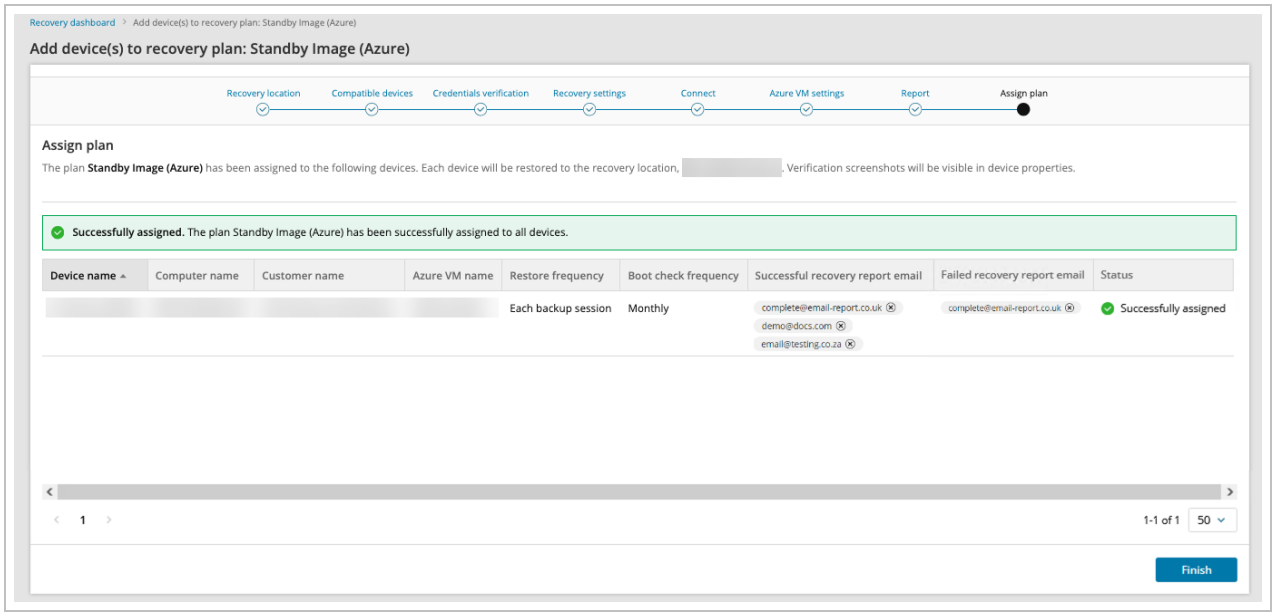
> If you do not want to add an email address to receive reports, click **Skip this step**

19. To remove all branding from the reports, use the **Remove Cove branding** toggle per device, or above the device list to apply the changes to all devices in this window



20. Confirm assigning the plan to the device(s)

21. Wait for the plan to be assigned until you see a confirmation banner on the page

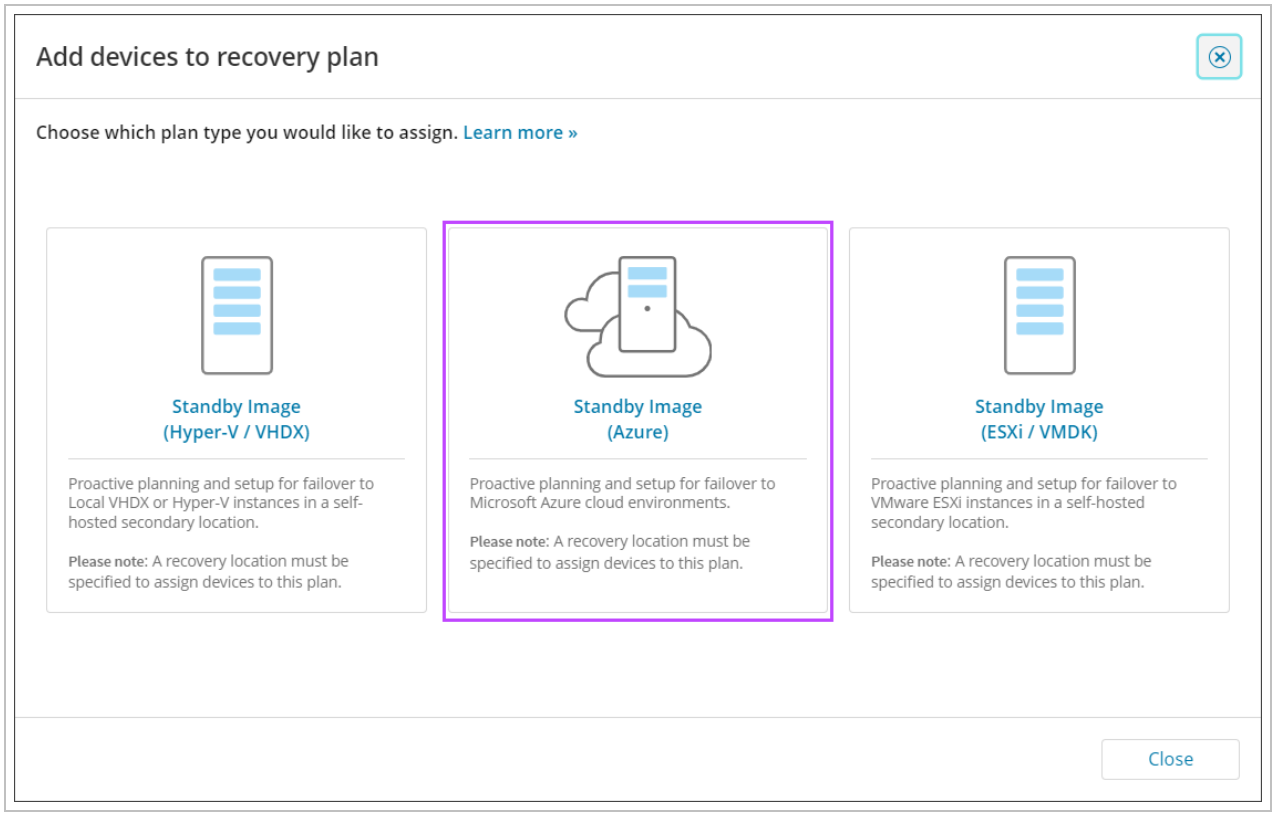


22. Click **Finish**

From Standby Image Overview

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Click **Add to Plan**

4. Select **Standby Image (Azure)**



5. You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the plan

Recovery Reports

When the device(s) assigned to the plan have **Successful recovery report email** or **Failed recovery report email** recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox.

Here is an example report **with** Cove branding:

Cove Data Protection

Recovery completed

Recovery plan: **Standby Image (Azure)**

Last recovery session completed successfully: April 05 2023 2:16:28 AM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Workstation
Operating system	Windows 10 Pro (19044), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 05 2023 2:16:28 AM
Recovery status	Completed
Recovery duration	1 minute and 57 seconds
Recovery location	pt-az-recovery-agent-1-0e70b668
Boot frequency	Each recovery session
Restore frequency	Each backup session
Recovery plan	Standby Image (Azure)
Screenshot verification	Completed

BACKUP DETAILS USED FOR THE RESTORE

Backup session time	April 05 2023 2:01:02 AM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

Below is a screenshot of the virtual machine created during the boot phase of recovery.

Here is an example **without** Cove branding:

Recovery completed

Recovery plan: **Standby Image (Azure)**

Last recovery session completed successfully: April 05 2023 2:16:28 AM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Workstation
Operating system	Windows 10 Pro (19044), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 05 2023 2:16:28 AM
Recovery status	Completed
Recovery duration	1 minute and 57 seconds
Recovery location	pt-az-recovery-agent-1-0e70b668
Boot frequency	Each recovery session
Restore frequency	Each backup session
Recovery plan	Standby Image (Azure)
Screenshot verification	Completed

BACKUP DETAILS USED FOR THE RESTORE

Backup session time	April 05 2023 2:01:02 AM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

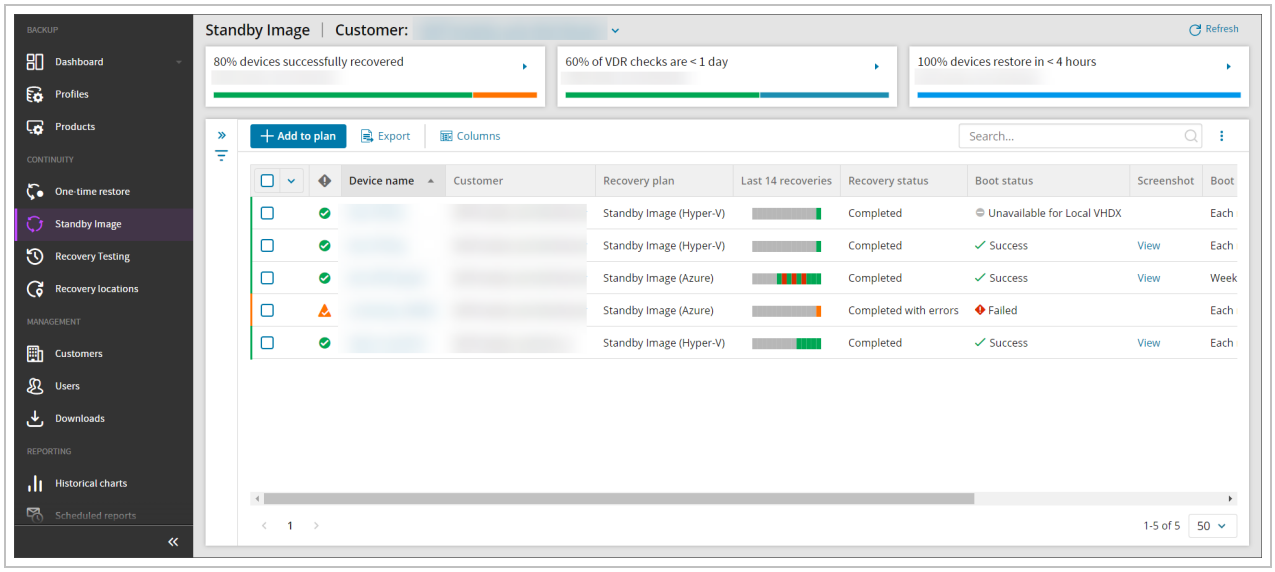
Below is a screenshot of the virtual machine created during the boot phase of recovery.

Monitor Standby Image Devices

From the Management Console, you can view the dedicated Standby Image Overview by selecting **Continuity** > **Standby Image** from the vertical menu on the left hand side.

This page will list devices assigned to the Standby Image plans:

- Standby Image to Hyper-V
- Standby Image to Azure
- Standby Image to ESXi



From this dashboard, you will see a specified set of columns detailing information relevant to devices using the Standby Image plan, including the continuity history of the last 14 recoveries, the recovery status, boot status, and plan assigned, along with some other information.

If no devices are assigned to either Standby Image plan, the dashboard will display a message to advise, along with a button to add devices to a plan.

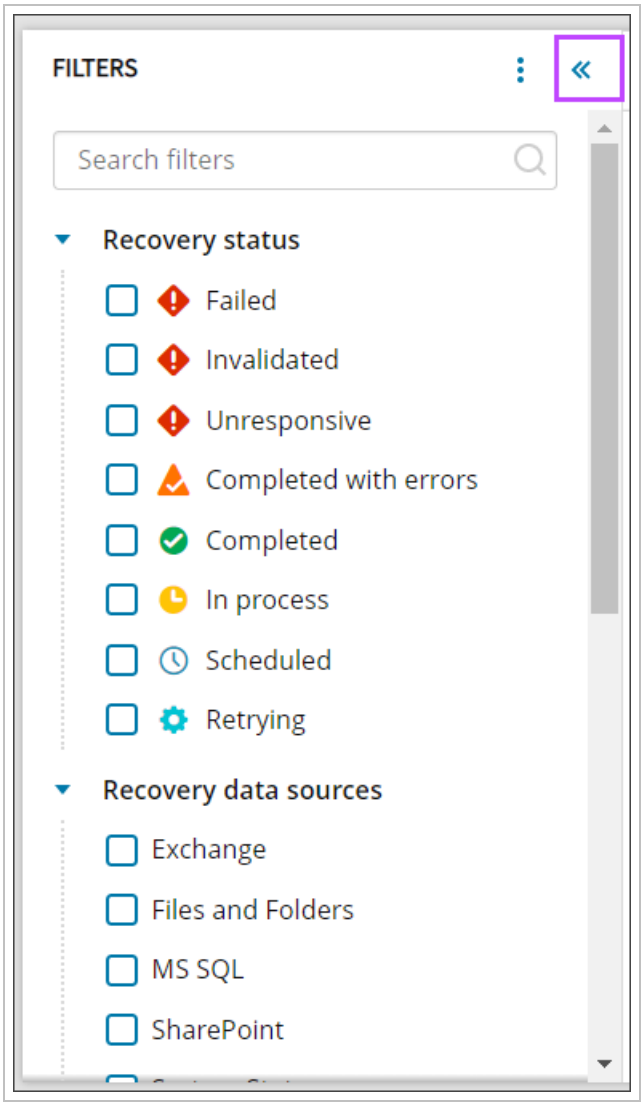
> If a device is assigned to **multiple** plans (i.e. **Standby Image to Hyper-V**, **Standby Image to Azure** and **Standby Image to ESXi**), the device will be listed for each instance of a plan and can be told apart by the **Recovery Plan** column.

Searching

Searching within the Standby Image overview can be done by using the search box over to the right hand side of the page, just above the devices list. The search can be performed by any text field.

Filtering

The Standby Image overview also includes functionality to filter devices using the filter menu to the left of the device list and can be displayed or hidden by clicking the double arrows.



From this menu, you can filter by:

Recovery status

- **Failed** - The recovery session has failed
- **Invalidated** - Device was moved to an inappropriate partner and so the session has failed
- **Unresponsive** - The recovery session was initiated but did not receive updates for at least 30 minutes because the recovery location restarted or was offline.
- **Completed with errors** - The recovery session completed, but encountered errors
- **Completed** - The recovery session completed with no errors
- **In process** - The recovery is currently in progress
- **Scheduled** - Devices just added to a recovery plan and are waiting for their first recovery session or devices where restores were paused and have since been resumed will display as scheduled
- **Retrying** - A restore session was not finished so the system is trying the restore again

Recovery data sources

- Exchange
- Files and Folders
- MS SQL
- SharePoint
- System State

Recovery session statistics

- Boot check frequency
  - Off
  - Every recovery session
  - Daily
  - Weekly
  - Biweekly
  - Monthly
- Boot Check Status
  - Success
  - Failed
  - Off
  - Unavailable for Local VHDX
- Continuous restores
  - Running
  - Paused
- Duration of the last completed recovery session
  - Sliding scale from 0 to unlimited

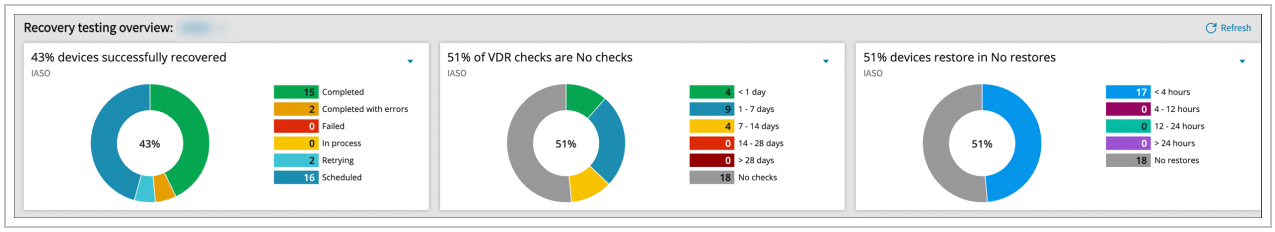
  in minutes
- Number of errors of the last completed recovery session
  - Sliding scale from 0 to unlimited
- Number of restored files
  - Sliding scale from 0 to unlimited
- Number of selected files
  - Sliding scale from 0 to unlimited
- Recovery Location name
  - Select the recovery location from a dropdown
- Recovery Plan
  - Standby Image (Hyper-V)
  - Standby Image (ESXi)
  - Standby Image (Azure)
- Restored size
  - Sliding scale from 0 to unlimited

  in KB and GB

- Recovery testing status of the last completed recovery session
  - Failed
  - Completed with errors
  - Completed
- Screenshot
  - Available
  - Not Available
- Selected size
  - Sliding scale from 0 to unlimited
  in KB and GB
- Timestamp of the last completed recovery session
  - Quick Picks of:
    - Last day
    - 1 - 7 days
    - 7 - 14 days
    - 14 - 28 days
    - > 28 days
  - Custom range, select a stat date and time and an end date and time

Widgets

Three widgets can be maximized at the top of the page, which allow for further filtering:



Device recovery status

This widget allows you to filter the devices by recovery status:

- Completed
- Completed with errors
- Failed
- In process
- Retrying
- Scheduled

VDR checks time frame

This widget allows you to see the percentage of devices whose recovery check completed within the following day ranges:

- < 1 day
- 1 - 7 days
- 7 - 14 days
- 14 - 28 days
- > 28 days
- No checks

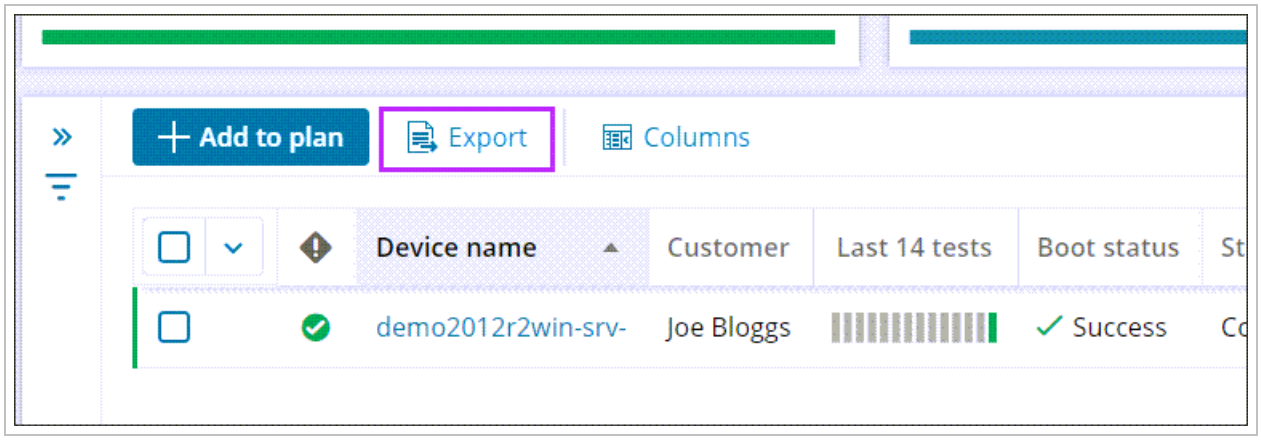
Device restore time frame

From this widget, you can filter devices by the how recent restores are done by the following time frames:

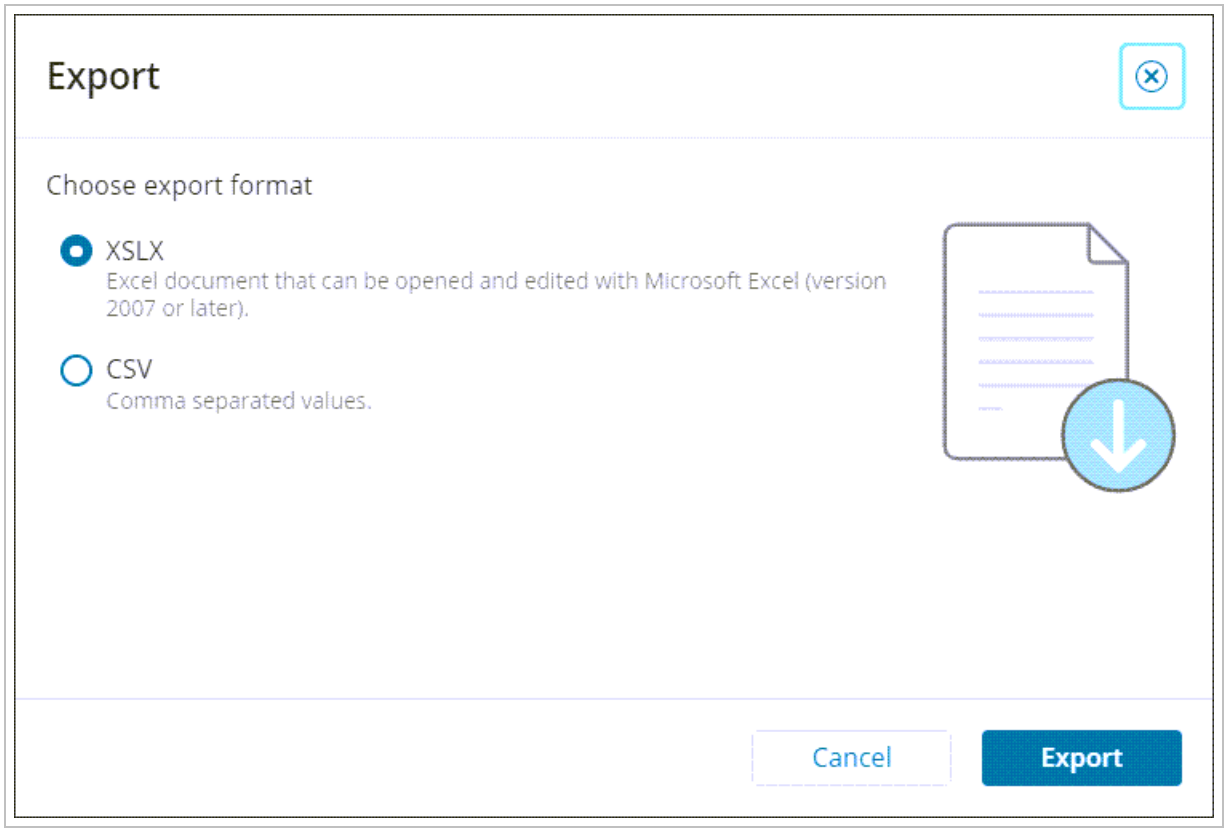
- < 4 hours
- 4 - 12 hours
- 12 - 24 hours
- > 24 hours
- No restores

Exporting

You may export a list of devices currently assigned a plan by clicking **Export**

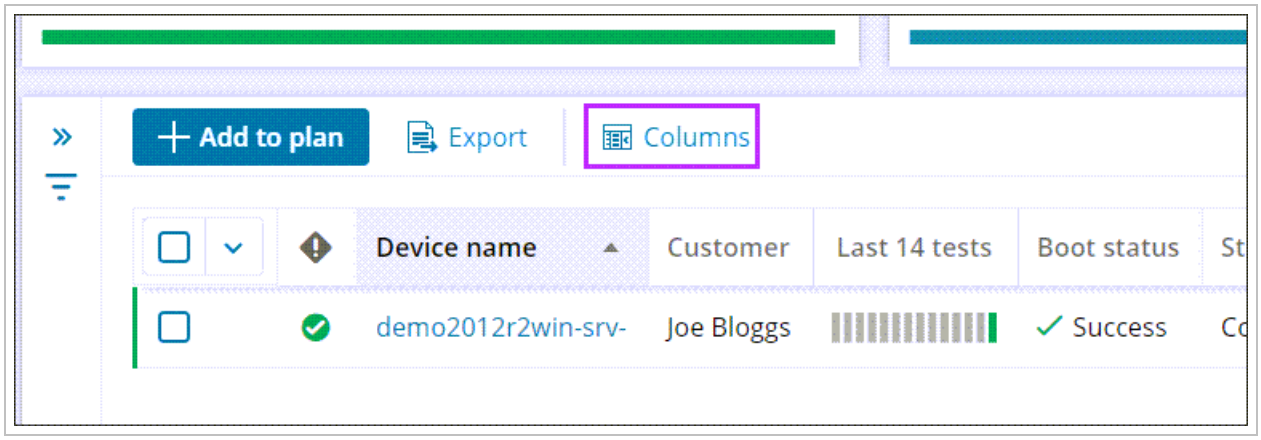


This will then provide a separate dialog where you can choose to export in either XSLX or CSV.

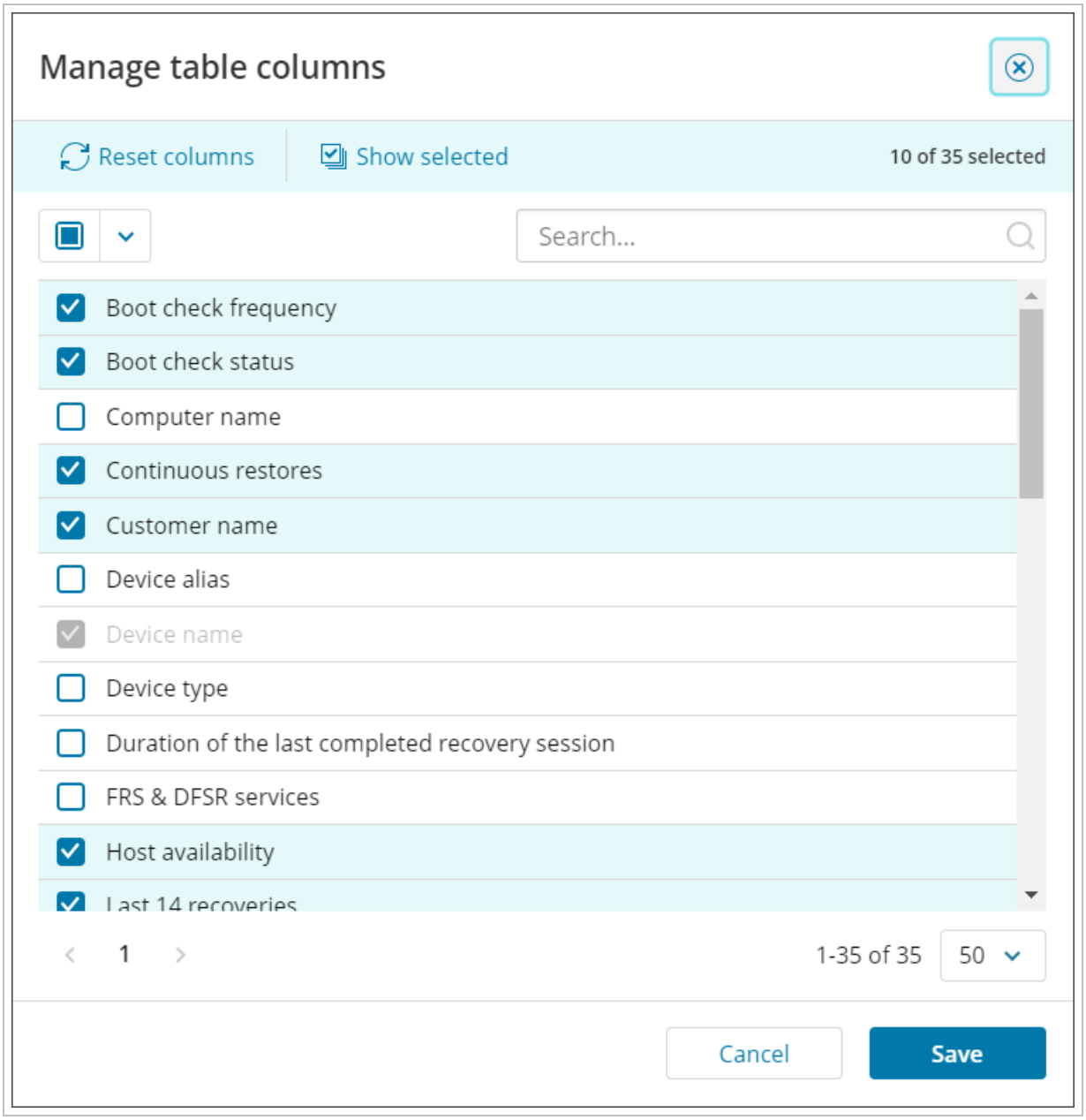


Manage Table Columns

Management Console allows you to manage the tables columns that can be seen within the Standby Image overview.



In the Manage table columns dialog, you can select and deselect columns based on the information you wish to view from the overview.

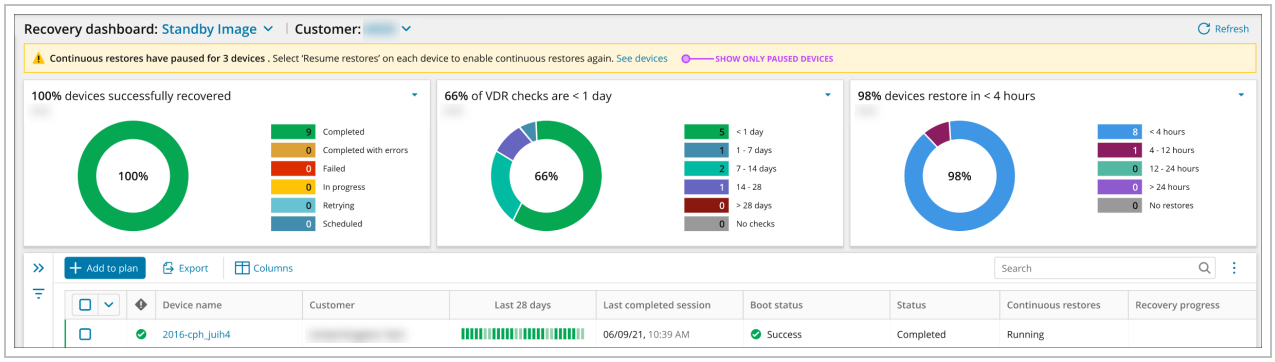


Pause Standby Image recovery

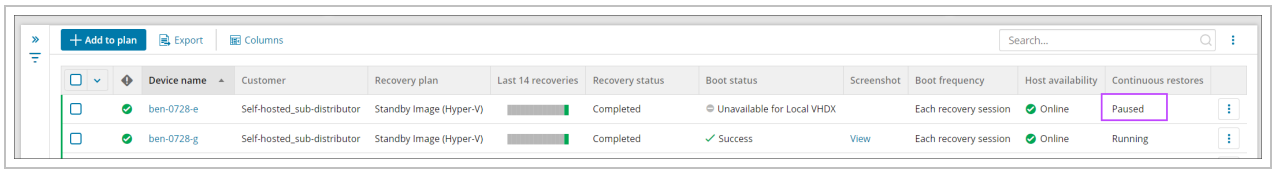
Once a Standby plan has been assigned to a device, the continuous restores can be paused and restarted. Pause or resume restores functionality there to provide a possibility to use the restored machine for failover in case of disaster.

> If a restored Virtual Machine is turned on manually, the Standby Image restore will automatically pause.

Pausing and restarting continuous restores can done be for single or multiple devices at a time. Once devices have been paused, a banner will be displayed at the top of the page to advise.

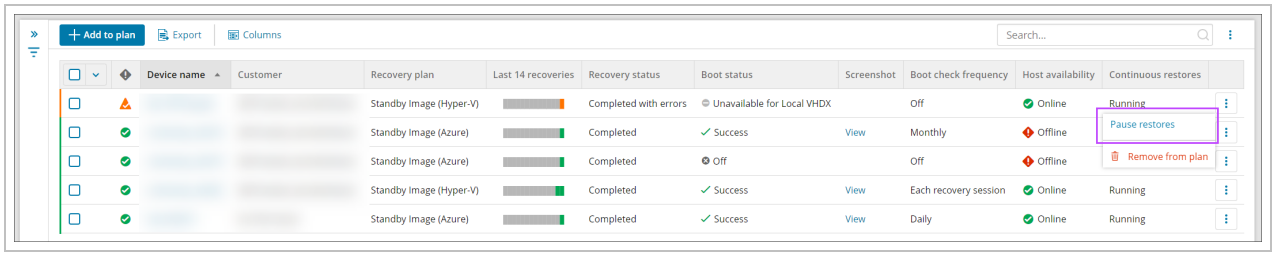


Click **See devices** to filter the devices list by **Continuous Restore: Paused** to only devices which are currently paused.



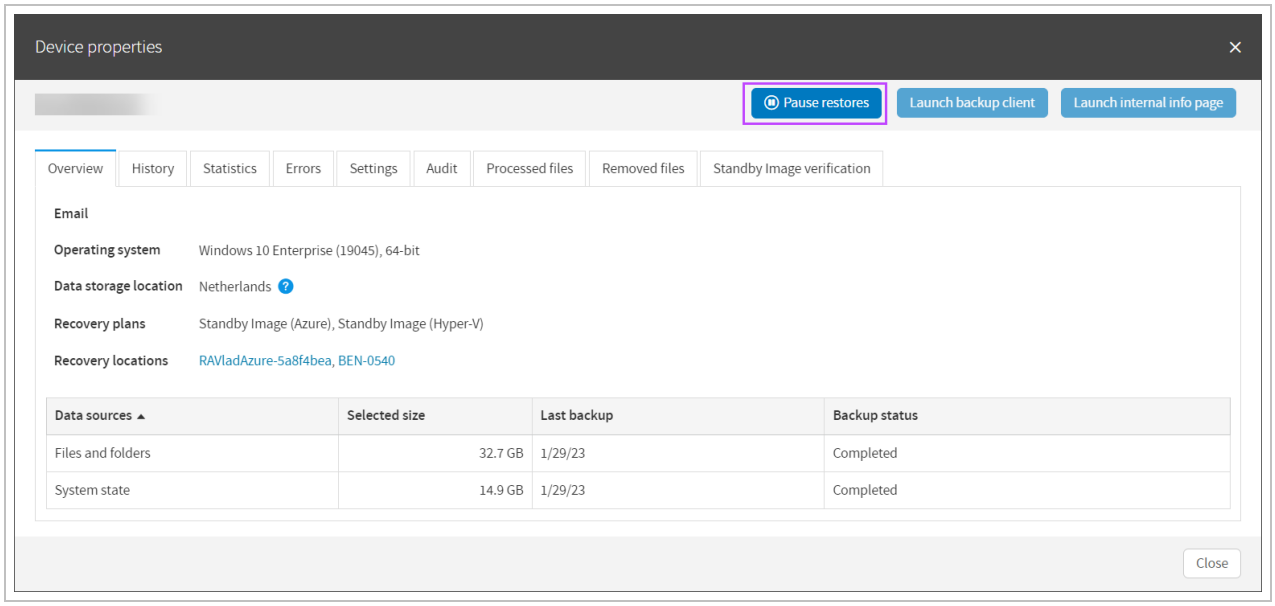
For single devices

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Click the menu action button to the right of the device (Three vertical dots)
4. Select **Pause Restores** or **Resume Restores**



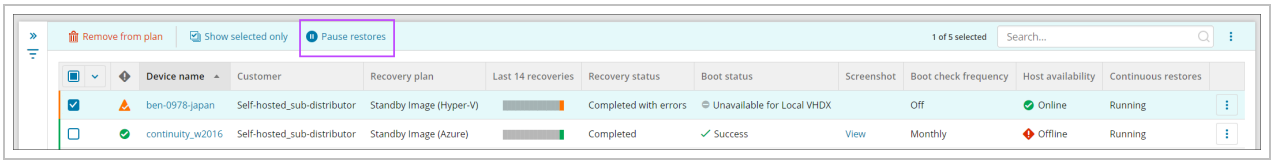
> This will differ depending on whether the plan is currently active, or has been paused already

It is also possible to pause restores from the Device Properties window:



For single or multiple devices

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Tick the checkbox for any devices that need paused from the list
4. In the top panel, select **Pause Restores** or **Resume Restores**



> This will differ depending on whether the plan is currently active, or has been paused already

Accessing device properties

The Device Properties window displays several tabs detailing information on the Backup device. Full details of the contents of each tab can be found on the Device management in Management Console page.

The two that are the most commonly used with Standby Image are the **Settings** tab and the **Standby Image Verification** tab.

Settings Tab

Broken into several sections, this tab contains:

General

This section provides the main device details:

- **customer** - Who device belongs to, can be changed to move the device to a different customer
- **Device name** - Cannot be changed

- **Installation key** - Cannot be changed
- **Creation date** - Cannot be changed
- **Expires on** - Can be amended to a date in the future, or set to **'no expiration'** if required

> You may also see the Request Passphrase button here if the device is set up to use this instead of its own security code/encryption key

Backup

This section contains:

- **Backup product** - Use the dropdown to change the Product used by the device
- **Profile** - Use the dropdown to change the Profile applied to the device

Recovery

On a device assigned to the Standby Image plan, this section will allow you to see plan in use and amend some details of this:

- **Recovery Plan** - Standby Image (Each backup session)
- **Recovery Location** - Cannot be changed from this panel. To change this, see Add Device to Recovery Location
- **Successful recovery report email** - Specify the email address(es) that will receive reports when the most recent Recovery as per the assigned plan has been successful
- **Failed recovery report email** - Specify the email address(es) that will receive reports when the most recent Recovery as per the assigned plan has failed
- **Remove Cove branding** - toggle branding of the email reports on or off
- **Restore format** - This option will not be available for Standby Image to Azure.
  - For **Standby Image to Hyper-V**, this is a choice between **Hyper-V** or **Local VHDX**
  - For **Standby Image to ESXi**, this is a choice between **ESXi** and Local **VHDX**

    > Further settings displayed are dependent on the Restore Format selected for the device. These settings can be changed as required.

> All Recovery Plans associate to the device will be included here, and can be minimized or expanded by clicking the arrow to the left of the plan name.

Device properties

Launch backup client | Launch internal info page

Overview | History | Statistics | Errors | Settings | Audit | Processed files | Removed files | Standby Image verification

General

Customer

Device name

Installation key

Creation date 2/21/23

Expires on 04/18/24 No expiration

Backup

Product _test

Profile -servers

Recovery

Standby Image (ESXi)

Recovery plan Standby Image (ESXi)

Recovery location ESXiRA

Successful recovery report email e.g email@email.com

Failed recovery report email e.g email@email.com

Remove Cove branding OFF

Restore format ESXi VMDK

Boot check frequency Daily

FRS and DFSR services OFF

Local Speed Vault OFF

CPU cores 4

RAM (GB) 4

VM Subnet mask Enter a custom subnet mask to the new virtual mac

VM gateway Enter a custom gateway to the new virtual machine

VM DNS server Enter a DNS server to be used on the restored mach

Separate multiple DNS servers with a comma or semicolon

VM IP address Enter a custom IP address to the new virtual machir

Standby Image (Hyper-V)

Recovery plan Standby Image (Hyper-V)

Recovery location BEN-6478

Successful recovery report email e.g email@email.com

Failed recovery report email e.g email@email.com

Remove Cove branding OFF

Restore format Hyper-V Local VHDX

Boot check frequency Daily

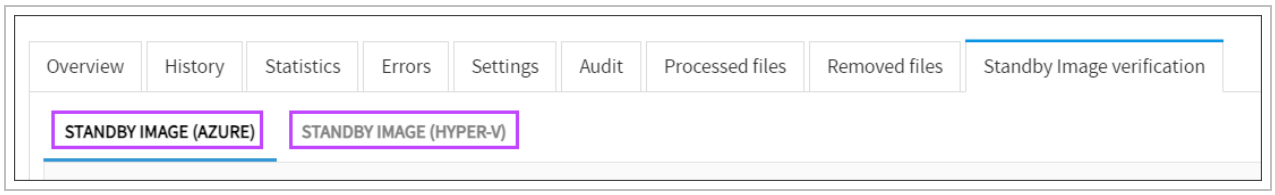
FRS and DFSR services OFF

Local Speed Vault OFF

Standby Image Verification Tab

To view statistics of the Standby Image and check the screenshots to ensure this has been successful, you can view this by following one of the below methods.

All plans associated to the device will have their own sub-tabs that can be selected to view the appropriate screenshot:



From Device Properties

1. Log in to the Management Console
2. Click the device name on either the Backup Dashboard or the Standby Image overview to open the Device Properties
3. Navigate to the **Standby Image Verification** tab

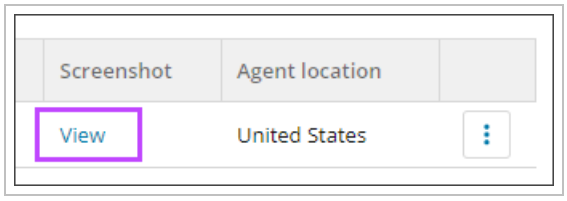
From Standby Image Overview

The Standby Image Verification tab can be viewed from the Standby Image overview in one of two ways:

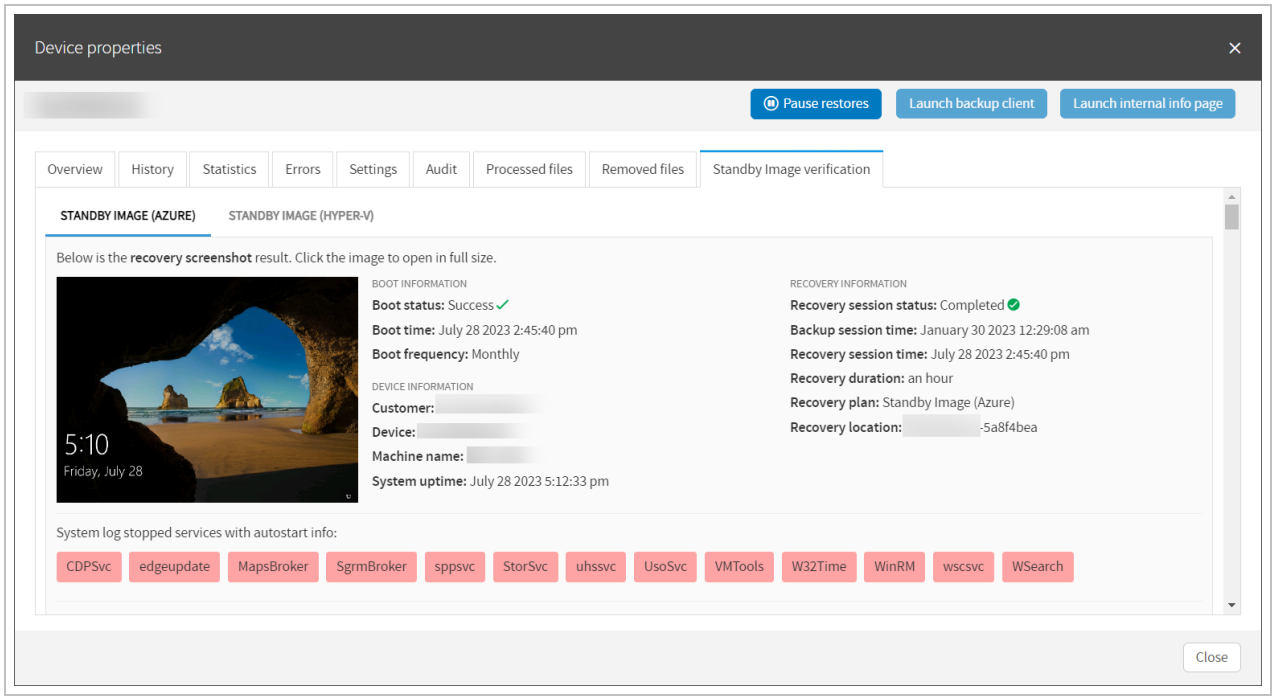
- Via theScreenshot column
- Via the Last 14 recoveries column

Screenshot column

1. Log in to the Management Console
2. Navigate to **Continuity** > **Standby Image**
3. Click **View** under the Screenshot column

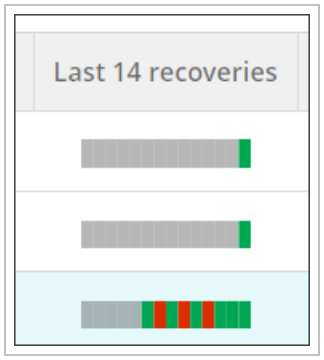


4. This will take you in to the Device Properties dialogue, where you will now see the **Standby Image Verification** tab:

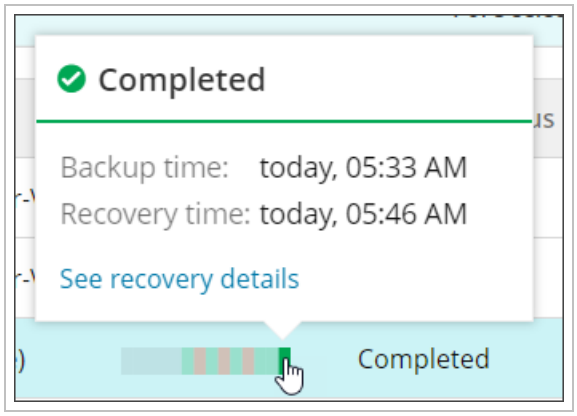


Last 14 recoveries column

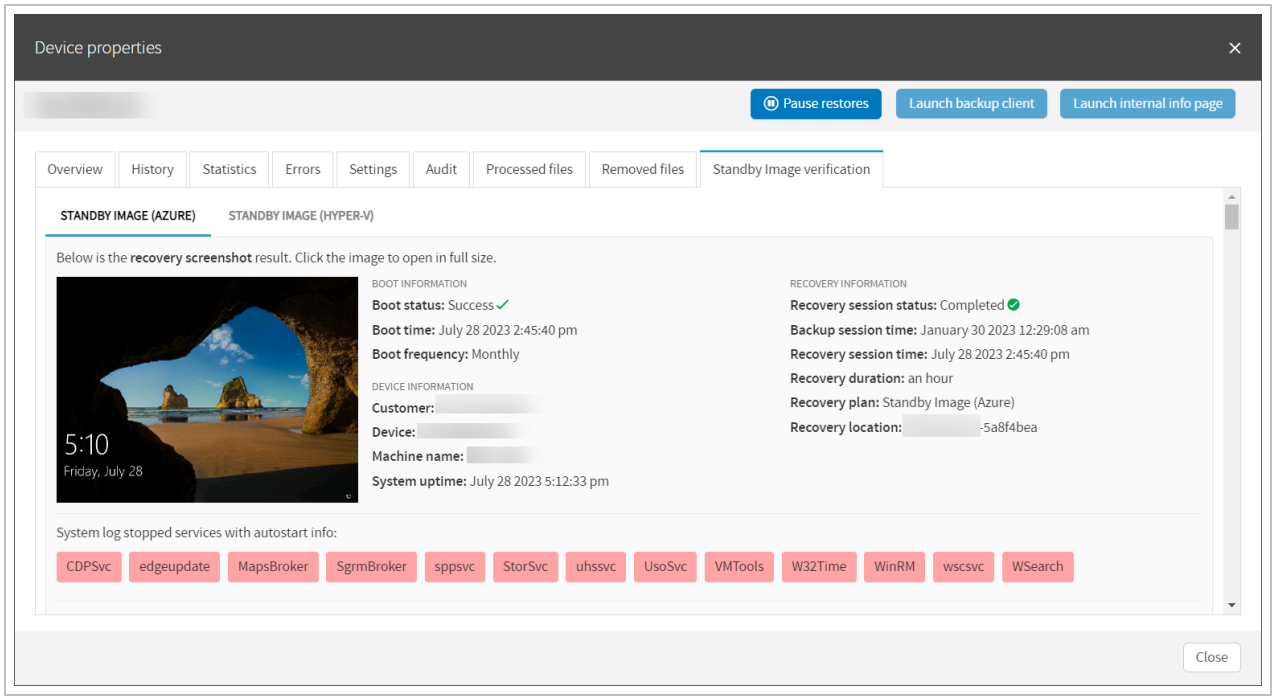
1. Log in to the Management Console
2. Navigate to **Continuity** > **Standby Image**
3. Hover your mouse over the most recent colored bar in the Last 14 recoveries column



4. Click **See recovery details** in the popup box that appears



5. This will take you in to the Device Properties dialogue, where you will now see the **Standby Image Verification** tab:



Standby Image to ESXi

Cove Data Protection (Cove)'s Standby Image to ESXi service runs a continuous restore of your data to VMWare ESXi and boots based on the frequency set during configuration of the plan.

> Devices **can** be assigned to **multiple Standby Image plans** at once, i.e. Standby Image to Hyper-V *and* Standby Image to Azure *and* Standby Image to ESXi.

> Restores can be performed to either a VMWare ESXi instance or to a Local VMDK file. Local VMDK files can be restored to either a Local Drive, or to a Network Share (NAS).

Standby Image Data Restored:

The following data sources are supported and restored to the ESXi recovery location given that they are selected for backup in the Product, or data source selection:

- System State
- Files and Folders
- Exchange
- SharePoint
- MS SQL

Requirements:

- Backup Manager version 17.4 and newer
- Devices and Recovery Locations must belong to the same Customer
- A Cove Data Protection (Cove) SuperUser or Manager account
- Recovery Locations must be added to the Management Console and the Recovery service must be installed on the recovery location **before** Standby Image recovery can occur

  - Recovery Location is a machine with the recovery service installed
  - Recovery service is a service which orchestrates all the recovery jobs for Standby Images

Limitations

- Standby Image cannot be used on the RMM integrated version of Backup (Managed Online Backup) or on the N-central integrated version of Backup (Backup and Recovery)
- Standby Image is **not** available for devices with disabled 'Virtual disaster recovery' feature in an assigned Product
- 32-bit architecture is not supported
- Restores run after each backup session for System State and Files and Folders. After the first restore, a virtual machine is created and kept on the selected host/storage, then with each subsequent restore the virtual machine is updated with only new data
- For a Virtual Machine restored to ESXi host, there is an option to automatically boot it and create a screenshot to check that the Virtual Machine is bootable, then send this screenshot to the Management Console so that users can check it
- Maximum supported capacity for virtual hard disks is **64 TB** per disk
- Devices can only be assigned to **one** Recovery Location

What's inside:

Enable Standby Image to ESXi

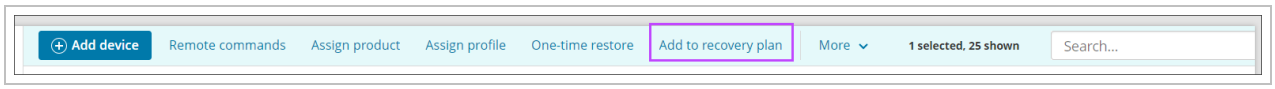
Devices **cannot** be added to a **Standby Image plan** if already assigned to a **Recovery Testing plan**.

Devices **can** be assigned to **multiple Standby Image plans** at once, i.e. Standby Image to Azure, to Hyper-V *and* to ESXi.

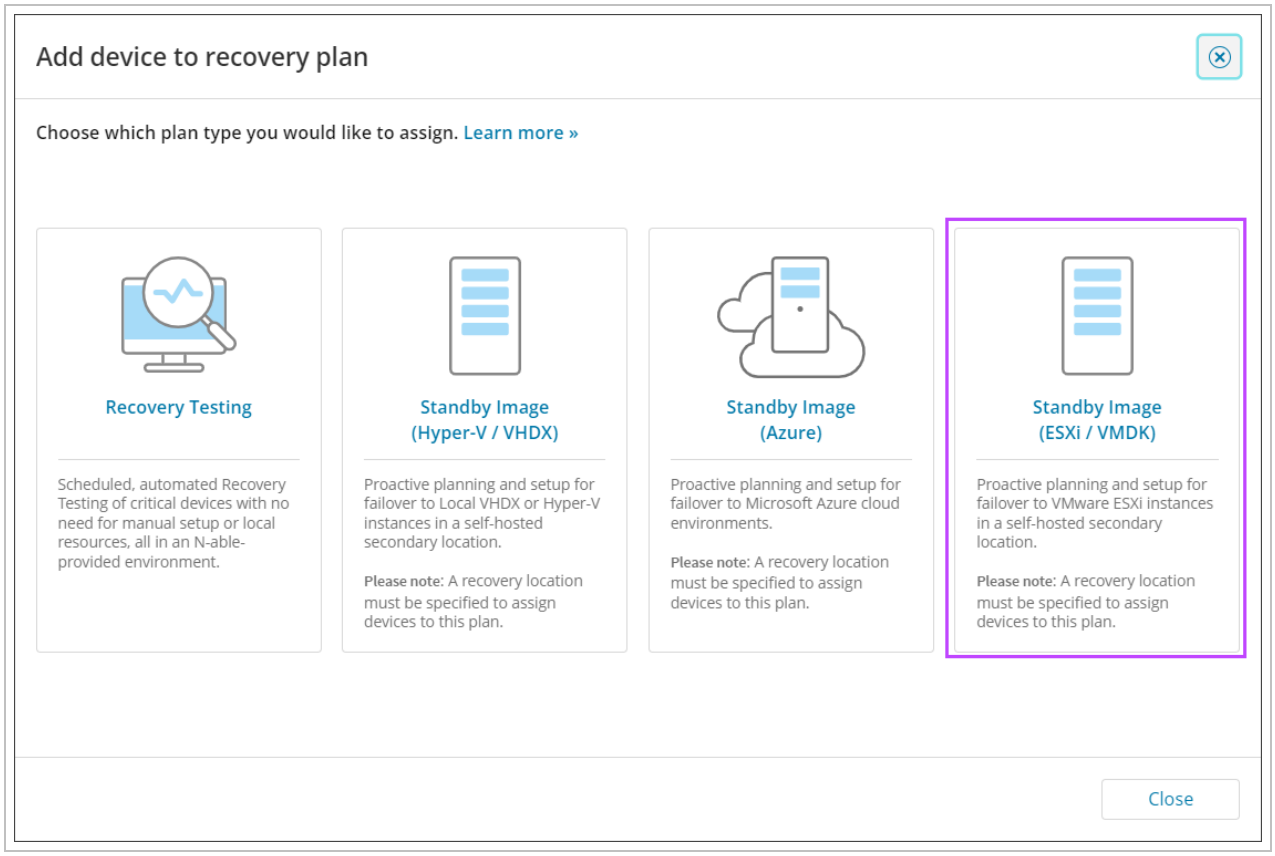
From Main Dashboard

To enable Standby Image to ESXi on a device from the Management Console's main Dashboard, follow the steps below:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan to
3. Click **Add to recovery plan** from the Toolbar



4. Select **Standby Image (ESXi)**

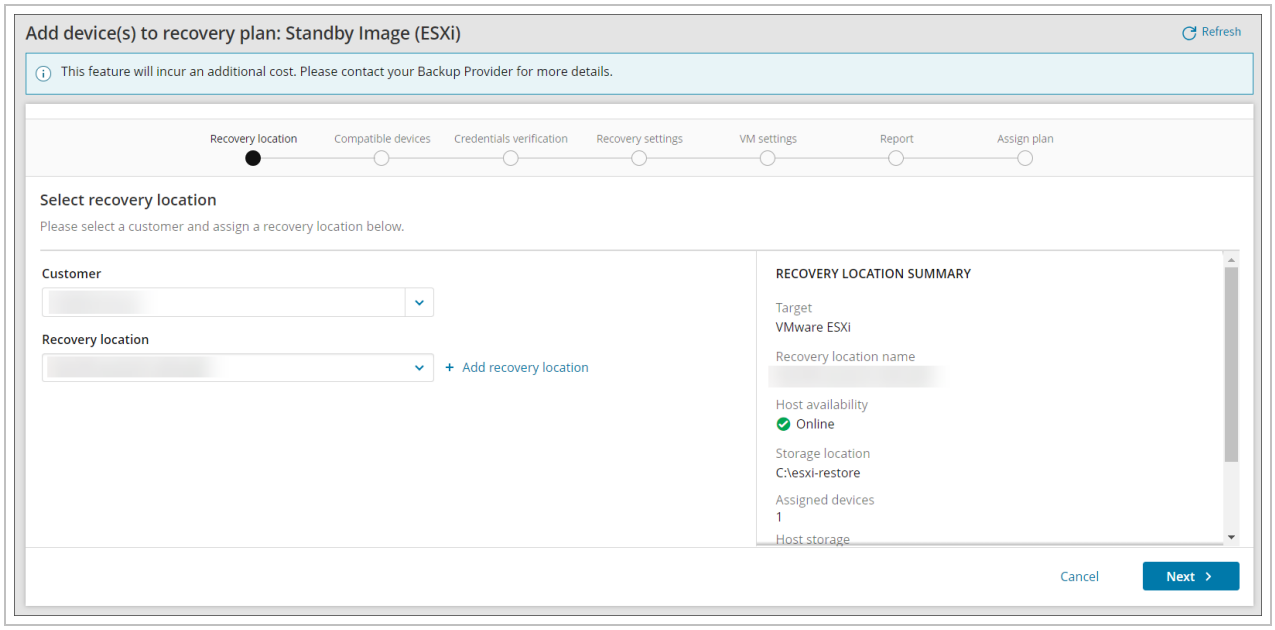


5. Select the customer the device(s) you wish to apply the Standby Image plan belong to

6. Choose the recovery location as was configured in Add Recovery Locations (ESXi)

> If the selected customer does not have any locations, you must add one before continuing by selecting **Add recovery location**.

> If the Recovery Location does not have a Storage Location, one must be provided before continuing



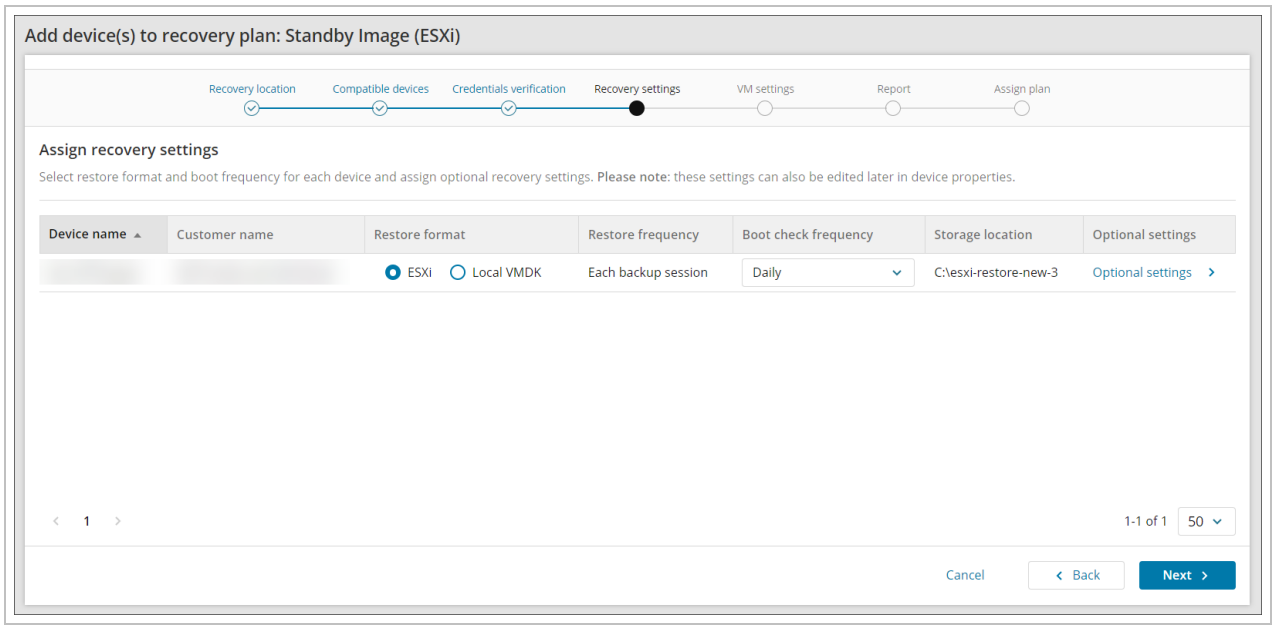
> It is not possible to assign a location for which the **Host availability** is "**Offline**"

7. Click **Next**
8. Confirm compatibility of the device(s) you want to apply the Standby Image plan on
9. Click **Next**
10. Enter the security code/encryption key or passphrase for the device(s). This can be either:
    - **Private encryption key** - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryption
    - **Passphrase encryption** - These are generated on demand for automatically installed devices. You can find information on this here

> If you are logged in as a security officer, this will be detected automatically.

11. Click **Next** to continue

12. Choose the restore format:
    - ESXi
    - Local VMDK



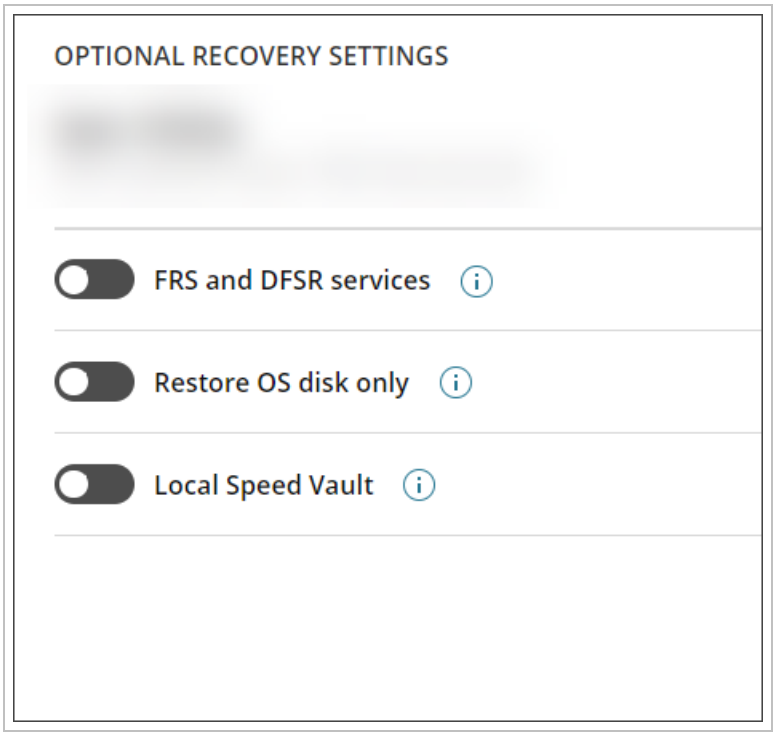
> If the Storage Location was configured as a Network Share, you will only be able to select Local VMDK as the restore format

13. Choose the boot check frequency:

> Available for **ESXi** restore format **only**, these are not available if Local VMDK is selected

    - Off
    - Every recovery session
    - Daily
    - Weekly
    - Biweekly
    - Monthly

14. Configure the **Optional Recovery Settings** for ESXi by clicking **Optional Settings** to the right of the storage location:



- **FRS and DFRS services** - If you are restoring Active Directory with multiple domain controllers, you should change the FRS and DFSR services to authoritative in the domain controller that will be started in the first place. Avoid marking several FRS/DFSR services as authoritative in the production environment as it can result in data loss. When the feature is on, the FRS and DFSR services are started on the target VM in the authoritative mode. The NETLOGON and SYSVOL shares become available, so the Active Directory and DNS services become functional again

  > More information about FRS/DFSR is available in the Microsoft Knowledge Base. Article IDs: KB2218556 and KB290762

- **Restore OS disk only** - Restoring the OS disk only will speed up restores
- **LocalSpeedVault** - If a LocalSpeedVault (LSV) is enabled on a backup device, the data is sent to both the LSV and the cloud or private storage location. During a restore, data is automatically downloaded from the LSV first to the local device which makes restore faster. If the LSV is not available or not synchronized, the restore data will be pulled from the cloud or private storage location. This takes place automatically and cannot be reconfigured

15. Click **Next** to configure the **Virtual Machine Settings**:

> Available for **ESXi** restore format **only**, these are not available if Local VMDK is selected

- **Connected Server(s)** - Select the server where the Virtual Machine will be allocated as added in Step 5: Add Storage Location and Server Connections
- **Data Center**
- **Host**
- **Storage**
- **Resource Pool**
- **Network**
- **Connect on startup** - connect to the selected network on startup
- **CPU Cores** - Select the number of CPU Cores to be allocated to the new virtual machine
- **RAM (GB)** - Select the amount of RAM in Gigabytes to be allocated to the new virtual machine
- **Source VM configuration** - When enabled, the same CPU and RAM settings as used on the source VM will be applied
- **VM IP address** – Assign a custom IP address to the virtual machine
- **VM subnet mask** – Assign a custom subnet mask to the virtual machine
- **VM gateway** – Assign a custom gateway to the virtual machine
- **VM DNS servers** – Assign the list of custom DNS servers (separated by comma), Example:

```
8.8.8.8 or 8.8.8.8,7.7.7.7
```

Connected server(s)

Data center

Host

Storage

Resource pool

Resources

Network

VIRTUAL

Connect on startup

CPU cores

4

RAM (GB)

4

Source VM configuration

VM IP address

Enter a custom IP address to the new virtual machine

IP addresses will increment by 1, if applied to all devices

VM Subnet mask

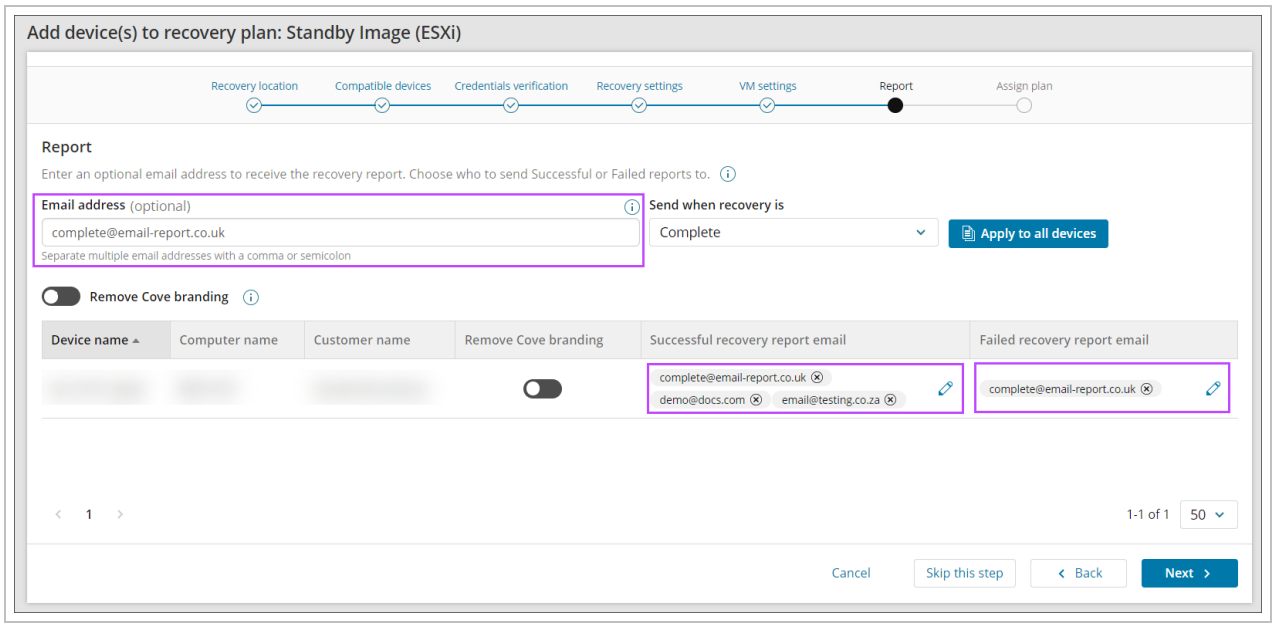
Enter a custom subnet mask to the new virtual machine

VM gateway

Enter a custom gateway to the new virtual machine

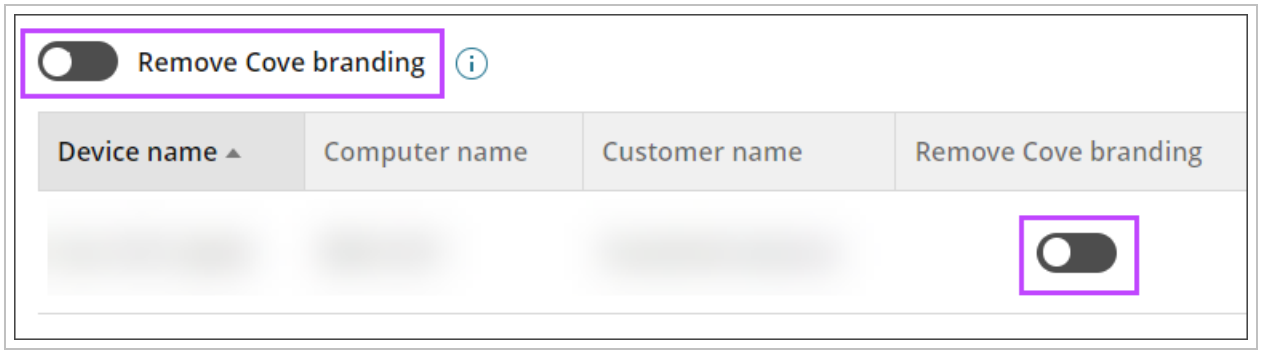
16. Click **Next** to progress to the **Report** window to enter one or more email addresses to receive a report when:
    a. The recovery is complete (Successful or Failed)
    b. The recovery was successful
    c. The recovery failed

> Multiple addresses should be separated using a comma or semi-colon



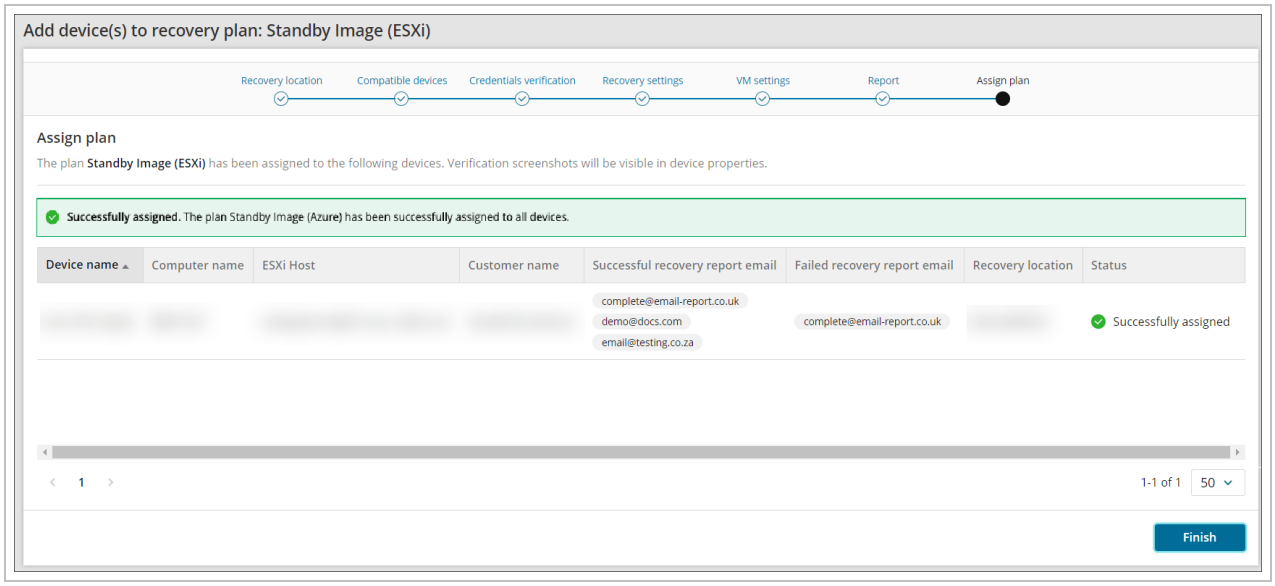
> If you do not want to add an email address to receive reports, click **Skip this step**

17. To remove all branding from the reports, use the **Remove Cove branding** toggle per device, or above the device list to apply the changes to all devices in this window



18. Confirm assigning the plan to the device(s)

19. Wait for the plan to be assigned until you see a confirmation banner on the page

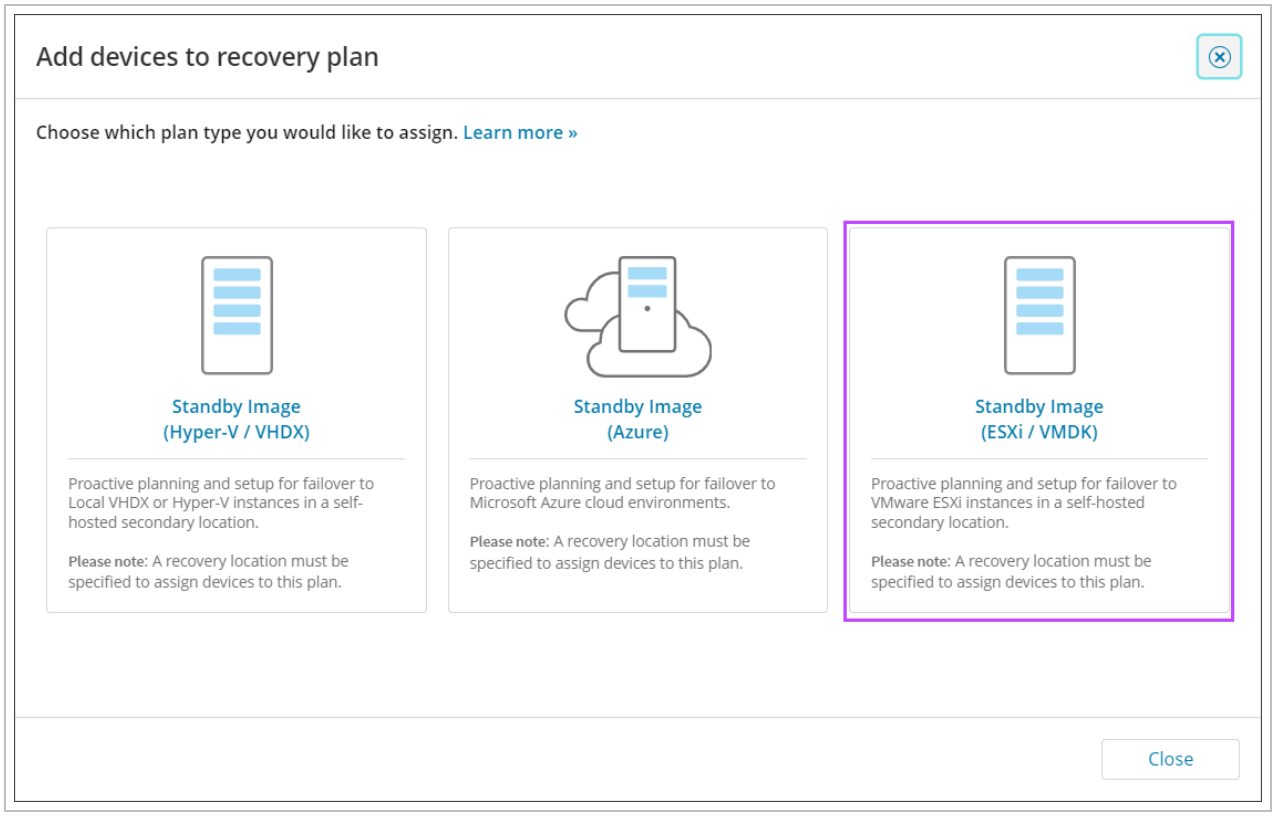


20. Click **Finish**

From Standby Image Overview

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Click **Add to Plan**

4. Select **Standby Image (ESXi)**



5. You will now be taken to the **add devices to recovery plan** wizard. Follow the steps from select the customer from the dropdown onwards

From Recovery Locations dashboard

Devices can be added to a Recovery Location from the **Continuity** > **Recovery Locations** page, thereby enabling the Standby Image Plan, using one of three methods:

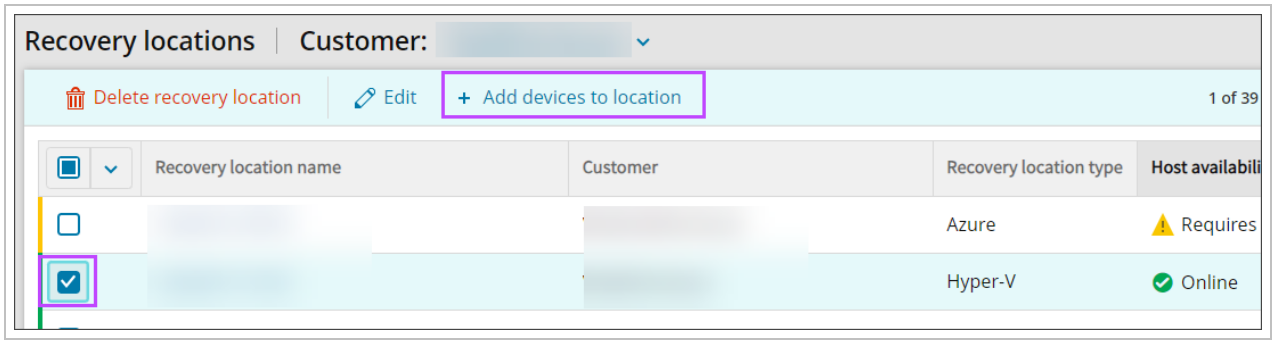
- Top bar menu
- Location context menu
- Right-hand menu

> These will only be available if the Recovery Location is **Online**.

Top bar menu

Available for Hyper-V and ESXi Locations **only**.

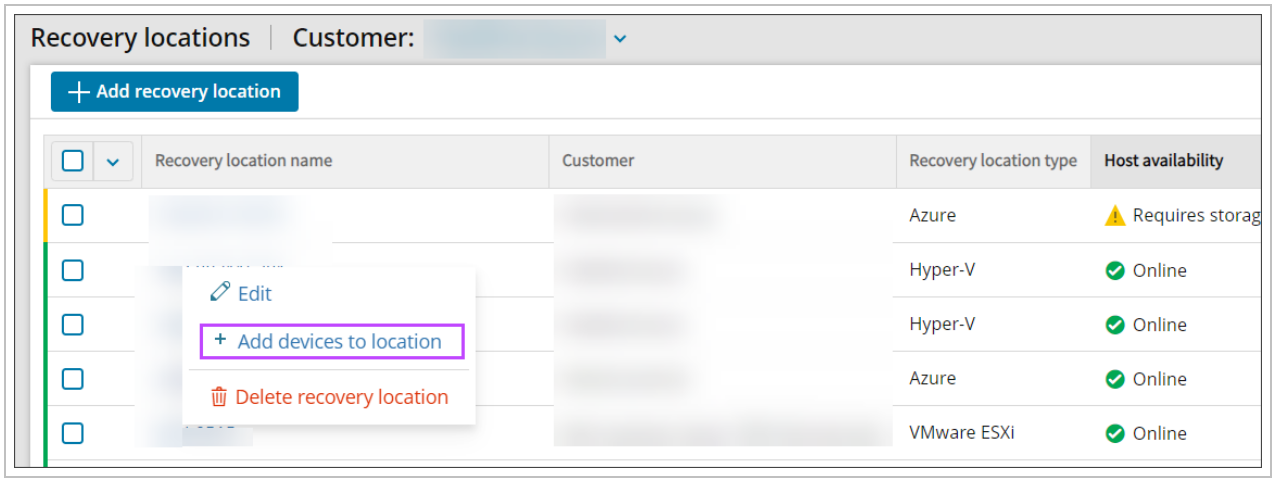
1. Select the checkbox for the Recovery Location to add the device to
2. At the top of the Recovery Locations page, select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
   a. Top bar menu
   b. Top bar menu

Location context menu

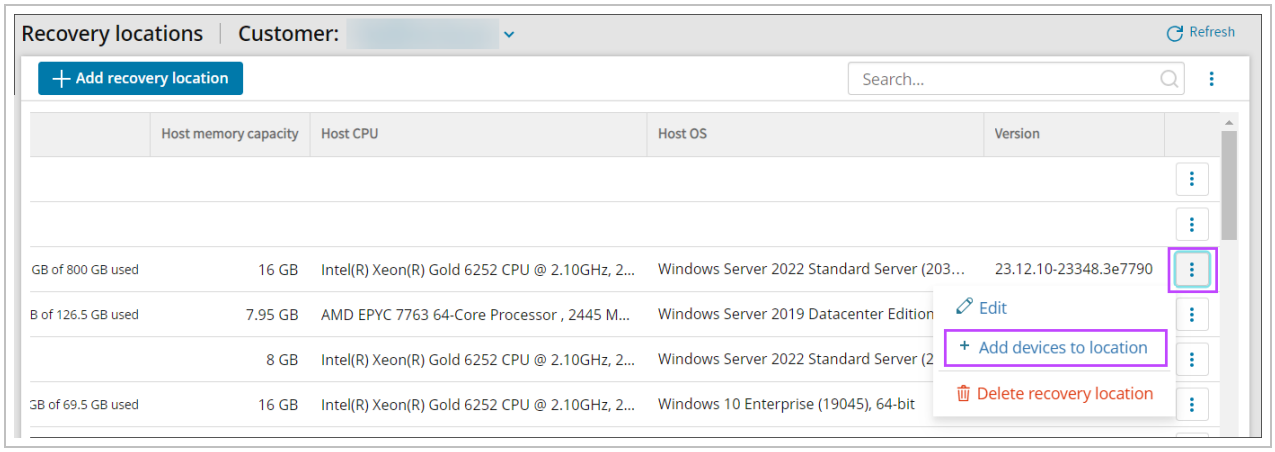
1. Right-click on the Recovery Location to add the device to
2. Select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
    a. Enable Standby Image to AzureDevices cannot be added to a Standby Image plan if already assigned to a Recovery Testing plan.Devices can be assigned to multiple Standby Image plans at once, i.e. Standby Image to Hyper-V and Standby Image to Azure. From Main DashboardTo enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:Log in to the Management Console under a SuperUser or Manager account In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan toClick Add to recovery plan from the Toolbar Select Standby Image (Azure)Select the customer the device(s) you wish to apply the Standby Image plan belong toChoose the recovery location as was configured in Add Recovery LocationsIf the selected customer does not have any locations, you must add one before continuing by selecting Add recovery location. See Add Recovery Locations for full details of adding a location.It is not possible to assign a location for which the Host availability is "Offline"Click NextConfirm the device selected from the Dashboard is compatible and click Next Enter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereClick Next to continueChoose the boot check frequency:OffEvery recovery sessionDailyWeeklyBiweeklyMonthlyIf you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Once connected, click NextClick Azure VM settings towards the right-hand side of the screen to open the settings configuration window:Configure the Azure VM Settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk typeData disk(s) typeVirtual NetworkSubnetAssign NSG and public IPDuring the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend blocking internet access for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.Click Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowConfirm assigning the plan to the device(s)Wait for the plan to be assigned until you see a confirmation banner on the pageClick FinishFrom Standby Image OverviewLog in to the Management Console under a SuperUser or Manager accountNavigate to Continuity > Standby ImageClick Add to PlanSelect Standby Image (Azure)You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the planRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding:
    b. Top bar menu
    c. Top bar menu

Right-hand menu

1. Click the action menu button for the Recovery Location, seen as three dots in a vertical line to the right of the location's version
2. Select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
    a. Enable Standby Image to AzureDevices cannot be added to a Standby Image plan if already assigned to a Recovery Testing plan.Devices can be assigned to multiple Standby Image plans at once, i.e. Standby Image to Hyper-V and Standby Image to Azure. From Main DashboardTo enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:Log in to the Management Console under a SuperUser or Manager account In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan toClick Add to recovery plan from the Toolbar Select Standby Image (Azure)Select the customer the device(s) you wish to apply the Standby Image plan belong toChoose the recovery location as was configured in Add Recovery LocationsIf the selected customer does not have any locations, you must add one before continuing by selecting Add recovery location. See Add Recovery Locations for full details of adding a location.It is not possible to assign a location for which the Host availability is "Offline"Click NextConfirm the device selected from the Dashboard is compatible and click Next Enter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereClick Next to continueChoose the boot check frequency:OffEvery recovery sessionDailyWeeklyBiweeklyMonthlyIf you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Once connected, click NextClick Azure VM settings towards the right-hand side of the screen to open the settings configuration window:Configure the Azure VM Settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk typeData disk(s) typeVirtual NetworkSubnetAssign NSG and public IPDuring the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend blocking internet access for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.Click Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowConfirm assigning the plan to the device(s)Wait for the plan to be assigned until you see a confirmation banner on the pageClick FinishFrom Standby Image OverviewLog in to the Management Console under a SuperUser or Manager accountNavigate to Continuity > Standby ImageClick Add to PlanSelect Standby Image (Azure)You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the planRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding:
    b. Top bar menu
    c. Top bar menu

Recovery Reports

When the device(s) assigned to the plan have **Successful recovery report email** or **Failed recovery report email** recipient

address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox.

Here is an example report with Cove branding:

Cove Data Protection

Recovery completed

Recovery plan: **Standby Image (ESXi)**

Last recovery session completed successfully: April 16 2024 3:45:39 AM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Workstation
Operating system	Windows 10 Enterprise (19045), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 16 2024 3:45:39 AM
Recovery status	Completed
Recovery duration	1 hour, 50 minutes and 18 seconds
Recovery location	ESXi.
Restore frequency	Each backup session
Recovery plan	Standby Image (ESXi)

BACKUP DETAILS USED FOR THE RESTORE

Backup session time	April 16 2024 3:35:44 AM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

BOOT TEST OVERVIEW

Screenshot verification	Not applicable
Boot check frequency	Off

Screenshot verification is not applicable

Here is an example **without** Cove branding:

Recovery completed

Recovery plan: **Standby Image (ESXi)**

Last recovery session completed successfully: April 16 2024 3:45:39 AM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Workstation
Operating system	Windows 10 Enterprise (19045), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 16 2024 3:45:39 AM
Recovery status	Completed
Recovery duration	1 hour, 50 minutes and 18 seconds
Recovery location	ESXi.
Restore frequency	Each backup session
Recovery plan	Standby Image (ESXi)

BACKUP DETAILS USED FOR THE RESTORE

Backup session time	April 16 2024 3:35:44 AM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

BOOT TEST OVERVIEW

Screenshot verification	Not applicable
Boot check frequency	Off

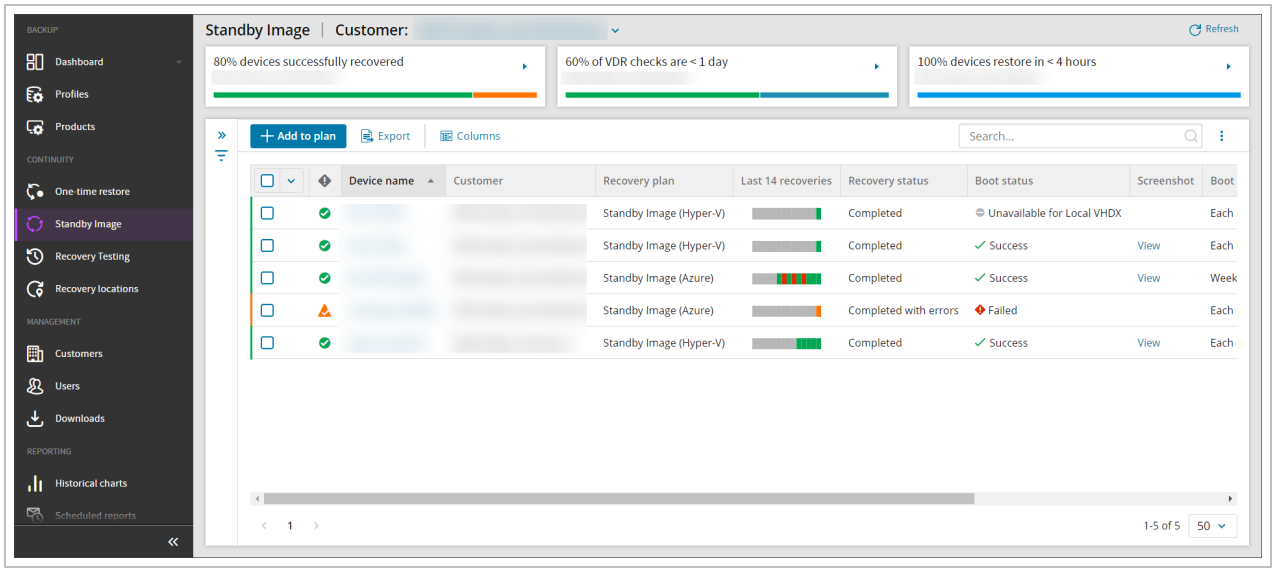
Screenshot verification is not applicable

Monitor Standby Image Devices

From the Management Console, you can view the dedicated Standby Image Overview by selecting **Continuity** > **Standby Image** from the vertical menu on the left hand side.

This page will list devices assigned to the Standby Image plans:

- Standby Image to Hyper-V
- Standby Image to Azure
- Standby Image to ESXi



From this dashboard, you will see a specified set of columns detailing information relevant to devices using the Standby Image plan, including the continuity history of the last 14 recoveries, the recovery status, boot status, and plan assigned, along with some other information.

If no devices are assigned to either Standby Image plan, the dashboard will display a message to advise, along with a button to add devices to a plan.

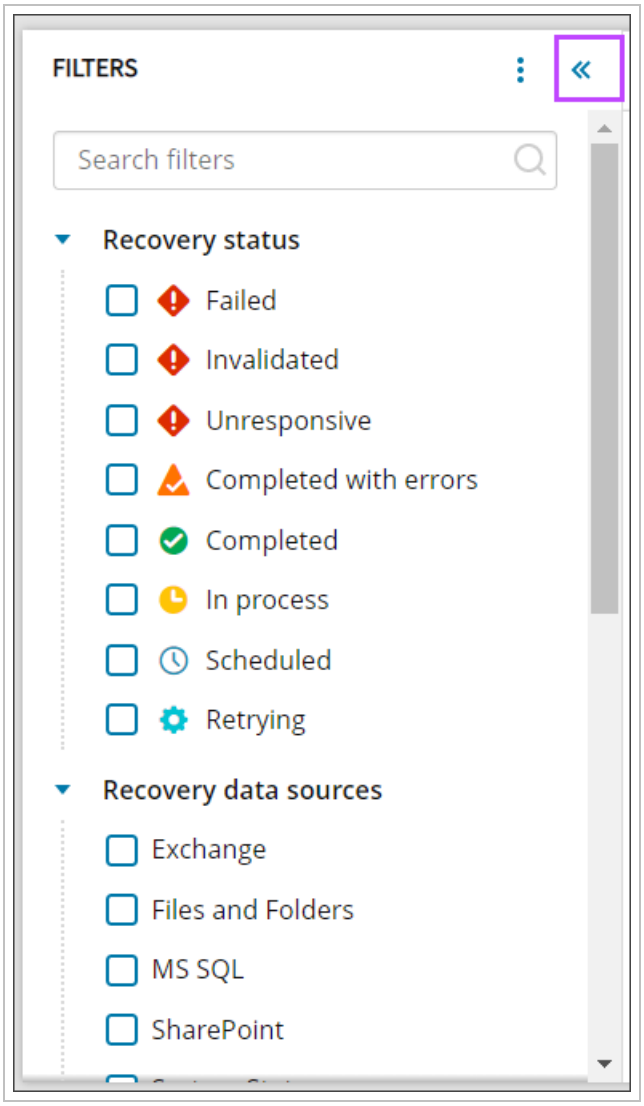
> If a device is assigned to **multiple** plans (i.e. **Standby Image to Hyper-V**, **Standby Image to Azure** and **Standby Image to ESXi**), the device will be listed for each instance of a plan and can be told apart by the **Recovery Plan** column.

Searching

Searching within the Standby Image overview can be done by using the search box over to the right hand side of the page, just above the devices list. The search can be performed by any text field.

Filtering

The Standby Image overview also includes functionality to filter devices using the filter menu to the left of the device list and can be displayed or hidden by clicking the double arrows.



From this menu, you can filter by:

Recovery status

- **Failed** - The recovery session has failed
- **Invalidated** - Device was moved to an inappropriate partner and so the session has failed
- **Unresponsive** - The recovery session was initiated but did not receive updates for at least 30 minutes because the recovery location restarted or was offline.
- **Completed with errors** - The recovery session completed, but encountered errors
- **Completed** - The recovery session completed with no errors
- **In process** - The recovery is currently in progress
- **Scheduled** - Devices just added to a recovery plan and are waiting for their first recovery session or devices where restores were paused and have since been resumed will display as scheduled
- **Retrying** - A restore session was not finished so the system is trying the restore again

Recovery data sources

- Exchange
- Files and Folders
- MS SQL
- SharePoint
- System State

Recovery session statistics

- Boot check frequency
  - Off
  - Every recovery session
  - Daily
  - Weekly
  - Biweekly
  - Monthly
- Boot Check Status
  - Success
  - Failed
  - Off
  - Unavailable for Local VHDX
- Continuous restores
  - Running
  - Paused
- Duration of the last completed recovery session
  - Sliding scale from 0 to unlimited

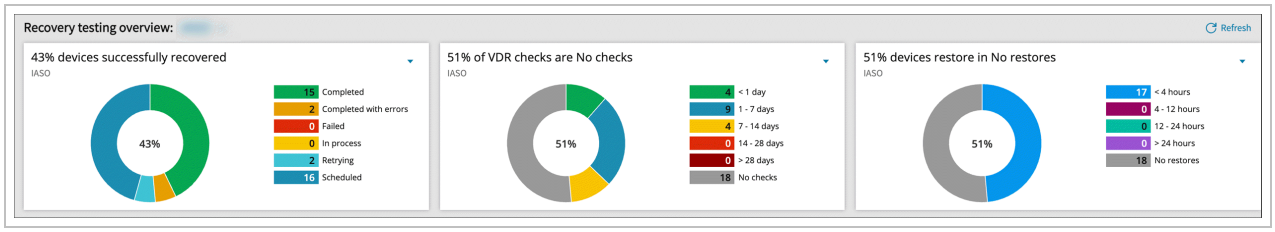
  in minutes
- Number of errors of the last completed recovery session
  - Sliding scale from 0 to unlimited
- Number of restored files
  - Sliding scale from 0 to unlimited
- Number of selected files
  - Sliding scale from 0 to unlimited
- Recovery Location name
  - Select the recovery location from a dropdown
- Recovery Plan
  - Standby Image (Hyper-V)
  - Standby Image (ESXi)
  - Standby Image (Azure)
- Restored size
  - Sliding scale from 0 to unlimited

  in KB and GB

- Recovery testing status of the last completed recovery session
  - Failed
  - Completed with errors
  - Completed
- Screenshot
  - Available
  - Not Available
- Selected size
  - Sliding scale from 0 to unlimited
  in KB and GB
- Timestamp of the last completed recovery session
  - Quick Picks of:
    - Last day
    - 1 - 7 days
    - 7 - 14 days
    - 14 - 28 days
    - > 28 days
  - Custom range, select a stat date and time and an end date and time

Widgets

Three widgets can be maximized at the top of the page, which allow for further filtering:



Device recovery status

This widget allows you to filter the devices by recovery status:

- Completed
- Completed with errors
- Failed
- In process
- Retrying
- Scheduled

VDR checks time frame

This widget allows you to see the percentage of devices whose recovery check completed within the following day ranges:

- < 1 day
- 1 - 7 days
- 7 - 14 days
- 14 - 28 days
- > 28 days
- No checks

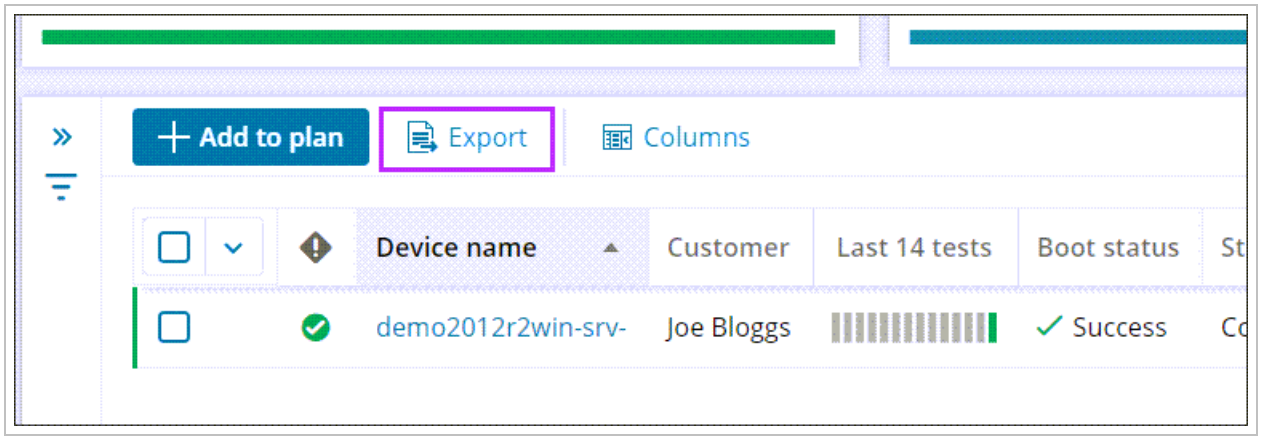
Device restore time frame

From this widget, you can filter devices by the how recent restores are done by the following time frames:

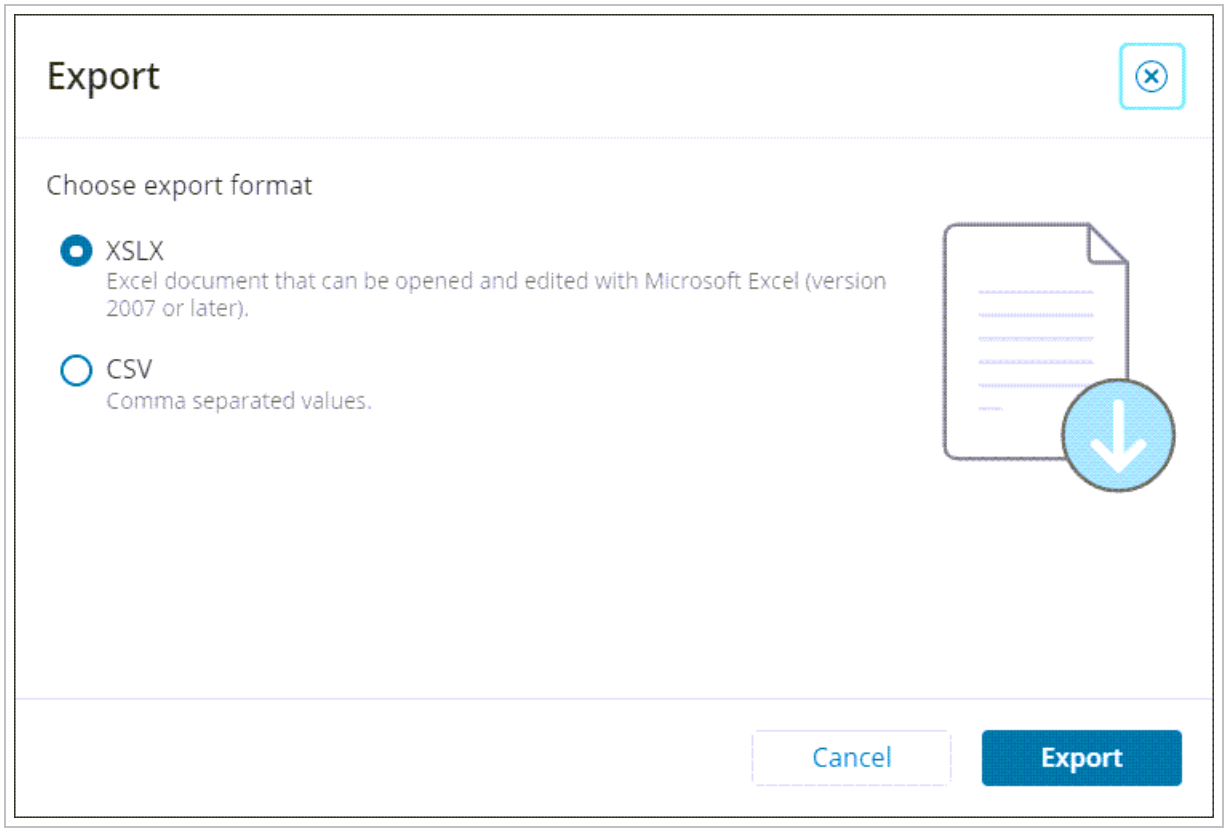
- < 4 hours
- 4 - 12 hours
- 12 - 24 hours
- > 24 hours
- No restores

Exporting

You may export a list of devices currently assigned a plan by clicking **Export**

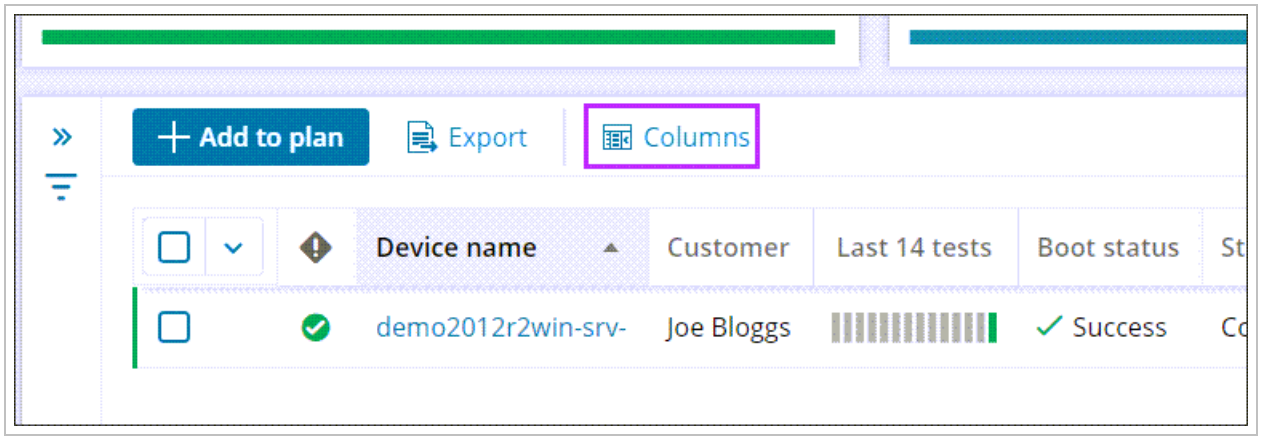


This will then provide a separate dialog where you can choose to export in either XSLX or CSV.

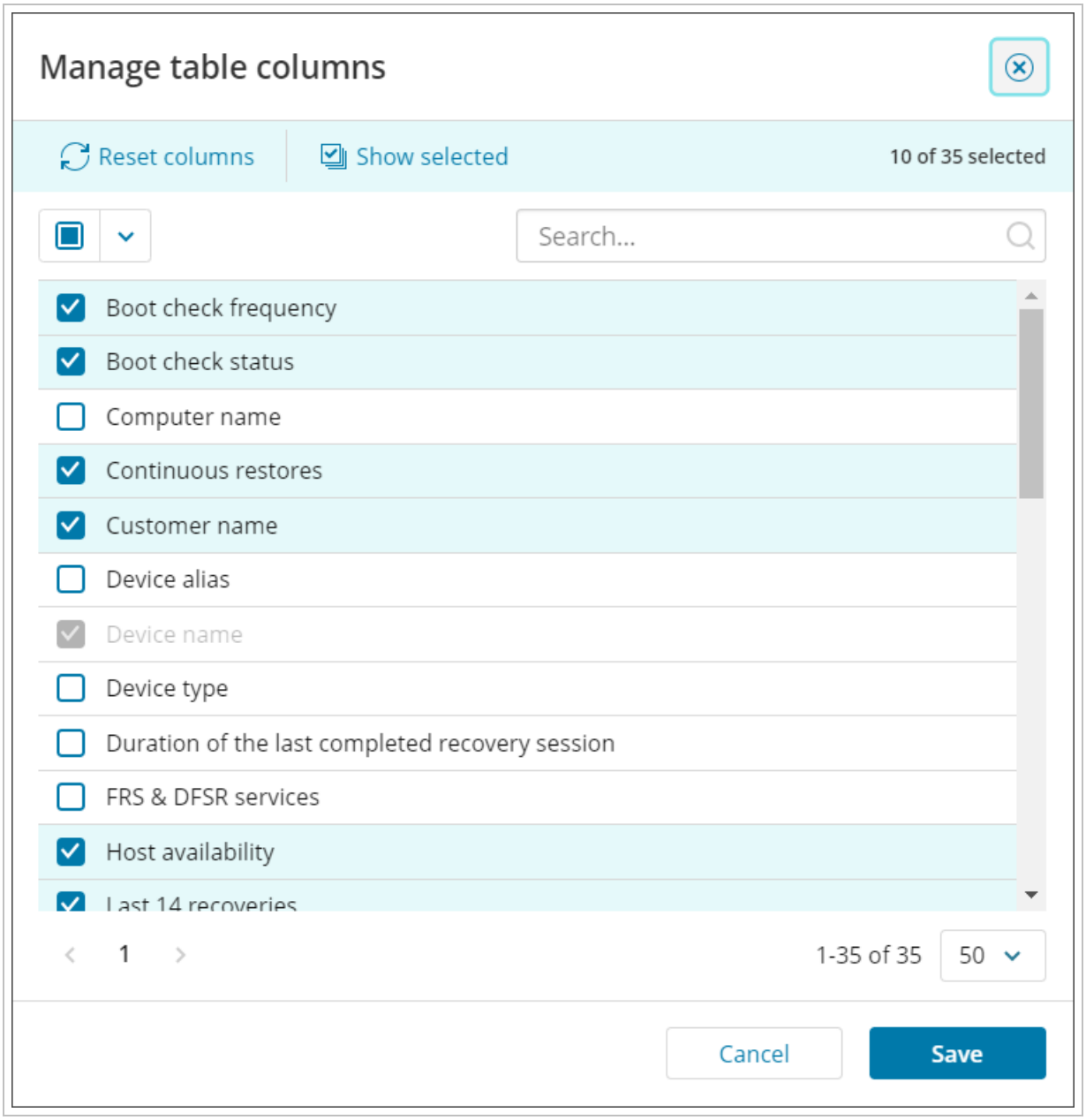


Manage Table Columns

Management Console allows you to manage the tables columns that can be seen within the Standby Image overview.



In the Manage table columns dialog, you can select and deselect columns based on the information you wish to view from the overview.

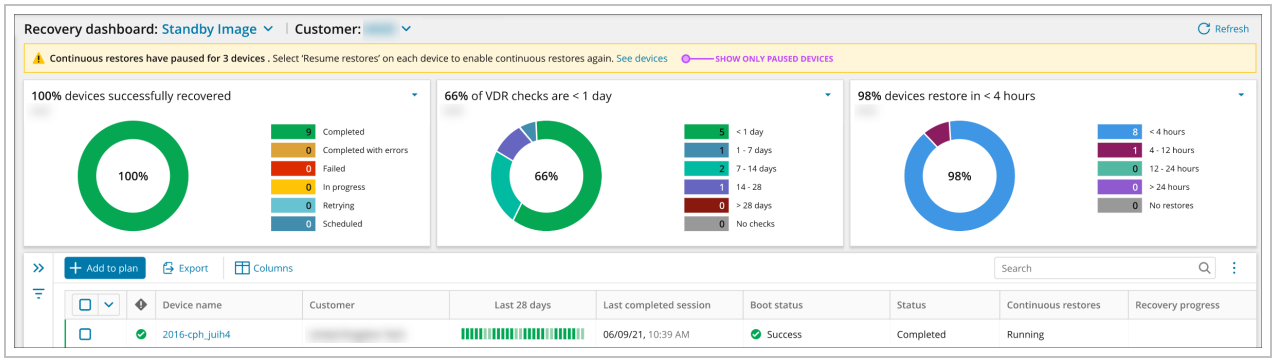


Pause Standby Image recovery

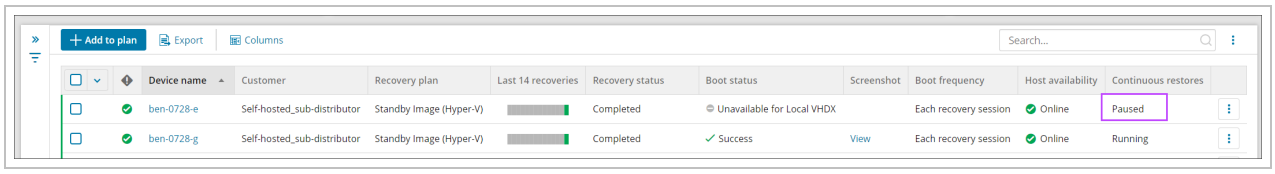
Once a Standby plan has been assigned to a device, the continuous restores can be paused and restarted. Pause or resume restores functionality there to provide a possibility to use the restored machine for failover in case of disaster.

> If a restored Virtual Machine is turned on manually, the Standby Image restore will automatically pause.

Pausing and restarting continuous restores can done be for single or multiple devices at a time. Once devices have been paused, a banner will be displayed at the top of the page to advise.

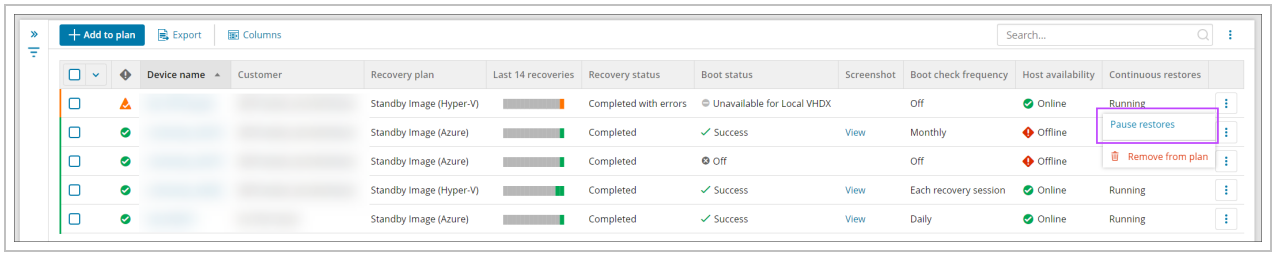


Click **See devices** to filter the devices list by **Continuous Restore: Paused** to only devices which are currently paused.



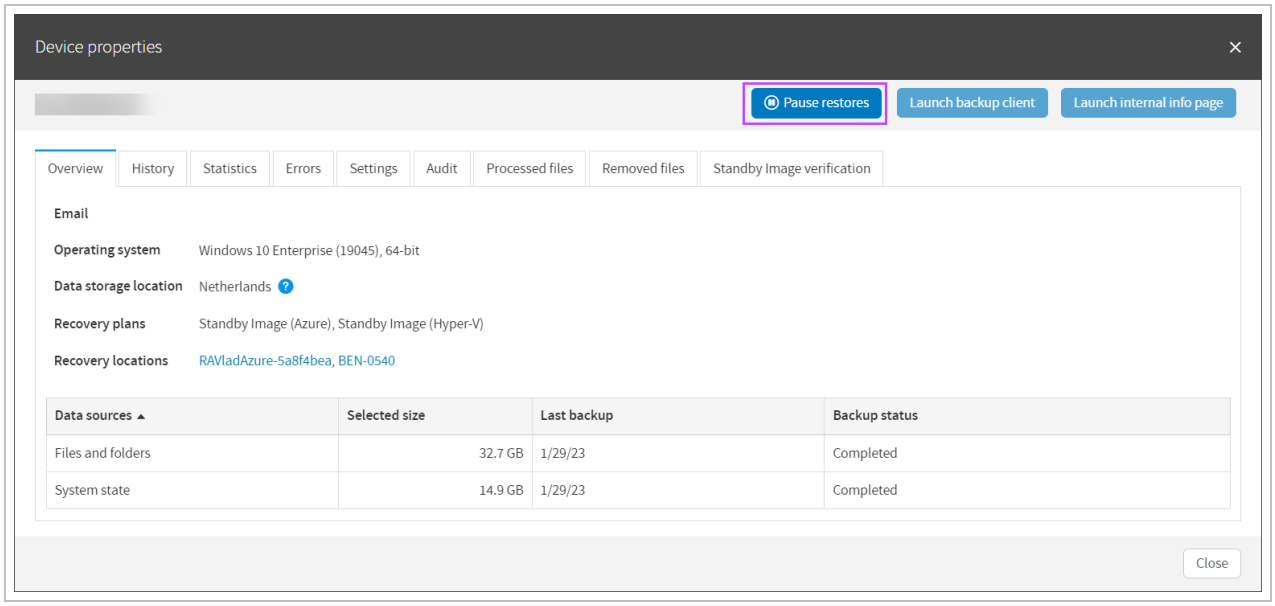
For single devices

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Click the menu action button to the right of the device (Three vertical dots)
4. Select **Pause Restores** or **Resume Restores**



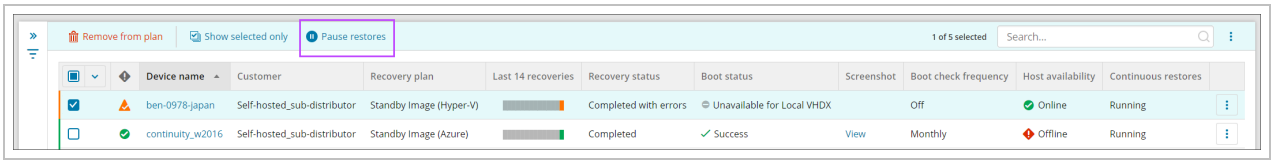
> This will differ depending on whether the plan is currently active, or has been paused already

It is also possible to pause restores from the Device Properties window:



For single or multiple devices

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Tick the checkbox for any devices that need paused from the list
4. In the top panel, select **Pause Restores** or **Resume Restores**



> This will differ depending on whether the plan is currently active, or has been paused already

Accessing device properties

The Device Properties window displays several tabs detailing information on the Backup device. Full details of the contents of each tab can be found on the Device management in Management Console page.

The two that are the most commonly used with Standby Image are the **Settings** tab and the **Standby Image Verification** tab.

Settings Tab

Broken into several sections, this tab contains:

General

This section provides the main device details:

- **customer** - Who device belongs to, can be changed to move the device to a different customer
- **Device name** - Cannot be changed

- **Installation key** - Cannot be changed
- **Creation date** - Cannot be changed
- **Expires on** - Can be amended to a date in the future, or set to **'no expiration'** if required

> You may also see the Request Passphrase button here if the device is set up to use this instead of its own security code/encryption key

Backup

This section contains:

- **Backup product** - Use the dropdown to change the Product used by the device
- **Profile** - Use the dropdown to change the Profile applied to the device

Recovery

On a device assigned to the Standby Image plan, this section will allow you to see plan in use and amend some details of this:

- **Recovery Plan** - Standby Image (Each backup session)
- **Recovery Location** - Cannot be changed from this panel. To change this, see Add Device to Recovery Location
- **Successful recovery report email** - Specify the email address(es) that will receive reports when the most recent Recovery as per the assigned plan has been successful
- **Failed recovery report email** - Specify the email address(es) that will receive reports when the most recent Recovery as per the assigned plan has failed
- **Remove Cove branding** - toggle branding of the email reports on or off
- **Restore format** - This option will not be available for Standby Image to Azure.
  - For **Standby Image to Hyper-V**, this is a choice between **Hyper-V** or **Local VHDX**
  - For **Standby Image to ESXi**, this is a choice between **ESXi** and Local **VHDX**

    > Further settings displayed are dependent on the Restore Format selected for the device. These settings can be changed as required.

> All Recovery Plans associate to the device will be included here, and can be minimized or expanded by clicking the arrow to the left of the plan name.

Device properties

Launch backup client | Launch internal info page

Overview | History | Statistics | Errors | Settings | Audit | Processed files | Removed files | Standby Image verification

General

Customer

Device name

Installation key

Creation date 2/21/23

Expires on 04/18/24 No expiration

Backup

Product _test

Profile -servers

Recovery

Standby Image (ESXi)

Recovery plan Standby Image (ESXi)

Recovery location ESXiRA

Successful recovery report email e.g email@email.com

Failed recovery report email e.g email@email.com

Remove Cove branding OFF

Restore format ESXi VMDK

Boot check frequency Daily

FRS and DFSR services OFF

Local Speed Vault OFF

CPU cores 4

RAM (GB) 4

VM Subnet mask Enter a custom subnet mask to the new virtual mac

VM gateway Enter a custom gateway to the new virtual machine

VM DNS server Enter a DNS server to be used on the restored mach

Separate multiple DNS servers with a comma or semicolon

VM IP address Enter a custom IP address to the new virtual machir

Standby Image (Hyper-V)

Recovery plan Standby Image (Hyper-V)

Recovery location BEN-6478

Successful recovery report email e.g email@email.com

Failed recovery report email e.g email@email.com

Remove Cove branding OFF

Restore format Hyper-V Local VHDX

Boot check frequency Daily

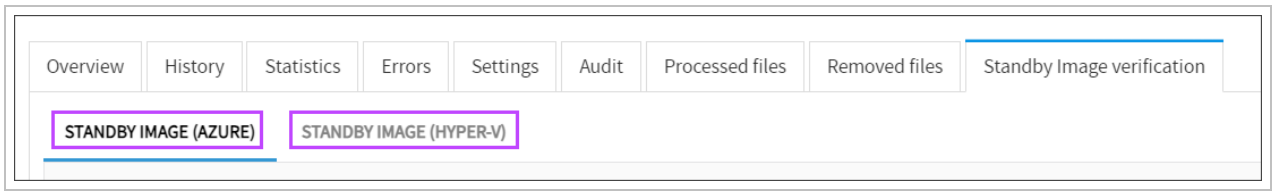
FRS and DFSR services OFF

Local Speed Vault OFF

Standby Image Verification Tab

To view statistics of the Standby Image and check the screenshots to ensure this has been successful, you can view this by following one of the below methods.

All plans associated to the device will have their own sub-tabs that can be selected to view the appropriate screenshot:



From Device Properties

1. Log in to the Management Console
2. Click the device name on either the Backup Dashboard or the Standby Image overview to open the Device Properties
3. Navigate to the **Standby Image Verification** tab

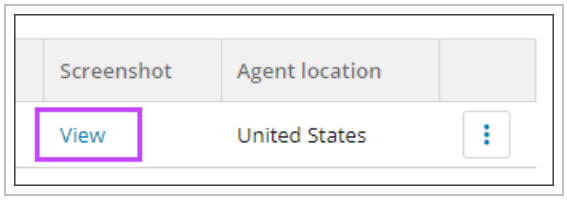
From Standby Image Overview

The Standby Image Verification tab can be viewed from the Standby Image overview in one of two ways:

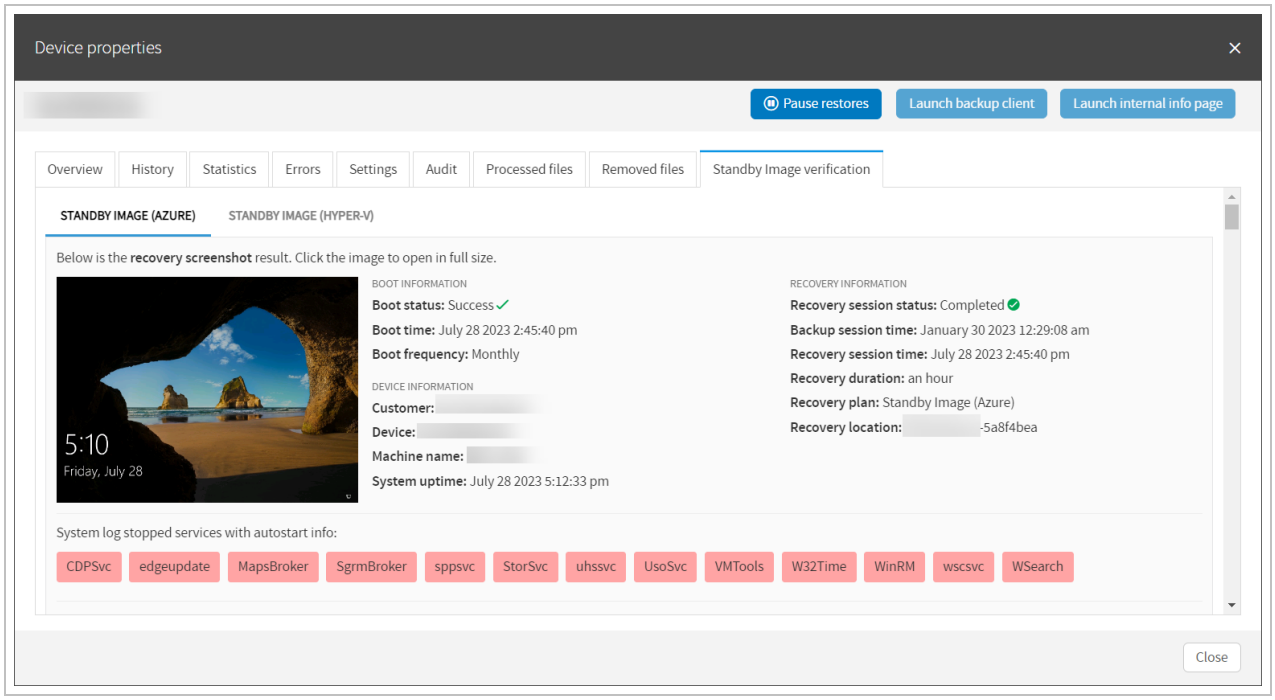
- Via theScreenshot column
- Via the Last 14 recoveries column

Screenshot column

1. Log in to the Management Console
2. Navigate to **Continuity** > **Standby Image**
3. Click **View** under the Screenshot column

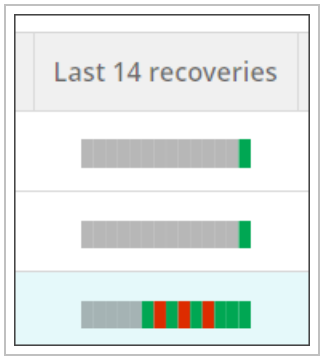


4. This will take you in to the Device Properties dialogue, where you will now see the **Standby Image Verification** tab:

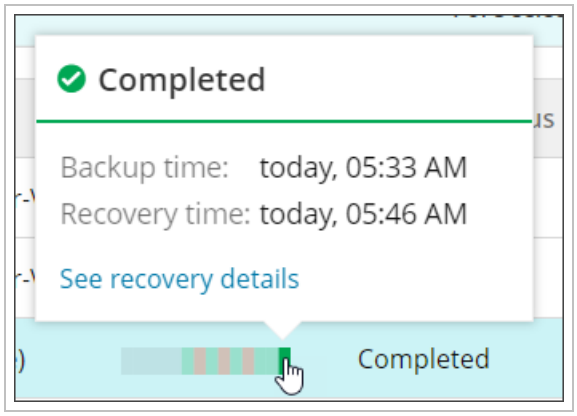


Last 14 recoveries column

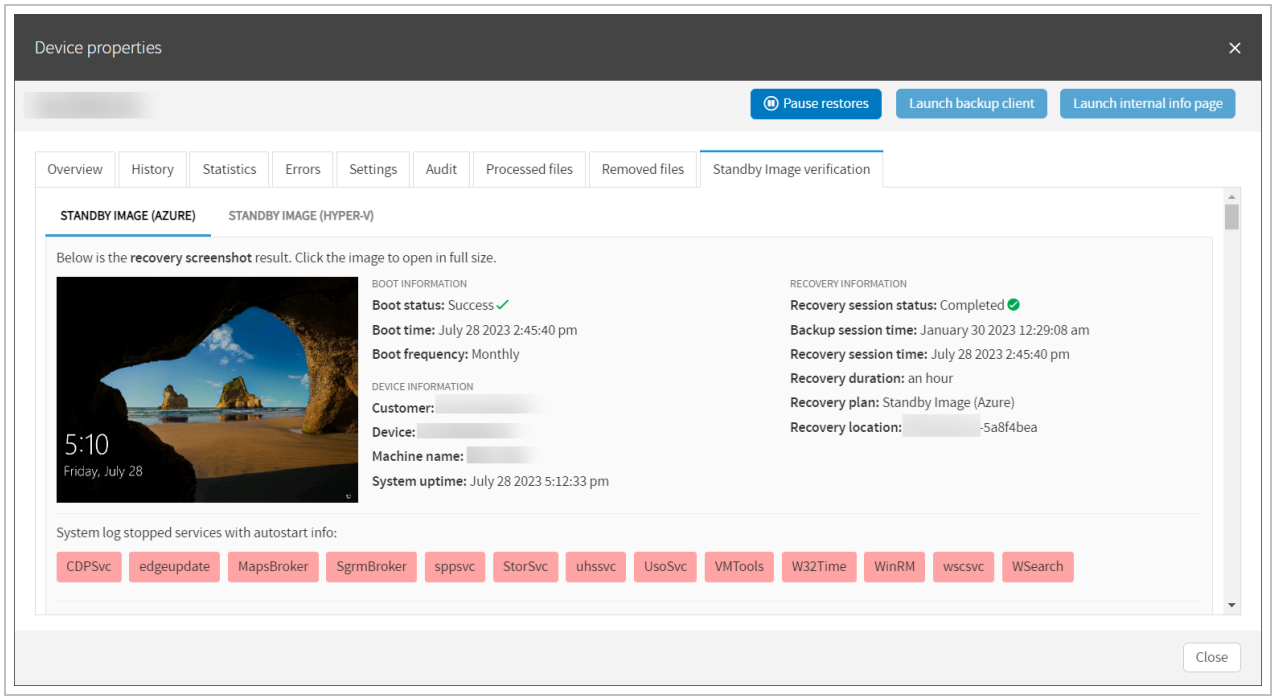
1. Log in to the Management Console
2. Navigate to **Continuity** > **Standby Image**
3. Hover your mouse over the most recent colored bar in the Last 14 recoveries column



4. Click **See recovery details** in the popup box that appears



5. This will take you in to the Device Properties dialogue, where you will now see the **Standby Image Verification** tab:



Standby Image Use in Case of Disaster

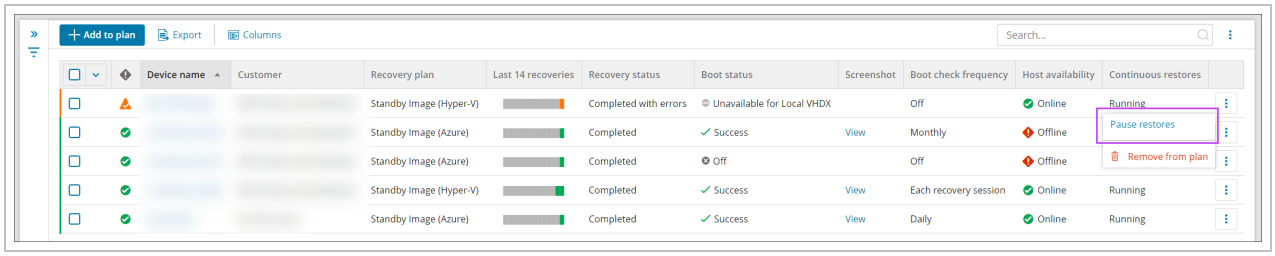
Using Standby Image, you can continuously restore the most recent backup to a secure location, either Hyper-V or to the Azure Cloud. In case of disaster, the restored machine can be used for failover by following the relevant procedures below.

For Hyper-V

To use a Standby Image to Hyper-V:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Find the affected device and click the menu action button to the right of the device (Three vertical dots)

4. Select **Pause Restores**



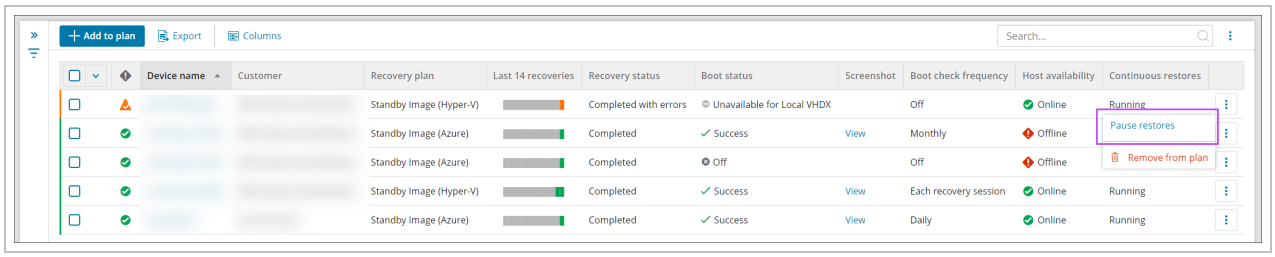
> By doing so, this halts further restoration for the device and prevents accidental damage to the Standby Image

5. Once paused, connect to the device hosting the Recovery Location
6. Navigate to the Hyper-V manager
7. Find the virtual machine created for the standby image device and select **Start**

For ESXi

To use Standby Image to ESXi:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Find the affected device and click the menu action button to the right of the device (Three vertical dots)
4. Select **Pause Restores**



> By doing so, this halts further restoration for the device and prevents accidental damage to the Standby Image

5. Connect to the device (virtual machine or dedicated server/host) by either:
   a. Sign in to the **vCenter Server** by using the **vSphere Client**
   b. Navigate to **Inventory** in the menu and find the virtual machine created
   c. Power it on and click **Launch remote console**

   Or

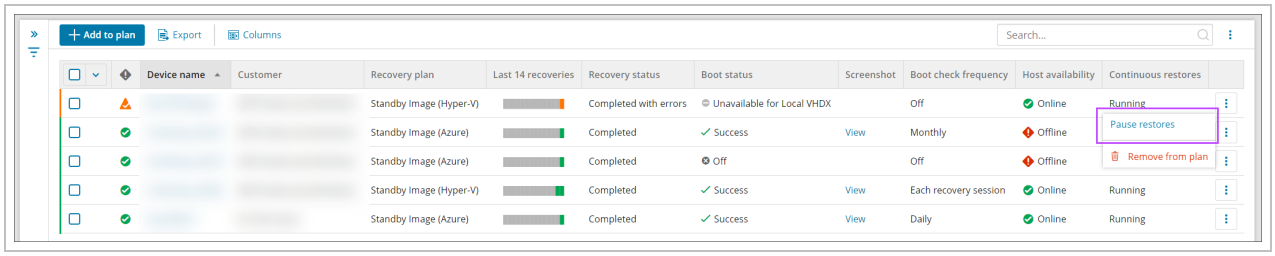
   a. If restoring to the ESXi server/host directly, login to the dedicated server/host machine

For Azure

To use a Standby Image to Azure:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Find the affected device and click the menu action button to the right of the device (Three vertical dots)

4. Select **Pause Restores**



> By doing so, this halts further restoration for the device and prevents accidental damage to the Standby Image

5. Sign into Microsoft Azure
6. Locate the machine associated to the device in Cove Data Protection. Navigate to the "Locks" section of this virtual machine and remove any existing locks.
7. Power on the machine hosted in Azure

Recovery Testing

Cove Data Protection (Cove)'s Recovery Testing service is a scheduled, automated service to test the recoverability of critical devices. There is no need for manual setup or local resources.

Choose to run Recovery Testing restore every 14 or 30 days and with each restore, a virtual machine is automatically created. Once the Virtual Machine has been created, we will boot it and create a screenshot to check that the Virtual Machine is bootable, then send this screenshot to the Management Console so that users can check it.

> The virtual machines that are created as part of Recovery Testing are **purged** once the restore is completed and the screenshot taken. This means these restored virtual machines are **not accessible** by the user.

Limitations

- Only devices with Backup Manager version 17.4 and above are supported for Recovery Testing
- Software-only devices are not compatible with Recovery Testing
- Recovery Testing cannot be used on the RMM integrated version of Backup (Managed Online Backup)
- There is a size restriction of <= 2 TB selected size per device. You can opt to use "Restore OS-disk only" (available only in standalone version) feature to bypass this limitation
- Recovery Testing restores only System State, Files and Folders, and MS SQL
- Recovery Testing is not available for devices with disabled ‘Virtual disaster recovery’ feature in the assigned product
- Recovery Testing does **not** support 32-bit architecture
- Maximum supported capacity for virtual hard disks is **64 TB** per disk
- Devices cannot be added to a Recovery Testing plan if already assigned to a Standby Image plan

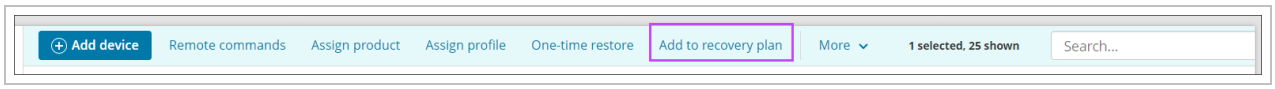
Enable Recovery Testing

> Devices cannot be added to a **Recovery Testing plan** if already assigned to a **Standby Image plan to Hyper-V** or **Standby Image to Azure plan**.

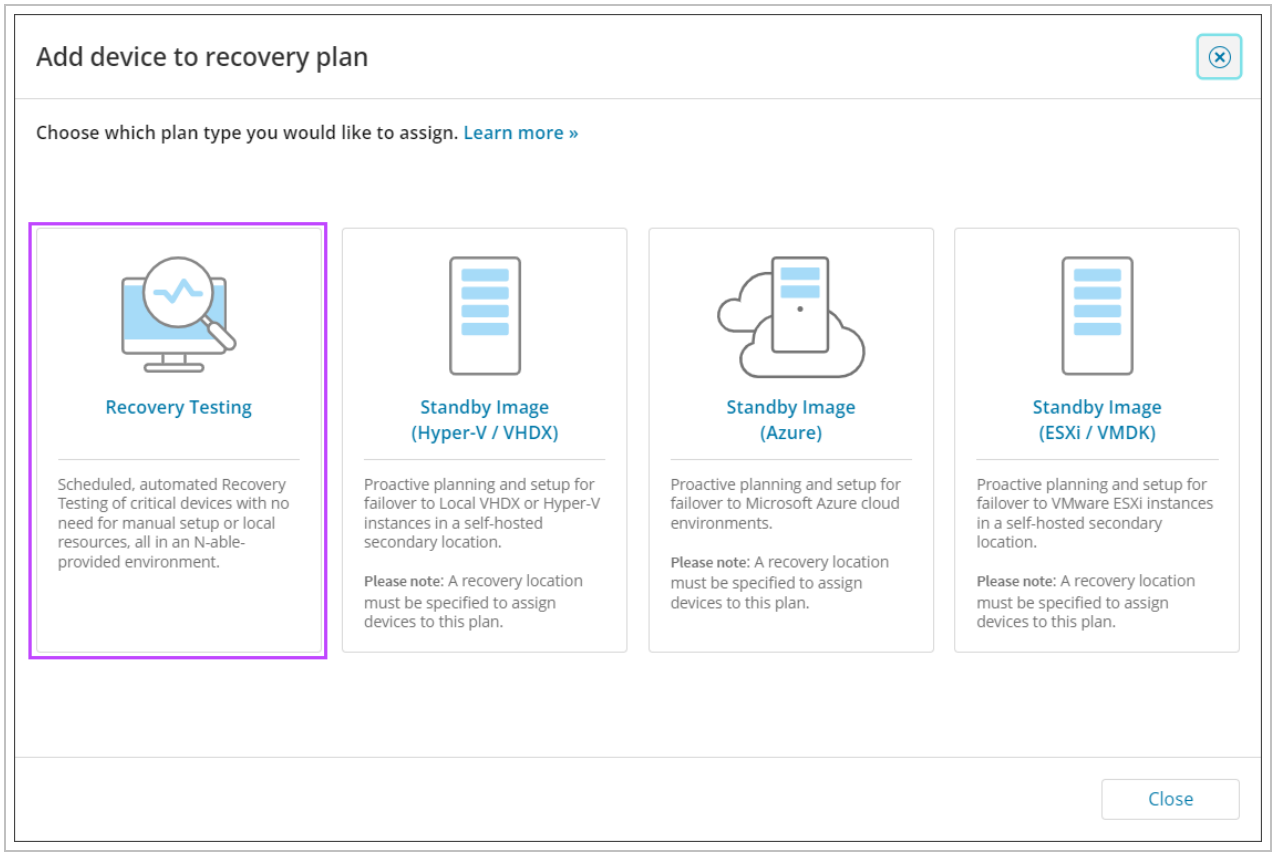
From Main Dashboard

To enable Recovery Testing on a device from the Management Console's main Dashboard, follow the steps below:

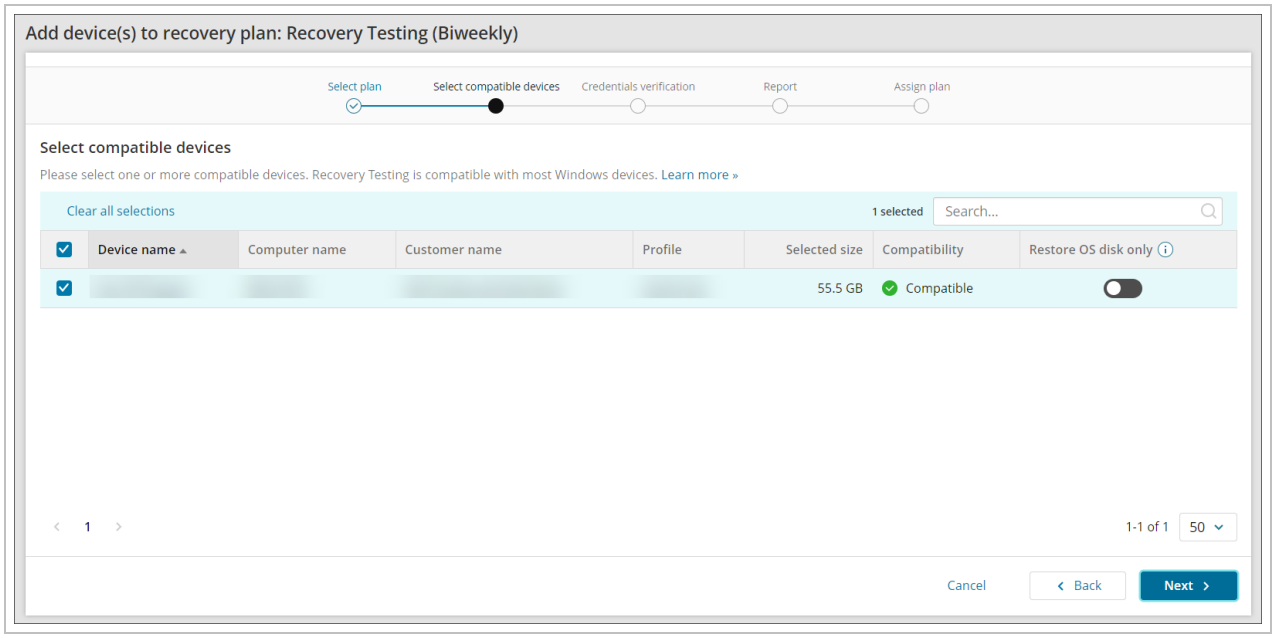
1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan to
3. Click **Add to recovery plan** from the Toolbar



4. Select **Recovery Testing**



5. Select the **customer** from the dropdown
6. Choose the frequency of the plan to assign:
   - **Biweekly** - This will automate the recovery with fortnightly boot testing and screenshot creation (every 14 days)
   - **Monthly** - This will automate the recovery with monthly boot testing and screenshot creation (every 30 days)
7. Click **Next**
8. Confirm the compatibility of devices and the selected size of the device's data and click **Next**



9. If you wish to skip all data drives, enable **Restore OS disk only**

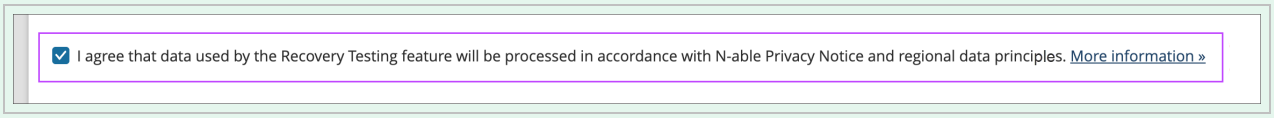
> This will restore the system drive and check the machine's bootability, but it will not restore the data drives.

> This function will be automatically enabled if the device is incompatible due to exceeding the 2TB selected size limitation

10. Enter the security code/encryption key or passphrase for the device(s). This can be either:
    - **Private encryption key** - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryption
    - **Passphrase encryption** - These are generated on demand for automatically installed devices. You can find information on this here

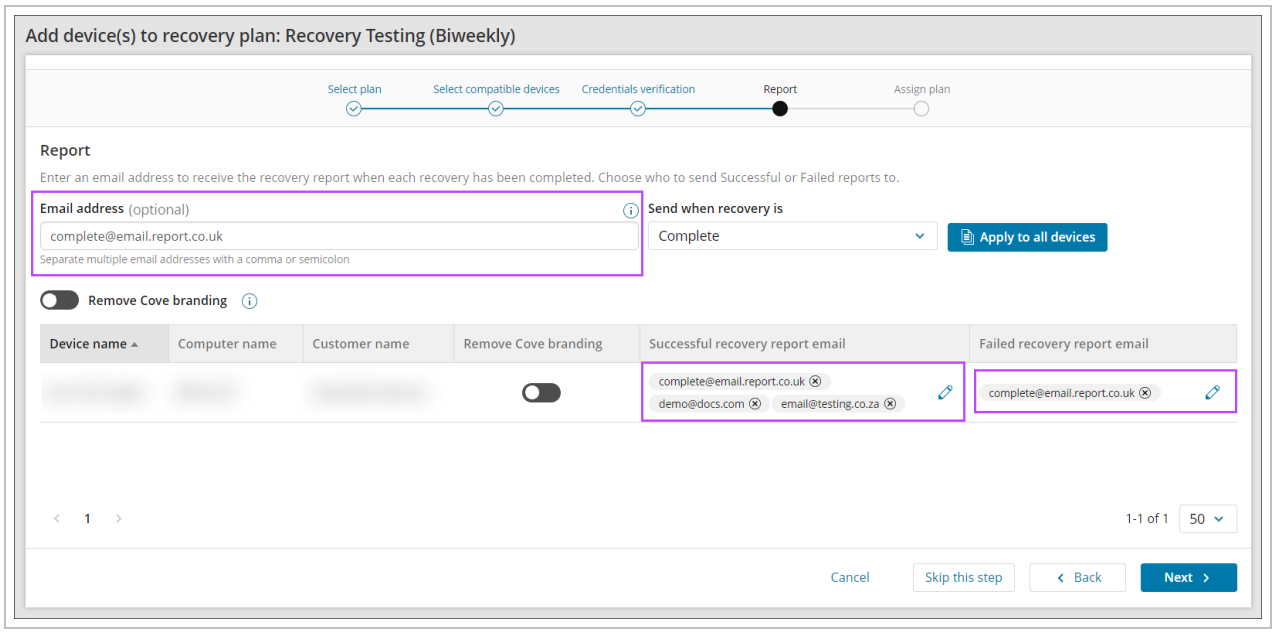
> If you are logged in as a security officer, this will be detected automatically.

> Any customer based in the EU (except Germany) will be required to agree to the policies linked.



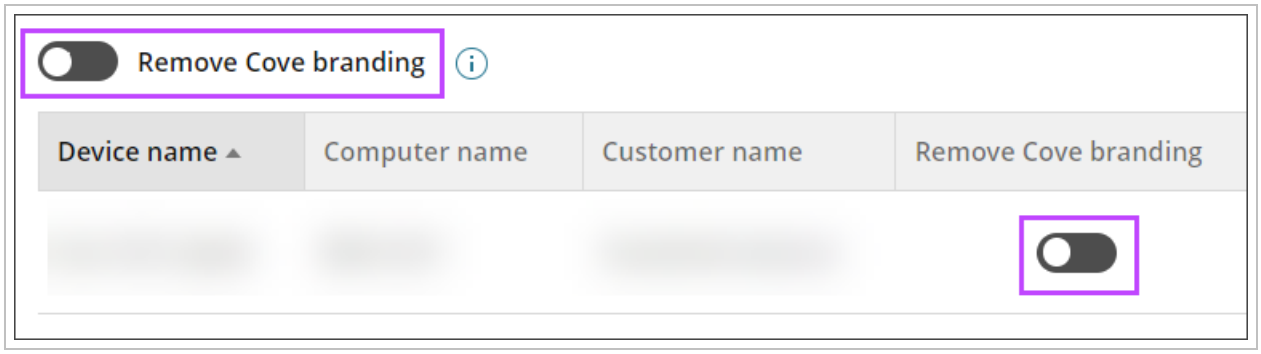
11. Click **Next** to progress to the **Report** window to enter one or more email addresses to receive a report when:
    a. The recovery is complete (Successful or Failed)
    b. The recovery was successful
    c. The recovery failed

> Multiple addresses should be separated using a comma or semi-colon

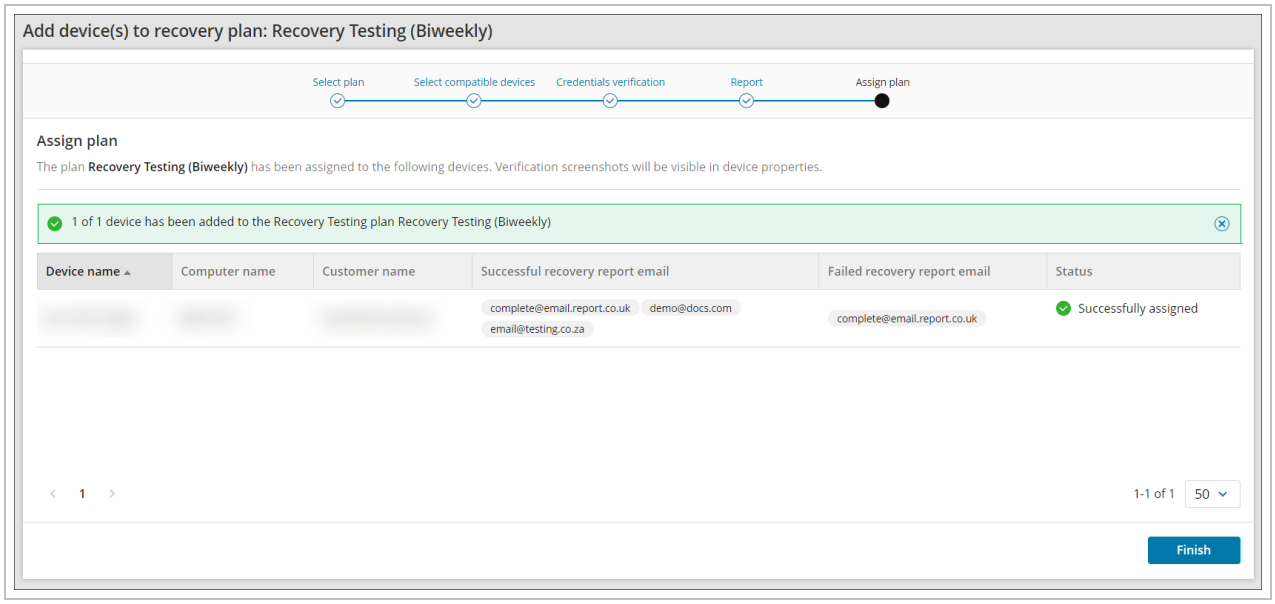


> If you do not want to add an email address to receive reports, click **Skip this step**

12. To remove all branding from the reports, use the **Remove Cove branding** toggle per device, or above the device list to apply the changes to all devices in this window



13. Select **Next** to enable the plan on the selected devices
14. You will now see the status of the plan has changed to **Completed** and the banner shows the number of devices added to the plan.



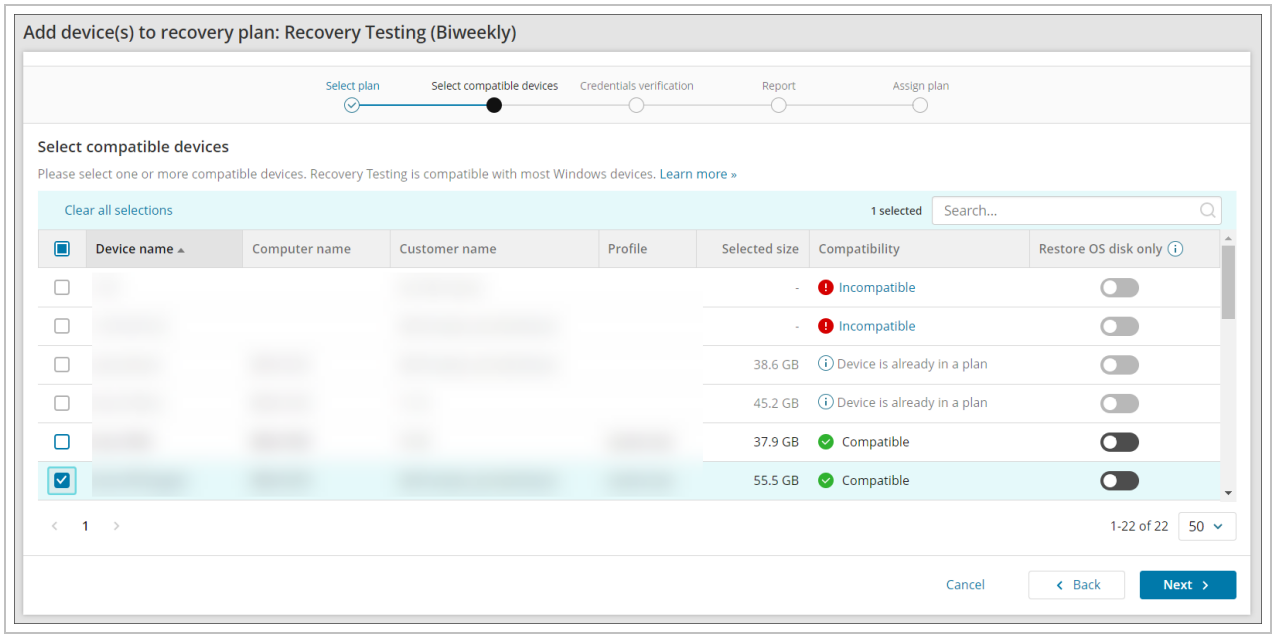
15. Click **Finish** to complete the process

From Recovery Testing Overview

To add Recovery Testing to devices from the dedicated Recovery Testing Overview:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Recovery Testing**
3. Click **Add to Plan**
4. Select the customer the device(s) you wish to apply the Recovery Testing plan belong to
5. Choose the restore frequency
    - Biweekly (every 14 days)
    - Monthly (every 30 days)
6. Click **Next**

7. Select all devices to apply the recovery testing plan



> In this window, it is possible to search compatible devices by Device Name, Customer Name and Profile

8. If you wish to skip all data drives, enable **Restore OS disk only**

> Use this function if the device is otherwise incompatible due to exceeding the 2TB selected size limitation

9. You will now be taken to the Add device to plan wizard. Follow the steps to enter the devices Security Code/Encryption Key starting at step #10 where you can now follow the above instructions to add the device to the plan

Recovery reports

When the device(s) assigned to the plan have **Successful recovery report email** or **Failed recovery report email** recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox.

Here is an example report **with** Cove branding:

Cove Data Protection

Recovery completed

Recovery plan: **Recovery Testing (Biweekly)**

Last recovery session completed successfully: March 20 2024 3:01:33 PM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	[redacted]
Device name	
Machine name	
Device type	Server
Operating system	Windows Server 2016 Standard Server (14393), 64-bit

RECOVERY OVERVIEW

Recovery session time	March 20 2024 3:01:33 PM
Recovery status	Completed
Recovery duration	21 minutes and 58 seconds
Recovery location	Germany
Recovery plan	Recovery Testing (Biweekly)
Screenshot verification	Completed

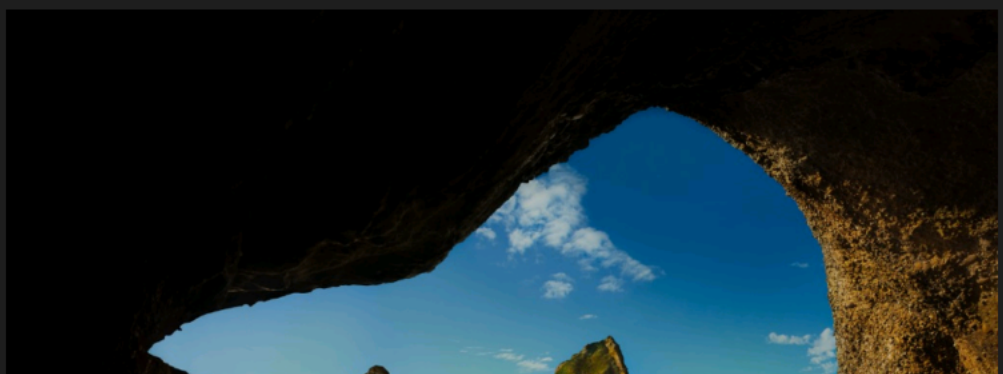
BACKUP DETAILS USED FOR THE RESTORE

Backup session time	March 20 2024 0:05:34 PM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

Below is a screenshot of the virtual machine created during the boot phase of recovery.



Here is an example **without** Cove branding:

Recovery completed

Recovery plan: **Recovery Testing (Biweekly)**

Last recovery session completed successfully: March 20 2024 3:01:33 PM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	[redacted]
Device name	
Machine name	
Device type	Server
Operating system	Windows Server 2016 Standard Server (14393), 64-bit

RECOVERY OVERVIEW

Recovery session time	March 20 2024 3:01:33 PM
Recovery status	Completed
Recovery duration	21 minutes and 58 seconds
Recovery location	Germany
Recovery plan	Recovery Testing (Biweekly)
Screenshot verification	Completed

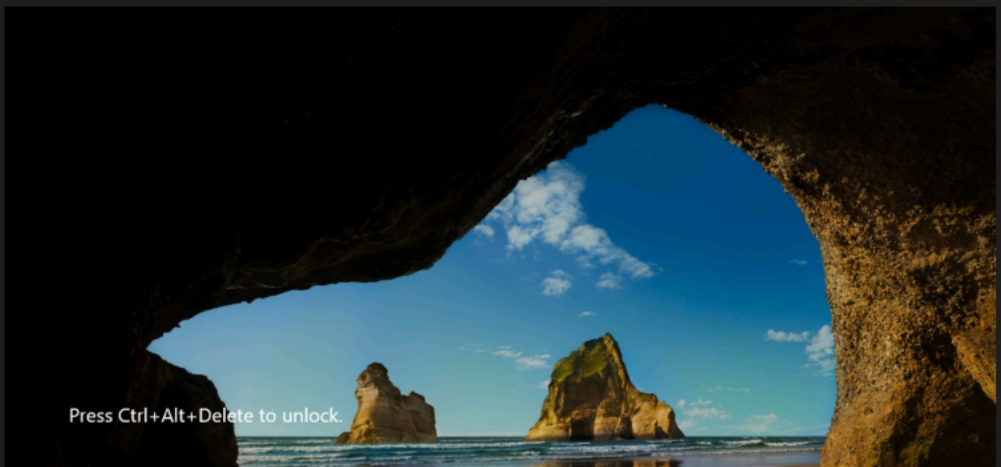
BACKUP DETAILS USED FOR THE RESTORE

Backup session time	March 20 2024 0:05:34 PM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

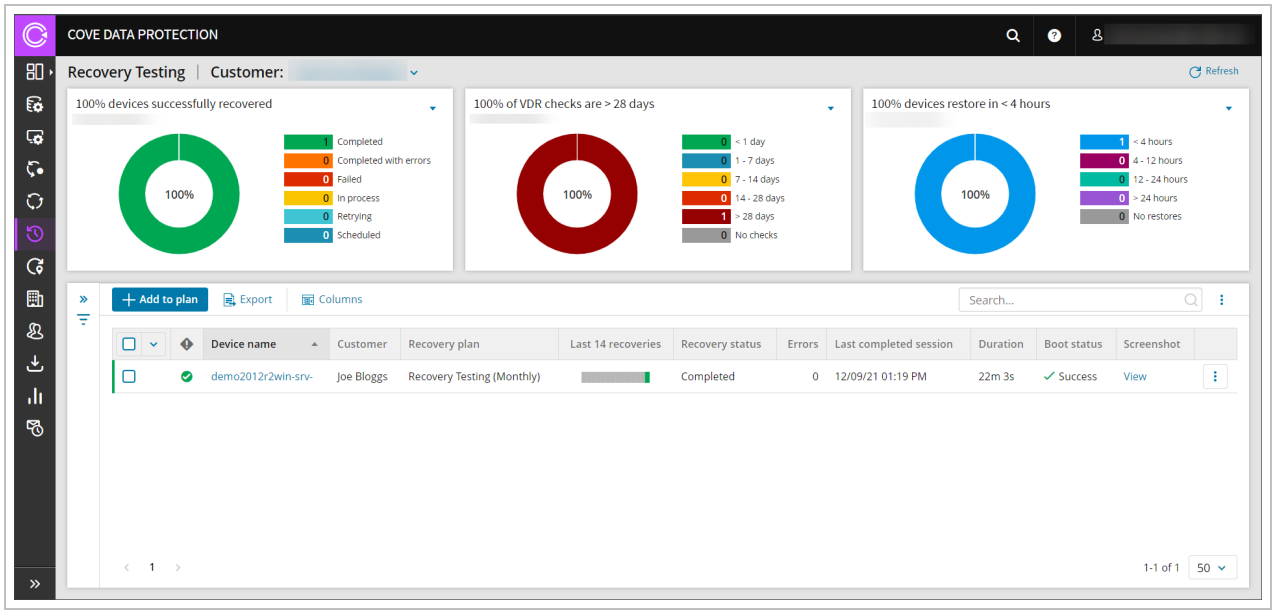
Below is a screenshot of the virtual machine created during the boot phase of recovery.



Monitor Recovery Testing Devices

From Recovery Testing Overview

From the Management Console, you can view the dedicated Recovery Testing overview by selecting **Continuity** > **Recovery Testing** from the vertical menu on the left hand side.

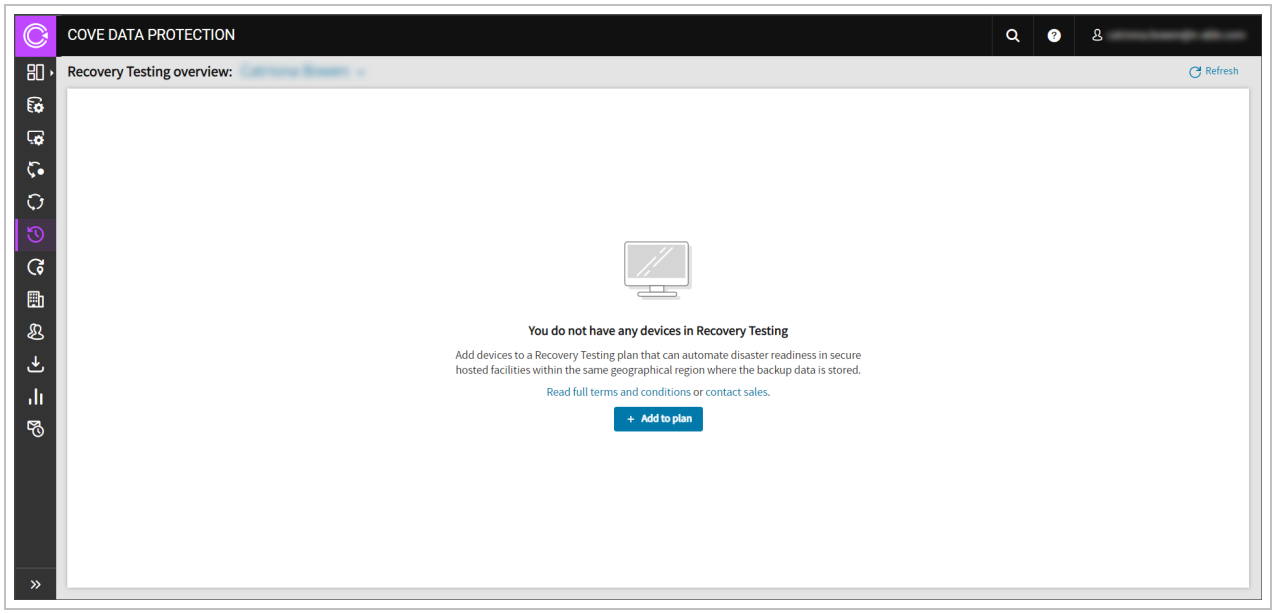


From this overview, you will see a specified set of columns detailing information relevant to Recovery Testing, including the continuity history of the last 14 recoveries, the status, and plan, along with some other information.

You can distinguish between Recovery Testing plans by the **Recovery Testing Plan** column. You will see one of two plan names:

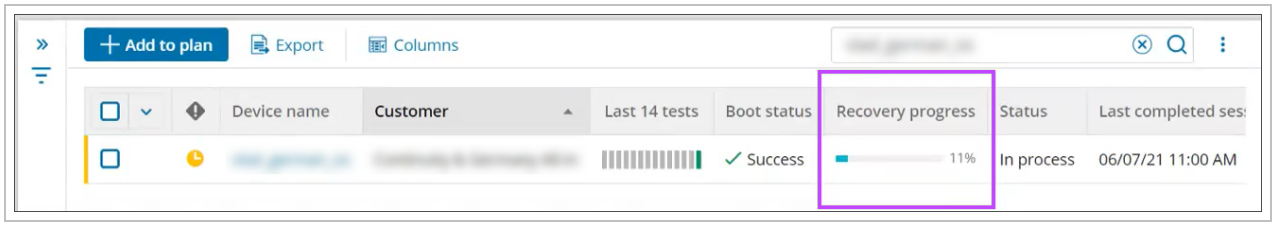
- Recovery Testing (Bi-Weekly)
- Recovery Testing (Monthly)

If no devices are assigned to the Recovery Testing, the overview will display a message to advise, along with a button to add devices to the plan.



Recovery Progress

From the Recovery Testing overview, the **Recovery Progress** column can be added, which will allow you to see the progress of the recovery as a percentage.



This column can be added by:

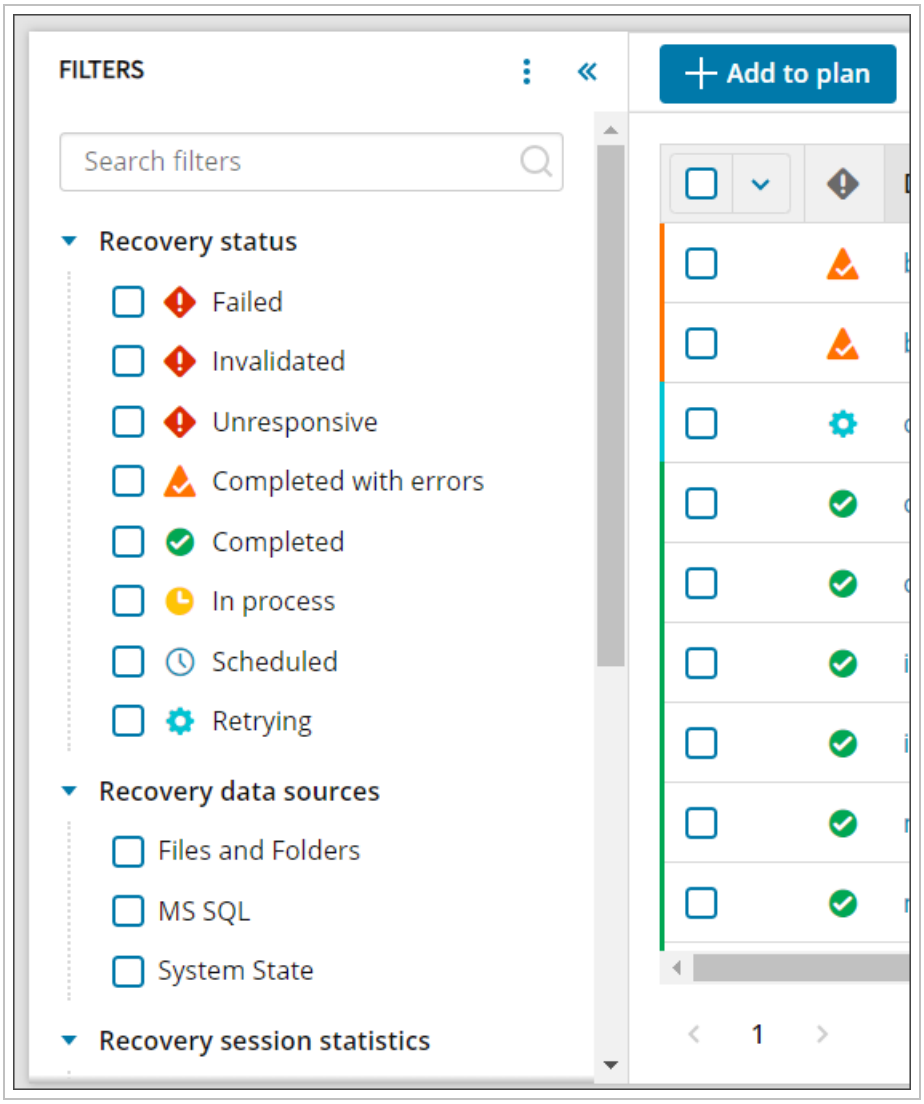
1. Selecting **Columns**
2. Search for and select **Recovery Progress**
3. Click **Save**

Searching

Searching within the Recovery Testing overview can be done by using the search box over to the right hand side of the page, just above the devices list. The search can be performed by any text field.

Filtering

The Recovery Testing overview also includes functionality to filter devices using the filter menu to the left of the device list and can be displayed or hidden by clicking the double arrows.



From this menu, you can filter by:

- Recovery status
  - Failed - The recovery session has failed
  - Invalidated - Device was moved to an inappropriate partner and so the session has failed
  - Unresponsive - The recovery session was initiated but did not get updates for at least 30 minutes and so the session has failed The recovery session was initiated but did not receive updates for at least 30 minutes because the recovery location was restarted or offline
  - Completed with errors - The recovery session completed, but encountered errors
  - Completed - The recovery session completed with no errors
  - In process - The recovery is currently in progress
  - Retrying - A restore session was not finished so the system is trying the restore again
  - Scheduled - Devices just added to a recovery plan and are waiting for their first recovery session or devices where restores were paused and have since been resumed will display as scheduled

- Recovery data sources
  - Files and Folders
  - MS SQL
  - System State
- Recovery testing session statistics
  - Boot Check Status
    - Success
    - Failed
    - Off
    - Unavailable for Local VHDX
  - Duration of the last completed recovery session
    - Sliding scale from 0 to unlimited
    in minutes
  - Number of errors of the last completed recovery session
    - Sliding scale from 0 to unlimited
  - Number of restored files
    - Sliding scale from 0 to unlimited
  - Number of selected files
    - Sliding scale from 0 to unlimited
  - Restored size
    - Sliding scale from 0 to unlimited
    in KB and GB
  - Screenshot
    - Available
    - Not Available
  - Selected size
    - Sliding scale from 0 to unlimited
    in KB and GB
  - Recovery testing status of the last completed recovery session
    - Failed
    - Completed with errors
    - Completed
  - Timestamp of the last completed recovery session
    - Quick Picks of:
      - Last day
      - 1 - 7 days
      - 7 - 14 days
      - 14 - 28 days
      - > 28 days
    - Custom range, select a stat date and time and an end date and time

Recovery status

- Failed - The recovery session has failed
- Invalidated - Device was moved to an inappropriate partner and so the session has failed
- Unresponsive - The recovery session was initiated but did not get updates for at least 30 minutes and so the session has failed
- Completed with errors - The recovery session completed, but encountered errors
- Completed - The recovery session completed with no errors
- In process - The recovery is currently in progress
- Retrying - A restore session was not finished so the system is trying the restore again
- Scheduled - Devices just added to a recovery plan and are waiting for their first recovery session or devices where restores were paused and have since been resumed will display as scheduled

Recovery data sources

- Exchange
- Files and Folders
- MS SQL
- SharePoint
- System State

Recovery testing session statistics

- Boot Status
  - Success
  - Failed
  - Off
  - Unavailable for Local VHDX
- Duration of the last completed recovery session
  - Sliding scale from 0 to unlimited

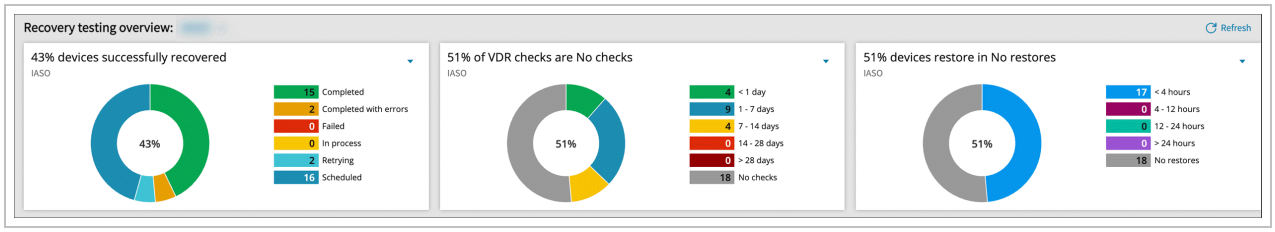
  in minutes
- Number of errors of the last completed recovery session
  - Sliding scale from 0 to unlimited
- Number of restored files
  - Sliding scale from 0 to unlimited
- Number of selected files
  - Sliding scale from 0 to unlimited
- Continuous restores
  - Paused
  - Running
- Recovery Location name
  - Select the Recovery Location name from the dropdown
- Restored size
  - Sliding scale from 0 to unlimited

  in KB and GB

- Screenshot
  - Available
  - Not Available
- Selected size
  - Sliding scale from 0 to unlimited
  in KB and GB
- Recovery testing status of the last completed recovery session
  - Failed
  - Completed with errors
  - Completed
- Timestamp of the last completed recovery session
  - Quick Picks of:
    - Last day
    - 1 - 7 days
    - 7 - 14 days
    - 14 - 28 days
    - > 28 days
  - Custom range, select a stat date and time and an end date and time

Widgets

Three widgets can be maximized at the top of the page, which allow for further filtering:



Device recovery status

This widget allows you to filter the devices by recovery status:

- Completed
- Completed with errors
- Failed
- In process
- Retrying
- Scheduled

VDR checks time frame

This widget allows you to see the percentage of devices whose recovery check completed within the following day ranges:

- < 1 day
- 1 - 7 days
- 7 - 14 days
- 14 - 28 days
- > 28 days
- No checks

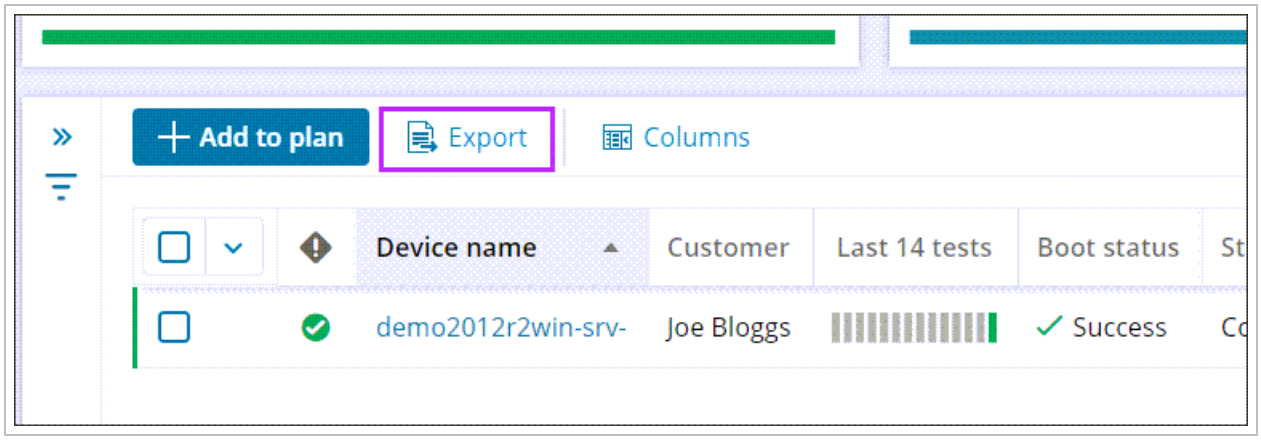
Device restore time frame

From this widget, you can filter devices by the how recent restores are done by the following time frames:

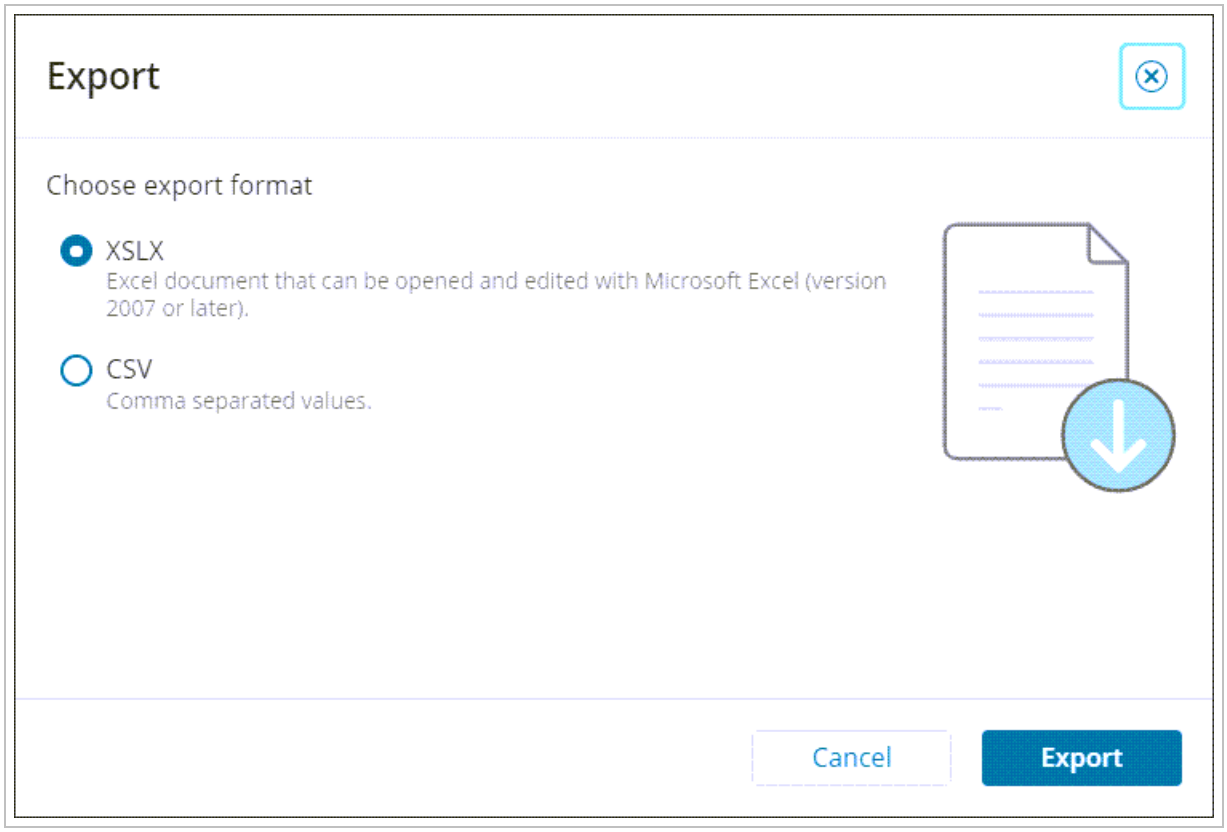
- < 4 hours
- 4 - 12 hours
- 12 - 24 hours
- > 24 hours
- No restores

Exporting

You may export a list of devices currently assigned a plan by clicking **Export**

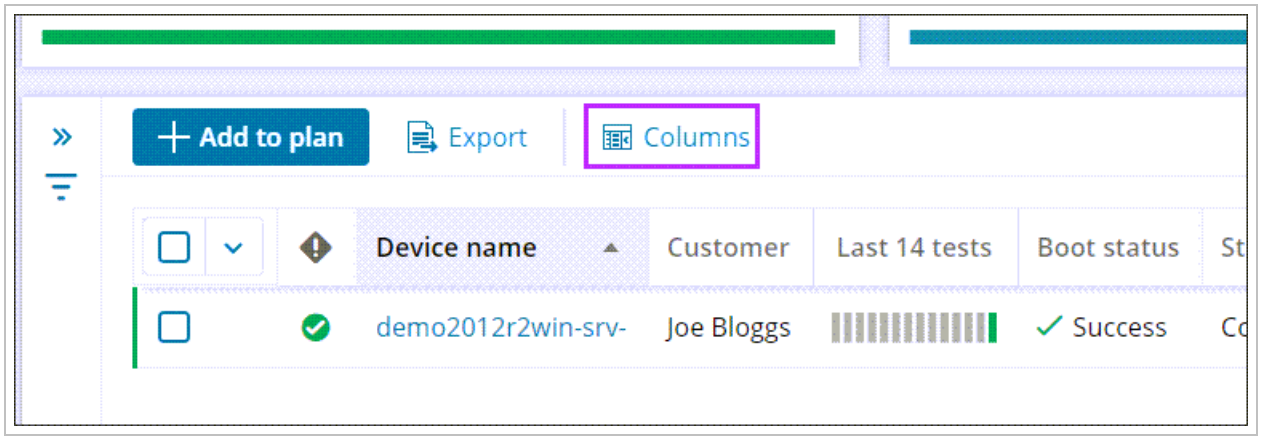


This will then provide a separate dialog where you can choose to export in either XSLX or CSV.

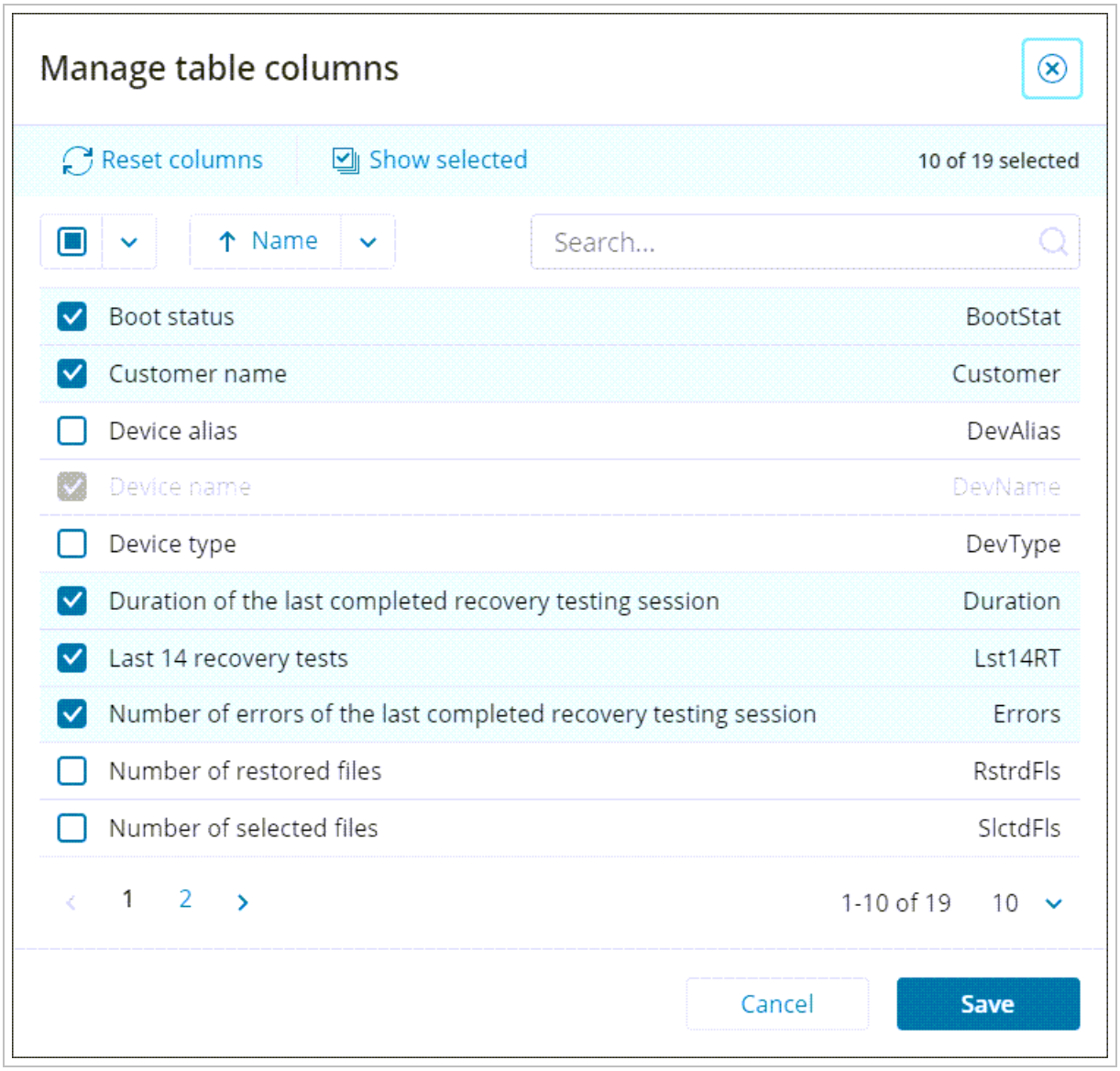


Manage Table Columns

Management Console allows you to manage the tables columns that can be seen within the Recovery Testing overview.



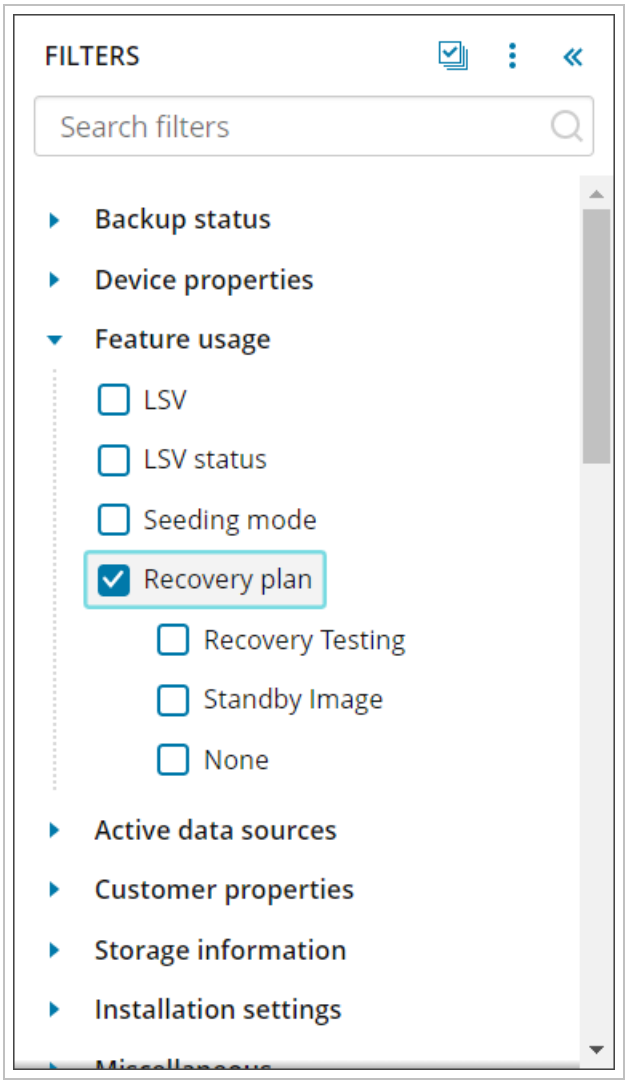
In the Manage table columns dialog, you can select and deselect columns based on the information you wish to view from the dashboard.



From Main Dashboard

Users of all roles can view devices in the Console with Recovery Testing enabled. They appear as regular Backup Manager devices in **Backup > Dashboard** and can be found by filtering in the Beta Dashboard:

1. Expand the **Filters** pane on the left of the Toolbar
2. Search for **Recovery Plan** in the **Feature Usage** section



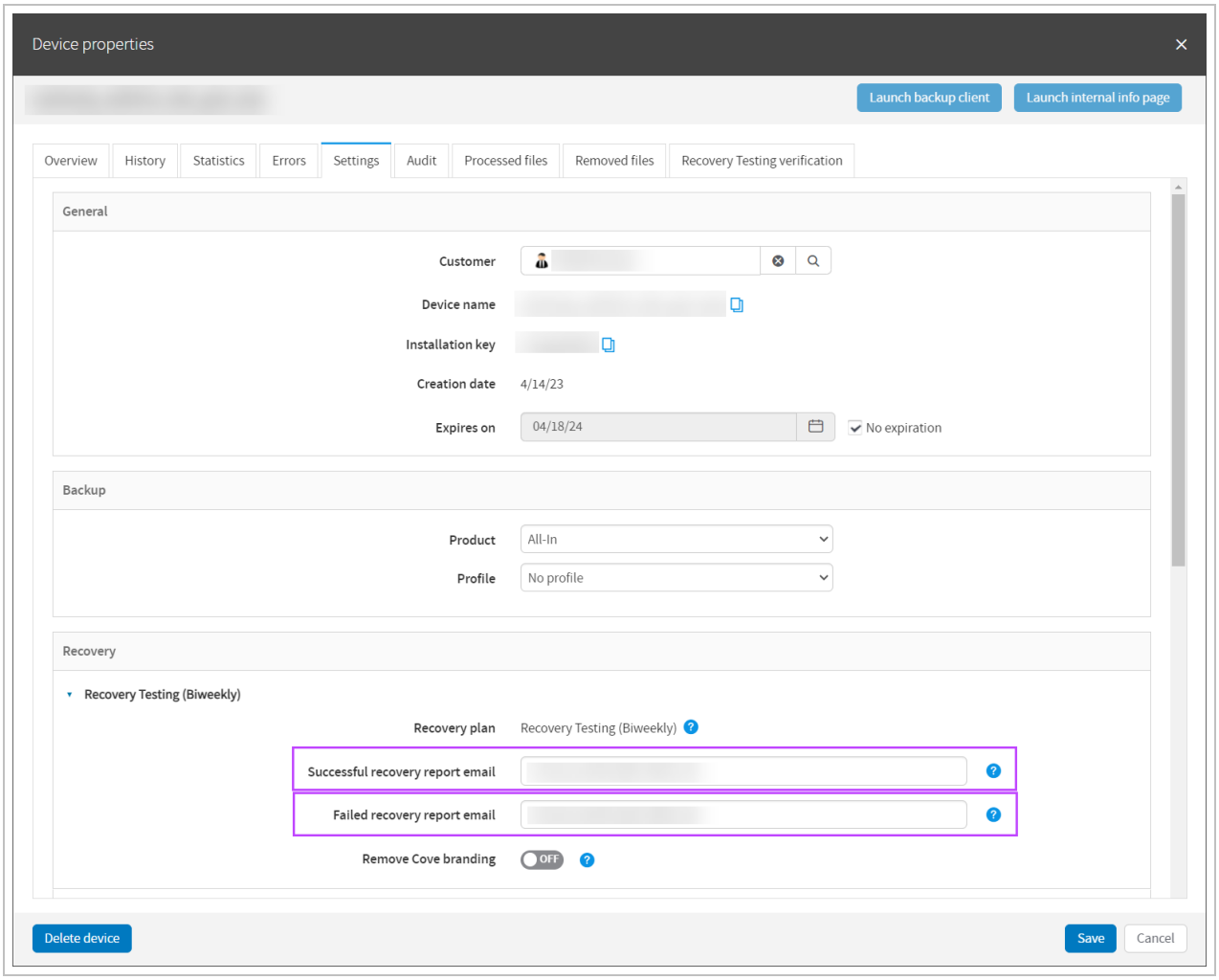
3. Tick the **Recovery Testing** plan

> Your devices list will automatically update to show only devices where the Recovery Testing plan is enabled.

Accessing device properties

As with any normal device, when you click on the device name, you will see the Device Properties dialogue. If the device is assigned to a plan, details of this will be visible in a Recovery section.

You can also add, remove, or amend the **Successful recovery report email** and **Failed recovery report email** recipient email addresses from here as well as toggle **Cove branding** on the reports on or off.



View results and check screenshots

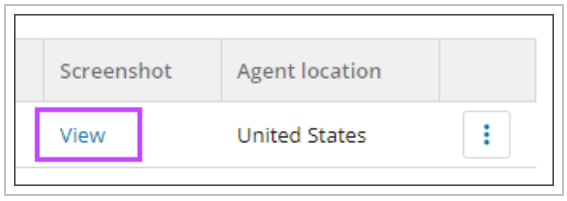
To view statistics of the Recovery Testing and check the screenshots to ensure this has been successful, you can view this by following one of the below methods:

From Device Properties

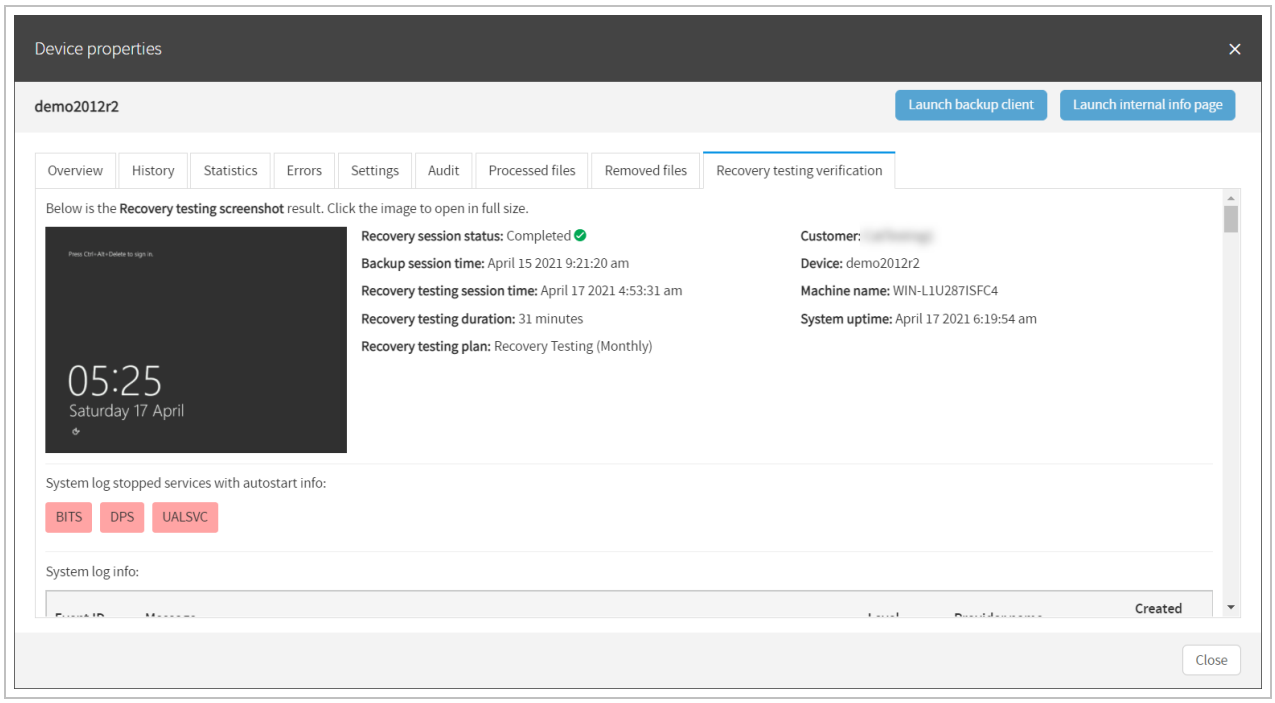
1. Log in to the Management Console under a **SuperUser** account
2. Click the device name to open Device Properties
3. Navigate to the **Recovery Testing Verification** tab

From Recovery Testing Overview

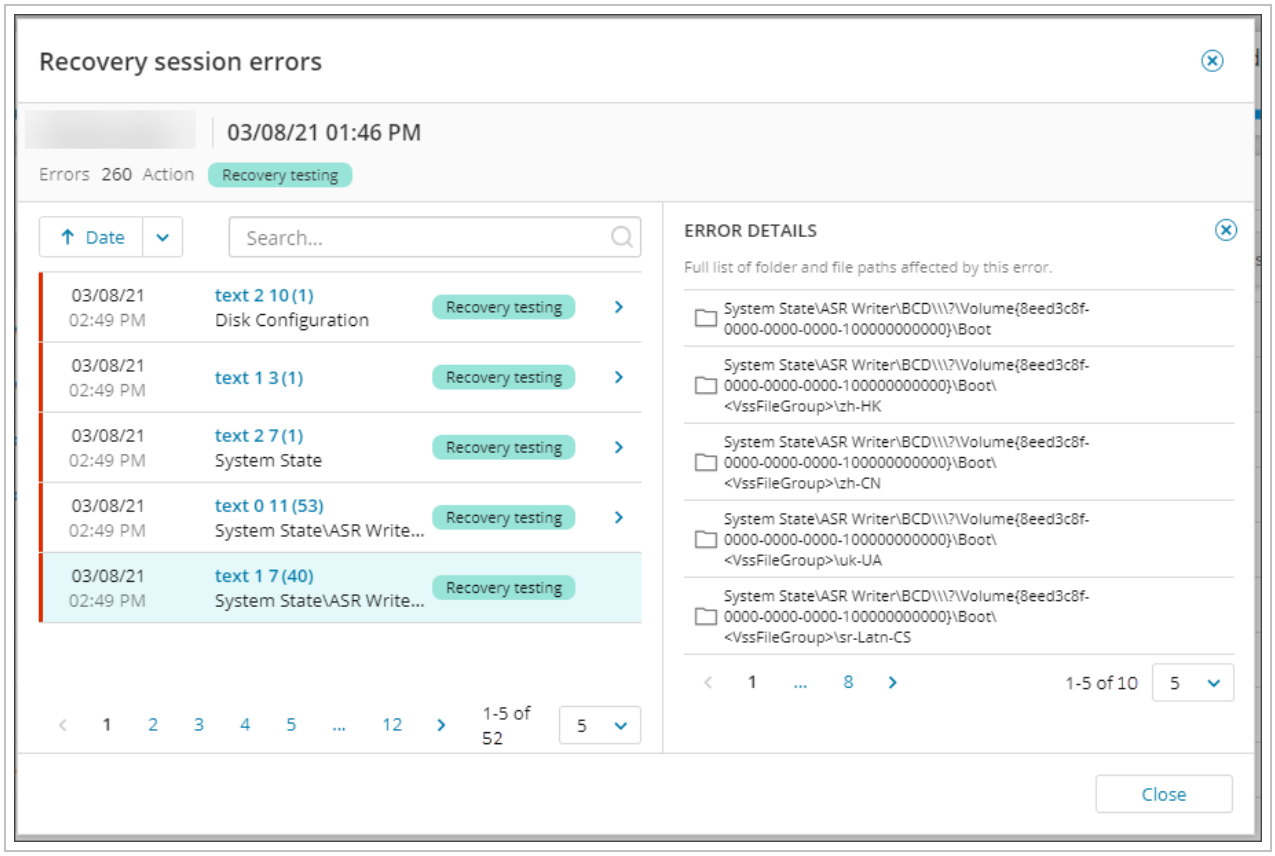
1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Testing**
3. Click **View** under the Screenshot column



4. This will take you in to the Device Properties dialogue, where you will now see the **Recovery testing verification** tab:



If an error was found during the recovery, you can view a wider look at the error details from the Recovery session errors dialog box.



This can be accessed by hovering over the recovery session with the error and selecting to show the Recovery session errors.

Recovery Testing Verification

In the **Recovery Testing Verification** tab you will see the screenshot taken from the virtual machine during the boot phase of Recovery Testing.

In this tab, you will also see information on the device, such as system uptime, when the session was last recovered, services that were stopped in order to perform the recovery and system log information.

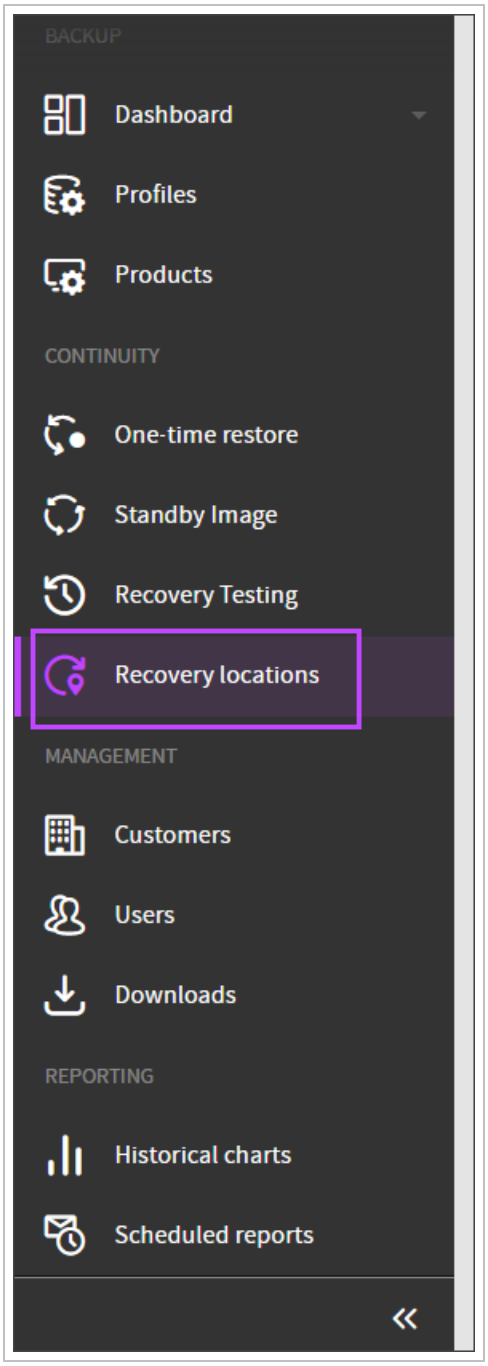
You can find full details on device statistics and what each tab is used for here.

> In the case of a failed test recovery, the captured screenshot may not display the error or state that caused the failure. To understand the cause of the failed restore, we recommend using the virtual recovery option in the Backup Manager or Recovery Console to recreate and diagnose the issue.

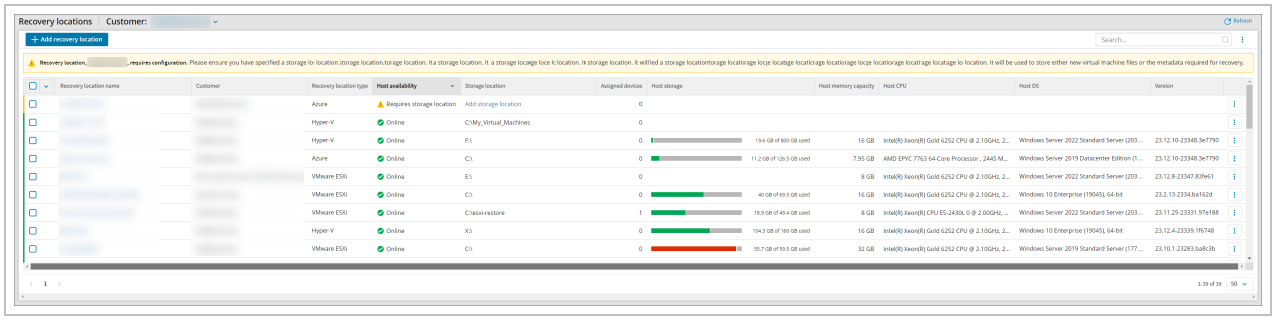
Recovery Locations

Recovery Locations, the host running the recovery service and processing data restores, can be added, edited, and deleted in the **Recovery Locations** page of the Management Console. They can be added prior to adding devices to the Standby Image plan, or on the first step of the Top bar menu, Enable Standby Image to AzureDevices cannot be added to a Standby Image plan if already assigned to a Recovery Testing plan.Devices can be assigned to multiple Standby Image plans at once, i.e. Standby Image to Hyper-V and Standby Image to Azure. From Main DashboardTo enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:Log in to the Management Console under a SuperUser or Manager account In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan toClick Add to recovery plan from the Toolbar Select Standby Image (Azure)Select the customer the device(s) you wish to apply the Standby Image plan belong toChoose the recovery location as was configured in Add Recovery LocationsIf the selected customer does not have any locations, you must add one before continuing by selecting Add recovery location. See Add Recovery Locations for full details of adding a location.It is not possible to assign a location for which the Host availability is "Offline"Click NextConfirm the device selected from the Dashboard is compatible and click Next Enter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereClick Next to continueChoose the boot check frequency:OffEvery recovery sessionDailyWeeklyBiweeklyMonthlyIf you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Once connected, click NextClick Azure VM settings towards the right-hand side of the screen to open the settings configuration window:Configure the Azure VM Settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk typeData disk(s) typeVirtual NetworkSubnetAssign NSG and public IPDuring the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend blocking internet access for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.Click Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowConfirm assigning the plan to the device(s)Wait for the plan to be assigned until you see a confirmation banner on the pageClick FinishFrom Standby Image OverviewLog in to the Management Console under a SuperUser or Manager accountNavigate to Continuity > Standby ImageClick Add to PlanSelect Standby Image (Azure)You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the planRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding: and Top bar menu wizards.

The Recovery Locations page can be found on the Management Console under the **Continuity** section:



The page displays several pieces of information relating to previously created recovery locations.



The columns displayed are:

- Recovery location name
- Customer
- Recovery location type
  - Azure
  - Hyper-V
  - VMware ESXi
- Host availability
  - Offline
  - Online
  - Requires a storage drive

    > Drive is required for Standby Image and Recovery Testing locations as this is the location in the file system where the new Virtual Machine files will be created. This is not required for Azure and ESXi locations
- Storage location

  > For Hyper-V, this can be added by clicking **Add storage location**, entering the drive letter or local path in the box and clicking **Save**
- Assigned devices
- Host storage
- Host memory capacity
- Host CPU
- Host OS
- Version

Minimum Requirements

For Standby Image and Recovery Testing, Windows Admin Center must be installed on the management machine, available here.

> This is not required for One-Time Restore.

Default Hardware Configuration

By default, each Recovery Location is configured to run 5 restores in parallel with a target VM size of 4 CPU cores and 4 GB of RAM. The following minimal configuration is recommended depending on the restore target:

- Hyper-V and ESXi
  - **CPU** - 22 Cores or more
  - **RAM** - 32 GB or more
  - **Restore Target Drive Capacity** - more than two times the size of the selected size of all devices combined
- Local VHD and Azure
  - **CPU** - 12 Cores or more
  - **RAM** - 16 GB or more
  - **Restore Target Drive Capacity** - more than two times the size of the selected size of all devices combined

Single device restore

To start Recovery Service on a Windows Server and run a single device restore we recommend the following hardware configuration, depending on the restore format:

- Hyper-V and ESXi
  - **CPU** - 6 Cores or more
  - **RAM** - 6 GB or more
  - **Restore Target Drive Capacity** - more than two times the size of the backed up data
- Local VHD and Azure
  - **CPU** - 4 Cores or more
  - **RAM** - 5 GB or more
  - **Restore Target Drive Capacity** - more than two times the size of the backed up data

> Also, make sure that Recovery Location operating system conforms to the requirements stated here: Virtual Disaster Recovery Requirements

Azure Requirements

To install the Recovery Location's recovery service on an Azure VM, the following requirements are necessary:

- A user created for you in your Azure tenant. The user must:
  - Have access to a subscription
  - Have access to a resource group you want to use to keep the Recovery Location VM and restored (target) Azure VMs
  - Be able to assign permissions on virtual machines within the resource group

Additional resources for more devices

The default number of parallel restores can be adjusted depending on the hardware you use for the Standby Image Recovery Location. When configuring each recovery location, it is important to do this in a way it is neither too big (as it might slow down the restore because the host will be overloaded) nor too low (as in this case you might not use the full capacity of your computing resources and hence receive a slower than ideal performance).

While network bandwidth and disk IOPS don't have any strict requirements to run the Standby Image Recovery Service it does directly affect the restore speed and low resources can cause poor performance.

CPU and RAM might be a blocker to adding more restores in parallel. If you do not have enough CPU and/or RAM it is possible to see performance degradation, failing restores, or Virtual Machine boot issues due to “out of memory“ errors.

We recommend reserving the following additional resources for **each extra device** when configuring a number of parallel restores:

- Hyper-V and ESXi
  - **CPU** - 4 cores
  - **RAM** - 4 GB
- Local VHD and Azure
  - **CPU** - 2 cores
  - **RAM** - 2 GB

> The requirements mentioned above are recommendations. You may set the number of cores and memory at your discretion, however, taking into account the recommendations above.
>
> If you have already had experience using Recovery Console and have a suitable configuration, it is possible to use the same configuration for Standby Image when taking into account the recovery of the same number of devices of a similar configuration.

Recommendations for Maximum Performance

Hardware

When running multiple restores in parallel, we recommend the following to increase the performance of each machine:

- Use SSD disks with higher IOPs
- A fast network connection with good bandwidth

Both the **target disk** and **system disk** should have enough performance as the system disk may be used by system services and Hyper-V.

Hypervisor Configuration

While required to effectively mitigate certain classes of vulnerabilities, the **core scheduler** (enabled by default for Windows Server 2019 and newer) may also potentially reduce performance. We recommend changing the scheduler to **Classic** to increase performance.

> This action should be done along with applying appropriate security controls to mitigate risks raised by this change.

> The free Hyper-V Server 2019 ISO can be found here.

Anti-Virus Recommended Exclusions

The following are recommended to add to the anti-virus exclusions list to allow for successful backups:

Recovery Service Exclusions

- `AuthTool.exe [file] SYSTEM_DRIVE:\Program Files\Recovery Service\*\AuthTool.exe`
- `unified_entry.exe [file]. SYSTEM_DRIVE:\Program Files\Recovery Service\*\unified_entry.exe`
- `RecoveryFP.exe [file] SYSTEM_DRIVE:\Program Files\Recovery Service\*\BM\RecoveryFP.exe`
- `VdrAgent.exe [file] SYSTEM_DRIVE:\Program Files\Recovery Service\*\BM\VdrAgent.exe`
- `ProcessController.exe [file] SYSTEM_DRIVE:\Program Files\Recovery Service\*\BM\ProcessController.exe`
- `ClientTool.exe [file] SYSTEM_DRIVE:\Program Files\Recovery Service\*\BM\ClientTool.exe`

Virtual Machines Exclusions

- `*.vhd RESTORE_TARGET_DRIVE\StandbyImage\*\vm\*.vhd`
- `*.vhdx RESTORE_TARGET_DRIVE\StandbyImage\*\vm\*.vhdx`

Hyper-V Processes Exclusions

- `%ProgramData%\Microsoft\Windows\Hyper-V [folder]`
- `Vmms [process]. %systemroot%\System32\Vmms.exe`
- `Vmwp [process]. %systemroot%\System32\Vmwp.exe`
- `Vmsp [process]. %systemroot%\System32\Vmsp.exe`
- `Vmcompute [process]. %systemroot%\System32\Vmcompute.exe`

System Network Configuration

When running a large number of parallel restores on the same recovery location, (around 50) a lot of network connections may be utilized. In order to improve the performance and stability of such heavily loaded systems it is recommend to adjust network configuration in the following way:

1. Increase ephemeral ports count, set up new values:
   a. `start = 20000`
   b. `number of ports = 45000`
2. Reduce `TcpTimedWaitDelay` to **5 seconds**

> See details here: Settings that can be Modified to Improve Network Performance - BizTalk Server

Add Recovery Locations

Instructions for how to Configure N-able Recovery Service on Azure Recovery Locations must be followed specifically, due to several differences in the Azure configuration.

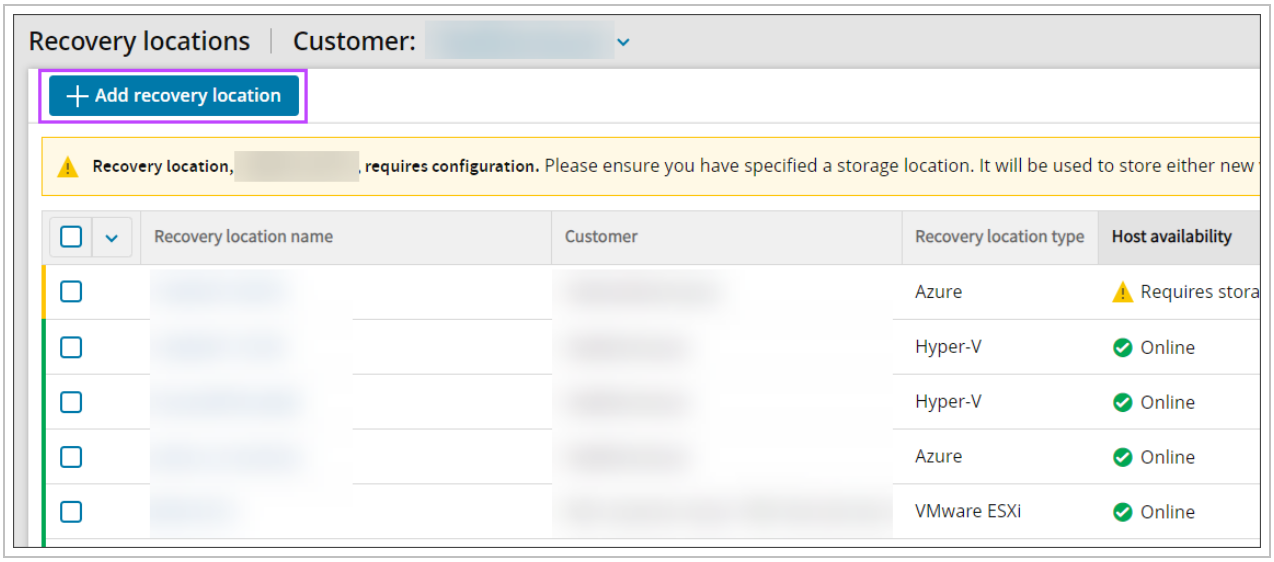
Instructions for how to Configure N-able Recovery Service on ESXi Host Server must followed specifically, due to several differences in the ESXi server configuration.

Instructions for how to Configure N-able Recovery Service on Hyper-V Server 2019 must be followed specifically, due to several differences in the Hyper-V 2019 server configuration.

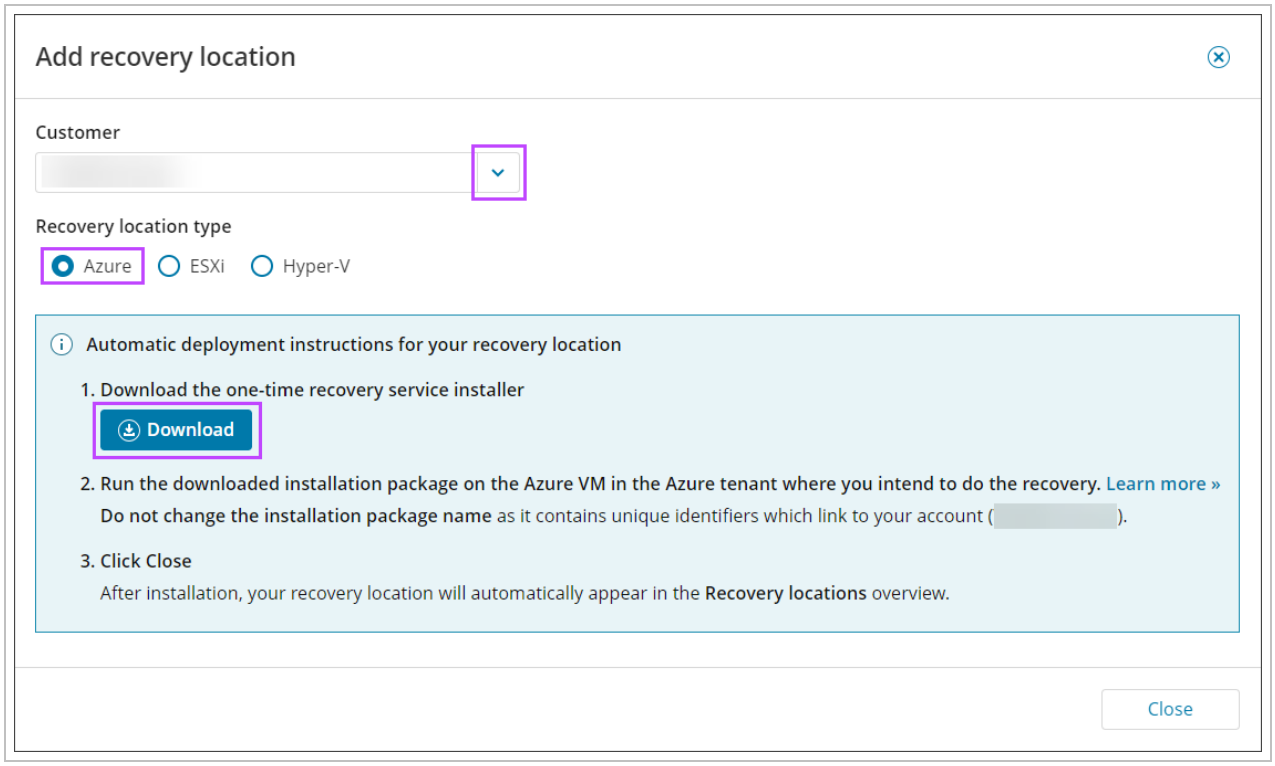
Create Recovery Locations

Azure

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Click **Add recovery location** at the top of the page



4. In the **Add Recovery Location wizard**, select the customer to attribute the recovery location to, from the dropdown



5. Select **Azure** as the Recovery Location Type
6. Download the recovery service installer and save it to an easily found place on your device

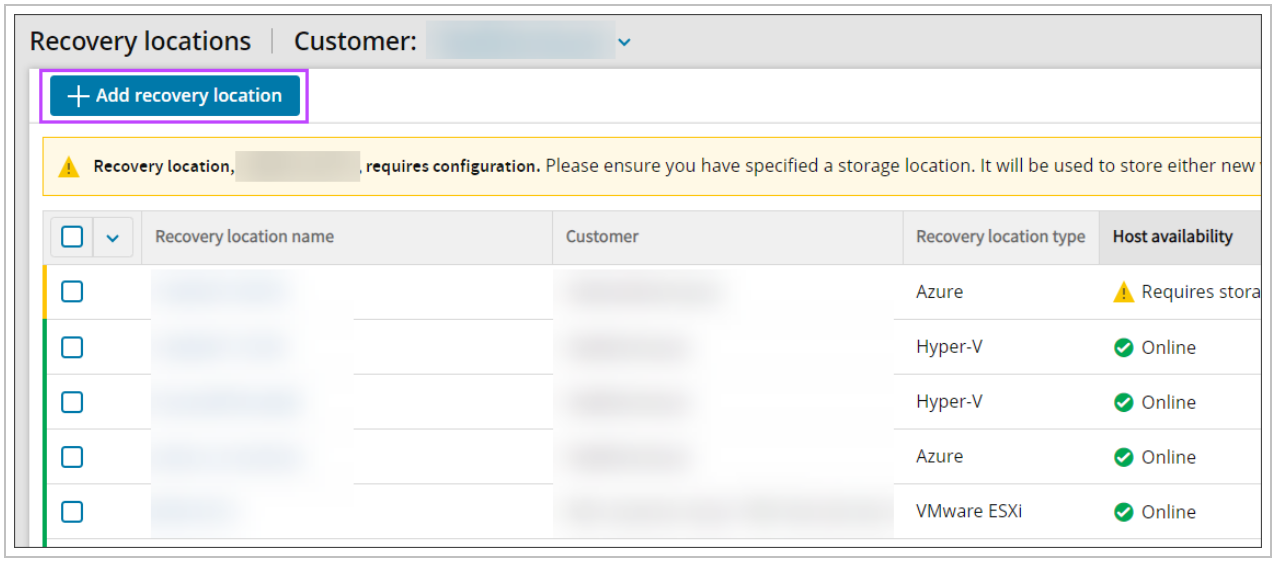
> Do **not** change the installation package name. The installation package name contains unique identifiers to your account.
>
> This is a one-time installer and can only be used to install a single instance of the recover service. The installer will fail if you attempt to use the same package for another installation.

7. Continue following the instructions on how to Create the Recovery Location VM
8. Then Installing and Configuring the Recovery Location on the Azure VM
9. Followed by Assigning Permissions to the Recovery Location VM

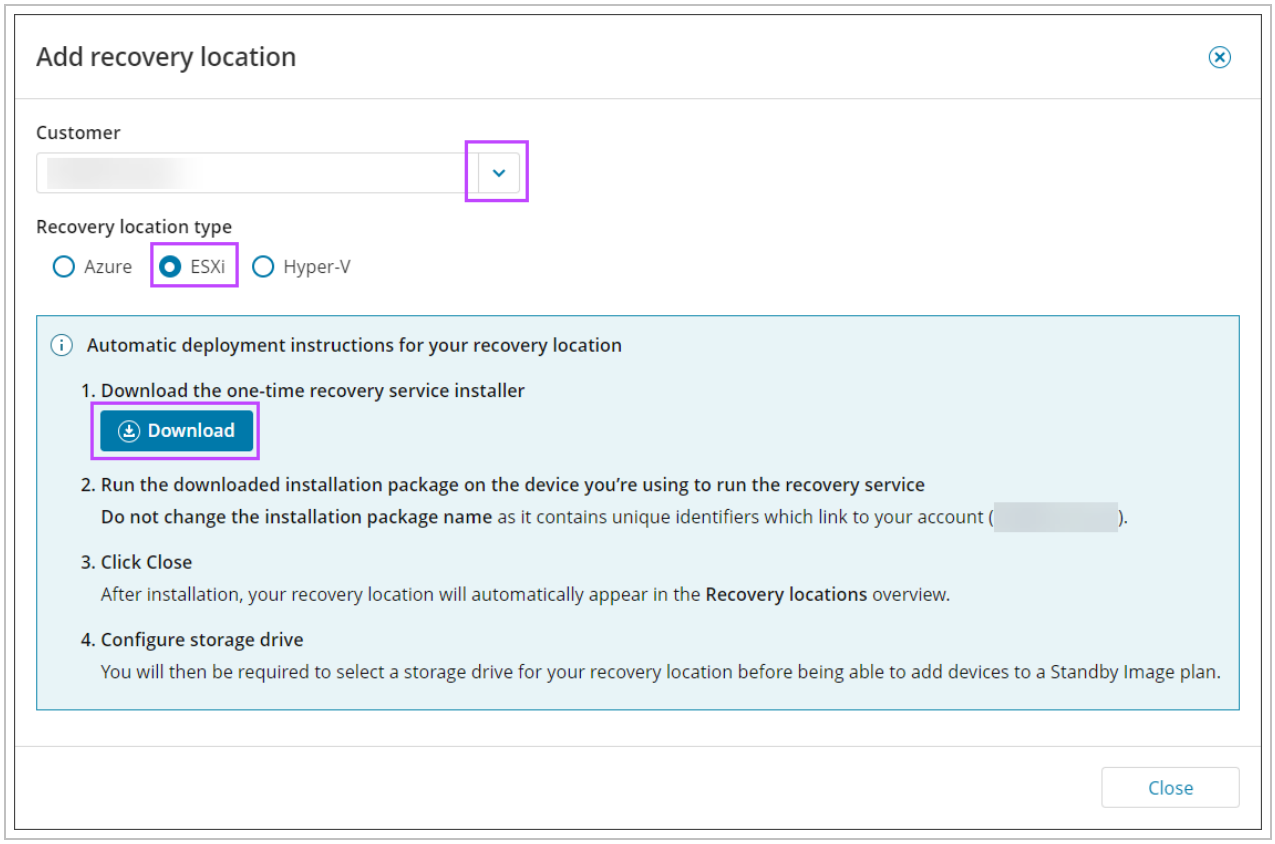
Only once location VMs are created, installed, configured and all permissions given, can you begin the One-Time Restore or Standby Image to Azure.

ESXi

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Click **Add recovery location** at the top of the page



4. In the **Add Recovery Location wizard**, select the customer to attribute the recovery location to from the dropdown



5. Select **ESXi** as the recovery location type
6. Download the recovery service installer

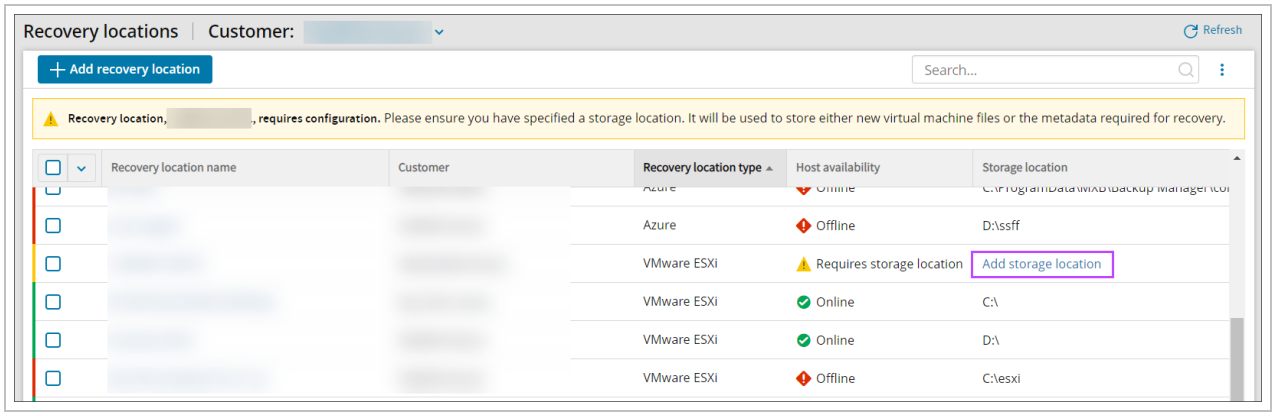
> Do **not** change the installation package name. The installation package name contains unique identifiers to your account.
>
> This is a one-time installer and can only be used to install a single instance of the recovery service. The installer will fail if you attempt to use the same package for another installation.

7. Run the downloaded installation package on the Virtual Machine as created in Step 3: Create Recovery Location Virtual Machine

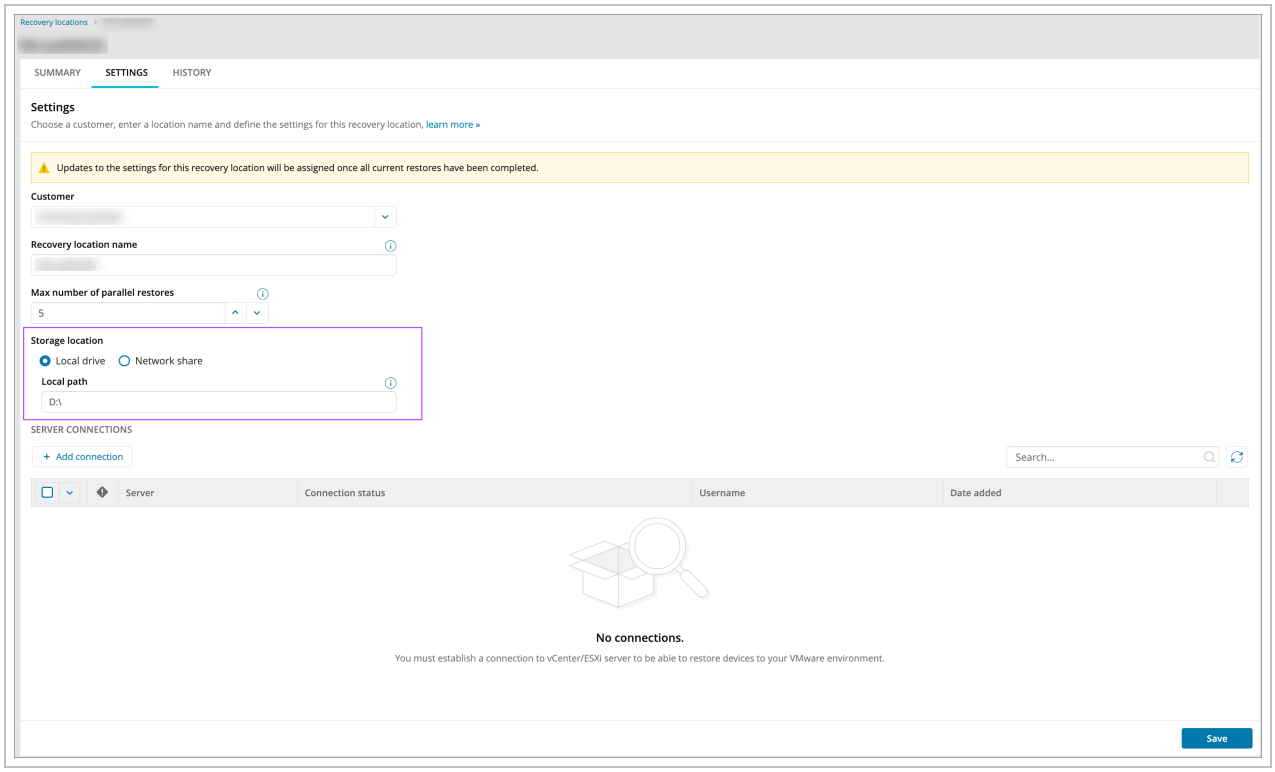
> The recovery location will appear in the list after installation is complete

Add Storage Location and Server Connections

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Find the new recovery location in the list and click **Add storage location**

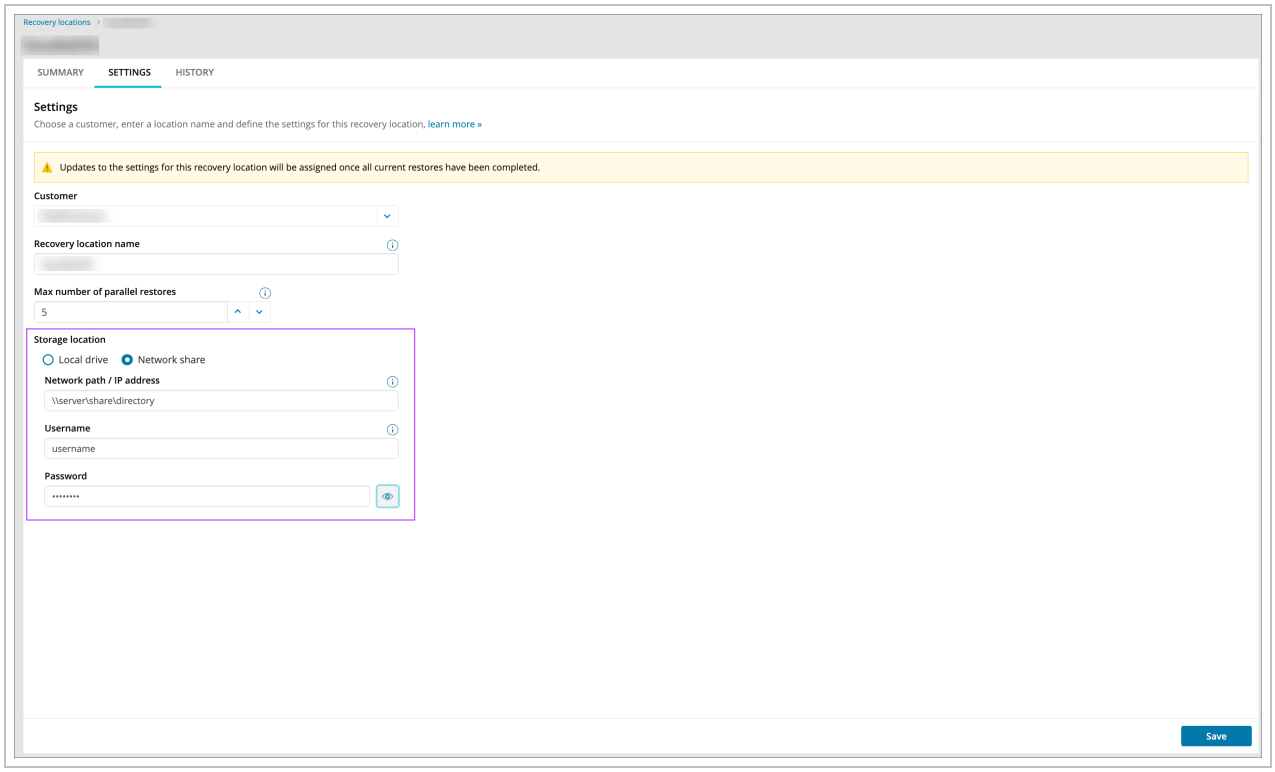


4. Provide local file path for the storage location
   - Local Drive:



> Without a storage location, connections **cannot** be made to any of the added servers. If you want to restore to Local VMDK is not obligatory to configure server connections. The VMDK file will be restored directly to the storage path, and not on the ESXi server.

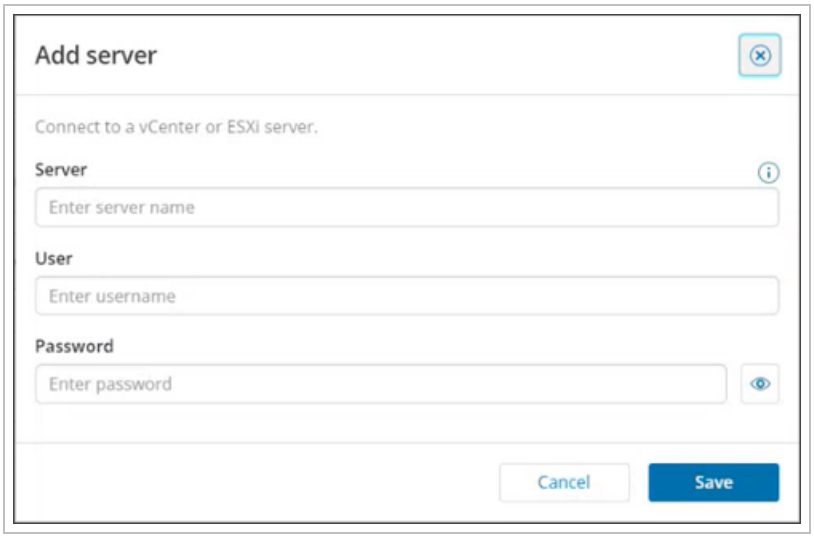
- Network Share:



> Recovery Locations using **Network Shares** will **not** see the option to configure any server connections as the restore will not be done on an ESXi server, and will be done on the Network Share to a Local VMDK restore format.

5. Click **Add Connection** to connect to the vCenter or ESXi server

> If using a connection to the vCenter server, you will be able to restore to any ESXi host connected to the vCenter server



6. Enter the vCenter or ESXi **server name** or **IP address**, and your username and password for this
7. Click **Save**

> Multiple server connections can be added to the recovery location, but must be done one at a time. Doing so will allow you to connect and restore to several ESXi hosts which are not connected to one vCenter Server

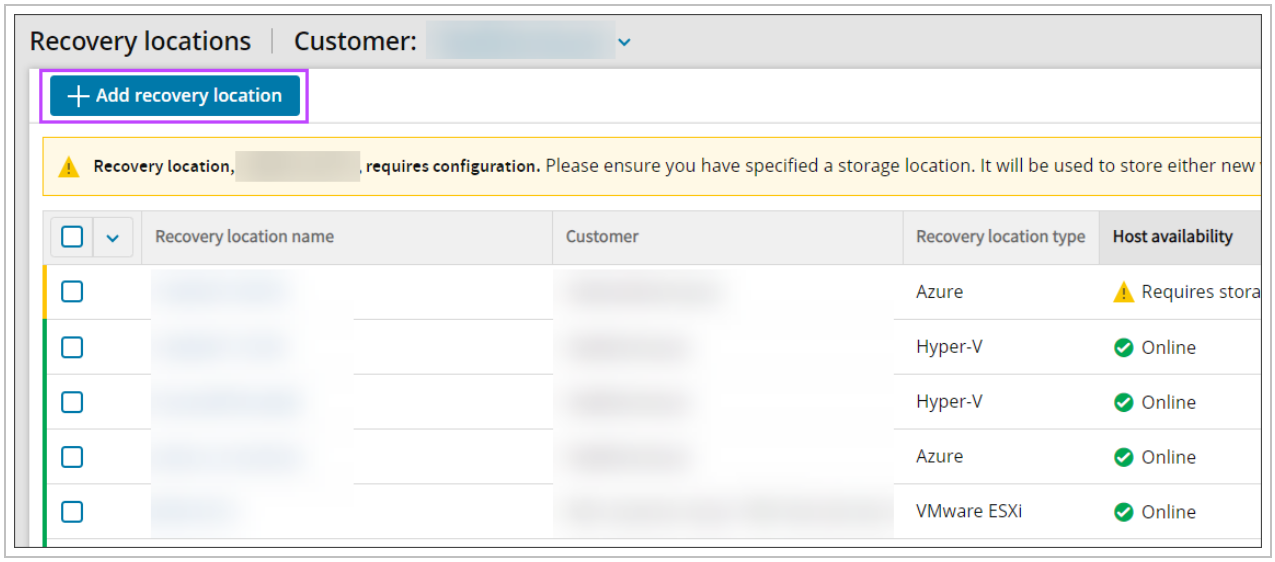
> You must click the **refresh** button to above the list of server connections to update the status from 'connecting' to 'connected'. The connection may take a few minutes.

Once locations are added, you may continue with adding devices to the Standby Image plan.

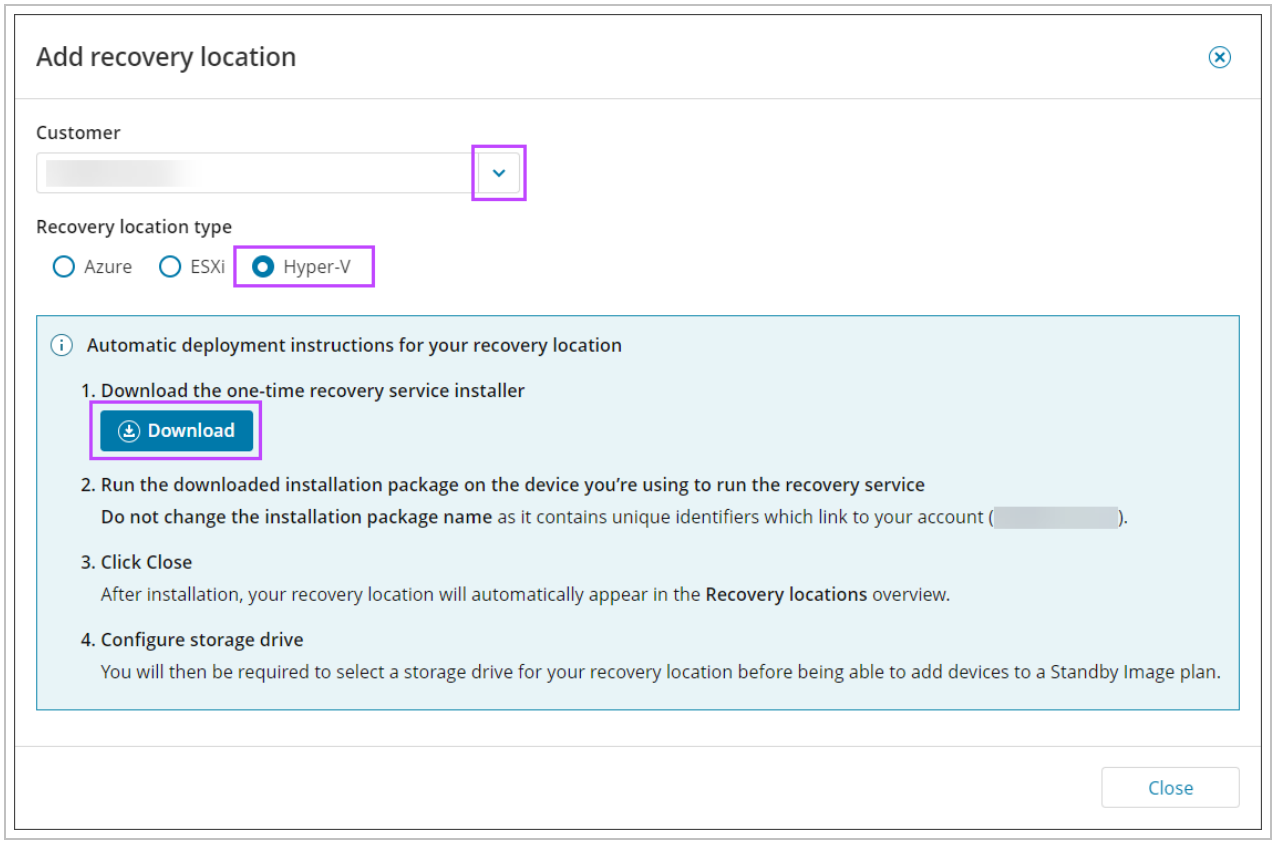
> Installing the Recovery Locations recovery service on an ESXi Host server requires additional configuration during the setup of the environment. See here for instructions on configuration of the recovery service on ESXi Host Servers.

Hyper-V

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Click **Add recovery location** at the top of the page



4. In the **Add Recovery Location wizard**, select the customer to attribute the recovery location to from the dropdown



5. Select **Hyper-V** as the recovery location type
6. Download the recovery service installer

> Do **not** change the installation package name. The installation package name contains unique identifiers to your account.
>
> This is a one-time installer and can only be used to install a single instance of the recovery service. The installer will fail if you attempt to use the same package for another installation.

7. Run the downloaded installation package on the device where the Virtual Machines should be restored to

> The recovery location will appear in the list after installation is complete

8. Give the recovery location a storage location by:
   a. Click **Add storage location**
   b. Enter the drive letter or local path to the folder where your virtual machine files will be stored in the box
   c. Click **Save**

Once locations are added, you may continue with adding devices to the Standby Image plan.

> Installing the Recovery Locations recovery service on a Hyper-V Server 2019 requires additional configuration during the setup of the Hyper-V. See here for instructions on configuration of the recovery service on Hyper-V Server 2019.

Add Device to Recovery Location

Devices can be added to a Recovery Location from the **Continuity** > **Recovery Locations** page, thereby enabling the Standby Image Plan, using one of three methods:

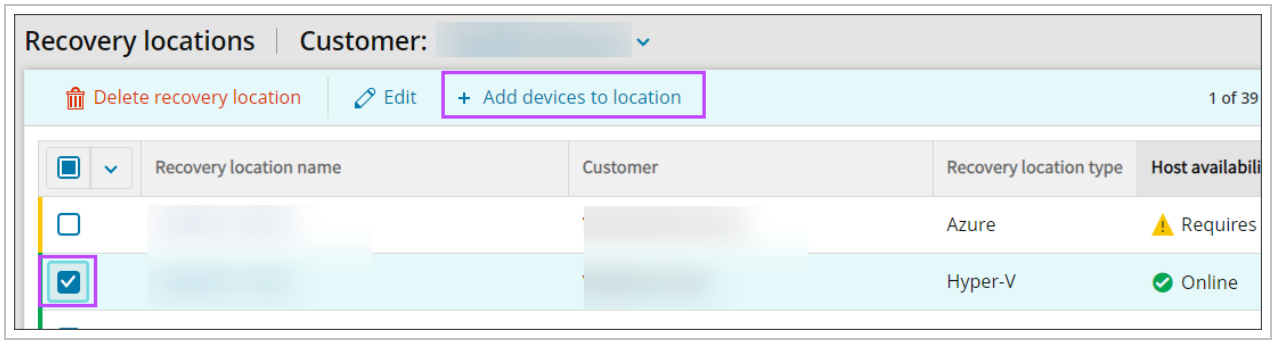
- Top bar menu
- Location context menu
- Right-hand menu

> These will only be available if the Recovery Location is **Online**.

Top bar menu

Available for Hyper-V and ESXi Locations **only**.

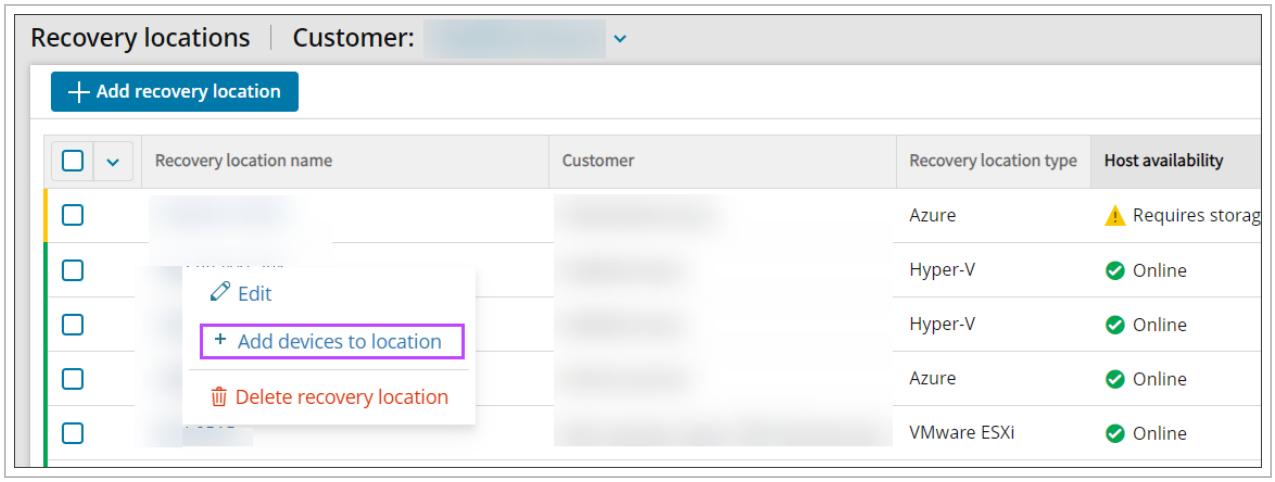
1. Select the checkbox for the Recovery Location to add the device to
2. At the top of the Recovery Locations page, select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
    a. Top bar menu
    b. Top bar menu

Location context menu

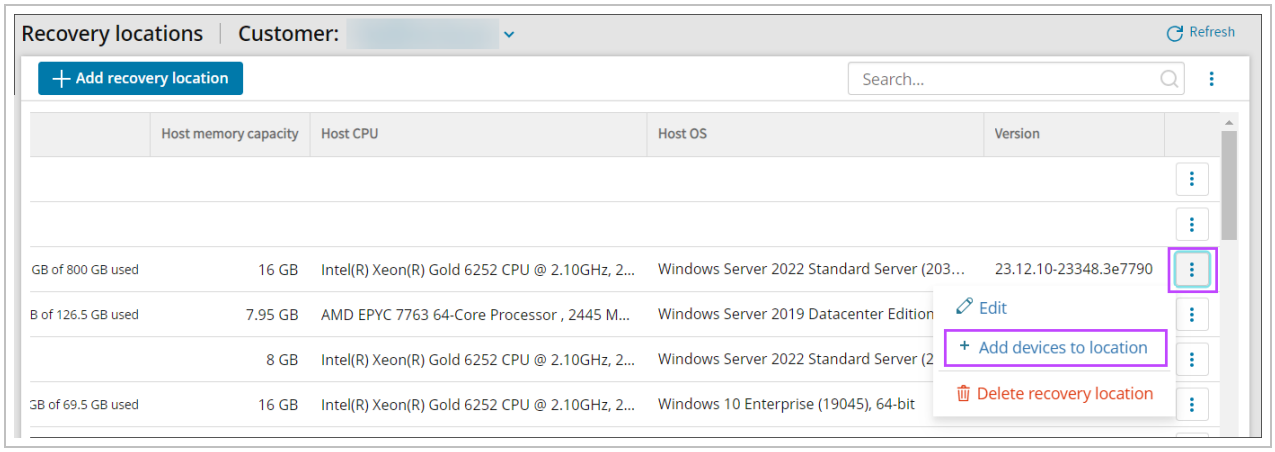
1. Right-click on the Recovery Location to add the device to
2. Select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
    a. Enable Standby Image to AzureDevices cannot be added to a Standby Image plan if already assigned to a Recovery Testing plan.Devices can be assigned to multiple Standby Image plans at once, i.e. Standby Image to Hyper-V and Standby Image to Azure. From Main DashboardTo enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:Log in to the Management Console under a SuperUser or Manager account In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan toClick Add to recovery plan from the Toolbar Select Standby Image (Azure)Select the customer the device(s) you wish to apply the Standby Image plan belong toChoose the recovery location as was configured in Add Recovery LocationsIf the selected customer does not have any locations, you must add one before continuing by selecting Add recovery location. See Add Recovery Locations for full details of adding a location.It is not possible to assign a location for which the Host availability is "Offline"Click NextConfirm the device selected from the Dashboard is compatible and click Next Enter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereClick Next to continueChoose the boot check frequency:OffEvery recovery sessionDailyWeeklyBiweeklyMonthlyIf you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Once connected, click NextClick Azure VM settings towards the right-hand side of the screen to open the settings configuration window:Configure the Azure VM Settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk typeData disk(s) typeVirtual NetworkSubnetAssign NSG and public IPDuring the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend blocking internet access for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.Click Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowConfirm assigning the plan to the device(s)Wait for the plan to be assigned until you see a confirmation banner on the pageClick FinishFrom Standby Image OverviewLog in to the Management Console under a SuperUser or Manager accountNavigate to Continuity > Standby ImageClick Add to PlanSelect Standby Image (Azure)You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the planRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding:
    b. Top bar menu
    c. Top bar menu

Right-hand menu

1. Click the action menu button for the Recovery Location, seen as three dots in a vertical line to the right of the location's version
2. Select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
    a. Enable Standby Image to AzureDevices cannot be added to a Standby Image plan if already assigned to a Recovery Testing plan.Devices can be assigned to multiple Standby Image plans at once, i.e. Standby Image to Hyper-V and Standby Image to Azure. From Main DashboardTo enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:Log in to the Management Console under a SuperUser or Manager account In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan toClick Add to recovery plan from the Toolbar Select Standby Image (Azure)Select the customer the device(s) you wish to apply the Standby Image plan belong toChoose the recovery location as was configured in Add Recovery LocationsIf the selected customer does not have any locations, you must add one before continuing by selecting Add recovery location. See Add Recovery Locations for full details of adding a location.It is not possible to assign a location for which the Host availability is "Offline"Click NextConfirm the device selected from the Dashboard is compatible and click Next Enter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereClick Next to continueChoose the boot check frequency:OffEvery recovery sessionDailyWeeklyBiweeklyMonthlyIf you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Once connected, click NextClick Azure VM settings towards the right-hand side of the screen to open the settings configuration window:Configure the Azure VM Settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk typeData disk(s) typeVirtual NetworkSubnetAssign NSG and public IPDuring the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend blocking internet access for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.Click Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowConfirm assigning the plan to the device(s)Wait for the plan to be assigned until you see a confirmation banner on the pageClick FinishFrom Standby Image OverviewLog in to the Management Console under a SuperUser or Manager accountNavigate to Continuity > Standby ImageClick Add to PlanSelect Standby Image (Azure)You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the planRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding:
    b. Top bar menu
    c. Top bar menu

Configure N-able Recovery Service on Azure Recovery Locations

Installing the Recovery Locations recovery service on Azure requires additional configuration during setup of the Azure VM:

- Check the Requirements
- Configuration
  - Step 1: Download the Recovery Service
  - Step 2: Create Recovery Location VM
  - Step 3: Assign Permissions to the Recovery Location VM
  - Step 4: Install the Recovery Service on the Recovery Location VM
  - Step 5: Add Antivirus Exclusions
  - Step 6: Configure Recovery Location in Management Console
- Check recovery location

Azure Requirements

To install the Recovery Location's recovery service on an Azure VM, the following requirements are necessary:

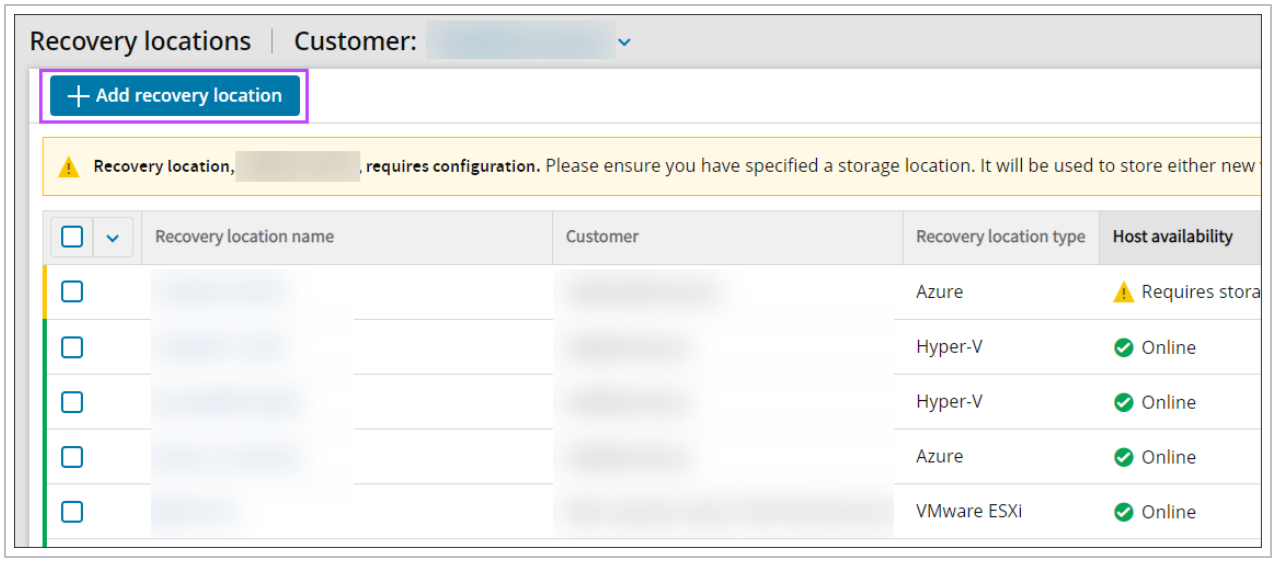
- A user created for you in your Azure tenant. The user must:
  - Have access to a subscription
  - Have access to a resource group you want to use to keep the Recovery Location VM and restored (target) Azure VMs
  - Be able to assign permissions on virtual machines within the resource group

Configuration

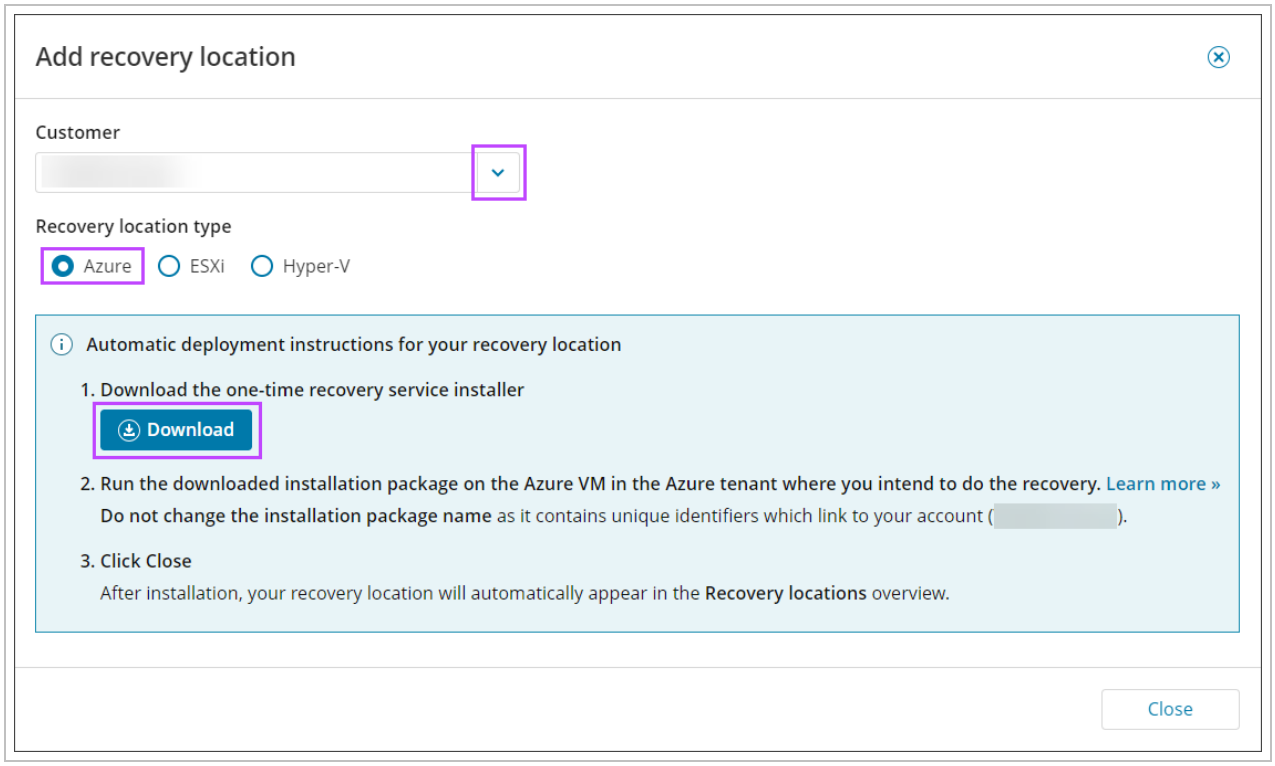
> It is important to follow the installation steps in the order below. If you grant the Recovery Location VM access to a resource group after installing the Recovery Service, you must then reboot the Recovery Location VM for these changes to take effect.

Step 1: Download the Recovery Service

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Click **Add recovery location** at the top of the page



4. In the **Add Recovery Location wizard**, select the customer to attribute the recovery location to, from the dropdown



5. Select **Azure** as the Recovery Location Type
6. Download the recovery service installer and save it to an easily found place on your device

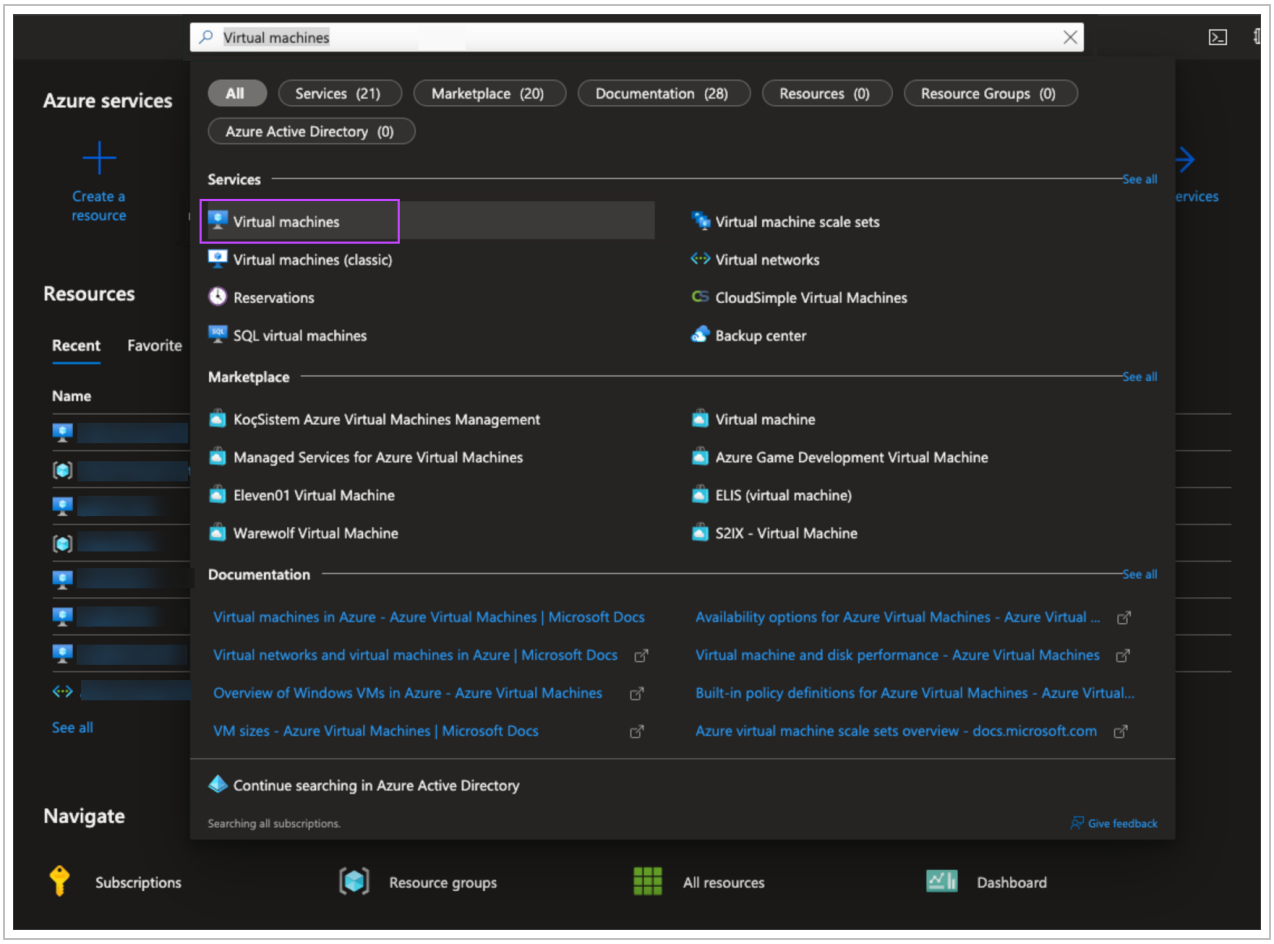
Do **not** change the installation package name. The installation package name contains unique identifiers to your account.

This is a one-time installer and can only be used to install a single instance of the recover service. The installer will fail if you attempt to use the same package for another installation.

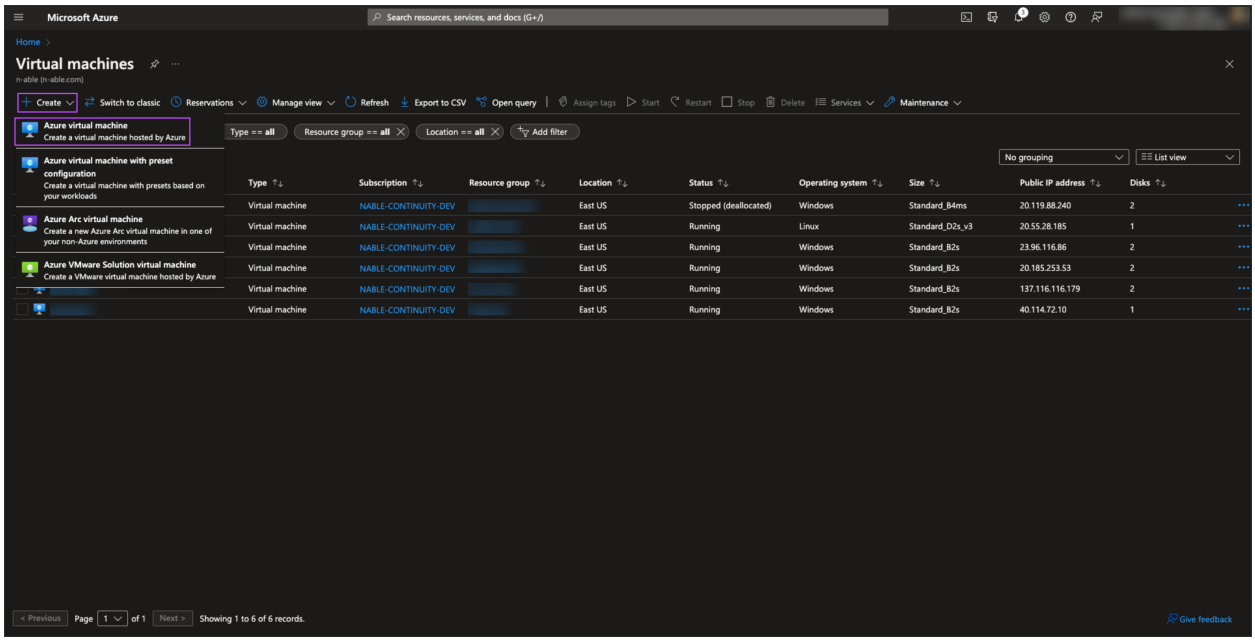
Do **not** run the installer at this point, there are additional changes that are required first.

Step 2: Create Recovery Location VM

1. Login to the Azure portal
2. Using the search bar within the Azure Portal, type **Virtual Machines**, then select the **Virtual Machines service** from the results



3. On the Virtual Machines page, select **+ Create** and select **Azure Virtual Machine** from the dropdown provided



4. On the Basics tab:

Microsoft Azure

Home > Virtual machines >

Create a virtual machine

Basics | Disks | Networking | Management | Monitoring | Advanced | Tags | Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * azure-on-demand

Create new

Instance details

Virtual machine name * -machine

Region * (US) East US

Availability options Availability zone

Availability zone * Zones 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more

Security type Standard

Image * Windows Server 2019 Datacenter - Gen2

See all images | Configure VM generation

VM architecture

- Arm64
- x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount

Size * Standard_D2s_v3 - 2 vcpus, 8 GiB memory (US$137.24/month)

See all sizes

Administrator account

Username *

The value must not be empty.

The value must be between 1 and 20 characters long.

Password *

The value must not be empty.

The value must be between 12 and 123 characters long.

Confirm password *

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular

a. Select a **Subscription** from the dropdown

> The subscription selected here will be used to keep future restored devices. When a subscription is selected for the Recovery Location, this subscription will be used to keep the devices being restored to Azure. A different subscription **cannot** be selected in the One-Time Restore wizard at Azure VM settings step.

b. Select the **Resource Group** you want to use to keep the Recovery Location VM

c. Provide a valid **Virtual Machine Name** for your Recovery Location VM

d. Select the geographic region

> Select the closest geographic region from geographic standpoint to the node where you store backups of the devices you are going to restore to Azure

e. In the **Image** field, select one of:
   a. **Windows Server 2019 Datacenter - Gen2(9)**
   b. **Windows (Windows 10 Pro), version 21H2 Gen 2**

f. Under the **Size** field, click **See all sizes** and search for **b4ms**

> This VM size is the lowest priced size that meets our hardware recommendations for Local VHD restores

g. Set a **Username** and **Password** for the Administrator account

h. For the **Select Inbound Ports** field choose one of:
   a. **RDP connections**
   b. **Bastion**

5. Click **Next : Disks**
6. On the **Disks** tab, select the **OS disk Type** of **Standard HDD**
7. Click **Next: Networking**
8. On the **Networking** tab specify the **vnet** and **subnet**

> The **Recovery Location VM** should be added to the **Network Security Group**, which allows outbound communication.

9. Click **Review + Create**

10. After a few seconds, the request will be validated. Review the settings and click **Create**

Microsoft Azure

Home > azure-on-demand > Marketplace > Virtual machine >

Create a virtual machine ...

Validation passed

Basics | Disks | Networking | Management | Monitoring | Advanced | Tags | **Review + create**

Cost given below is an estimate and not the final price. Please use Pricing calculator for all your pricing needs.

PRODUCT DETAILS

1 X Standard B4ms
by Microsoft
Terms of use | Privacy policy

Subscription credits apply

0.1820 USD/hr
Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

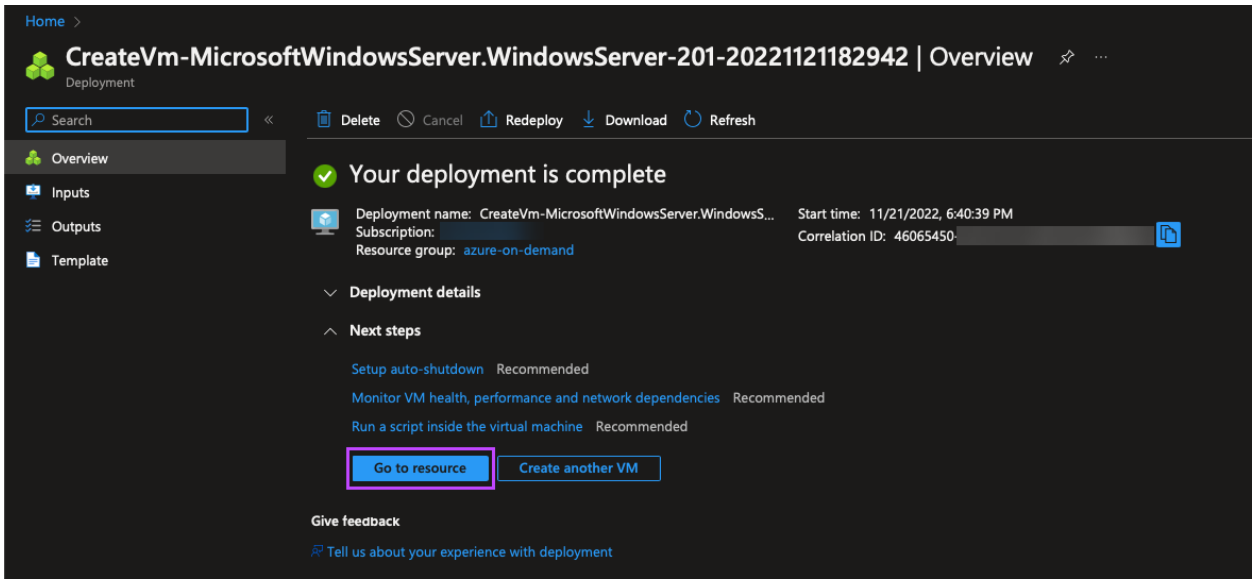
Basics

Subscription	[redacted]
Resource group	azure-on-demand
Virtual machine name	[redacted]-machine
Region	East US
Availability options	Availability zone
Availability zone	1
Security type	Standard
Image	Windows Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard B4ms (4 vcpus, 16 GiB memory)
Username	[redacted]
Already have a Windows license?	No
Azure Spot	No

Disks

OS disk type	Standard HDD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

11. A page will display with the progress of the deployment. Once deployment is complete, you are able to go to the resource by clicking **Go to resource**

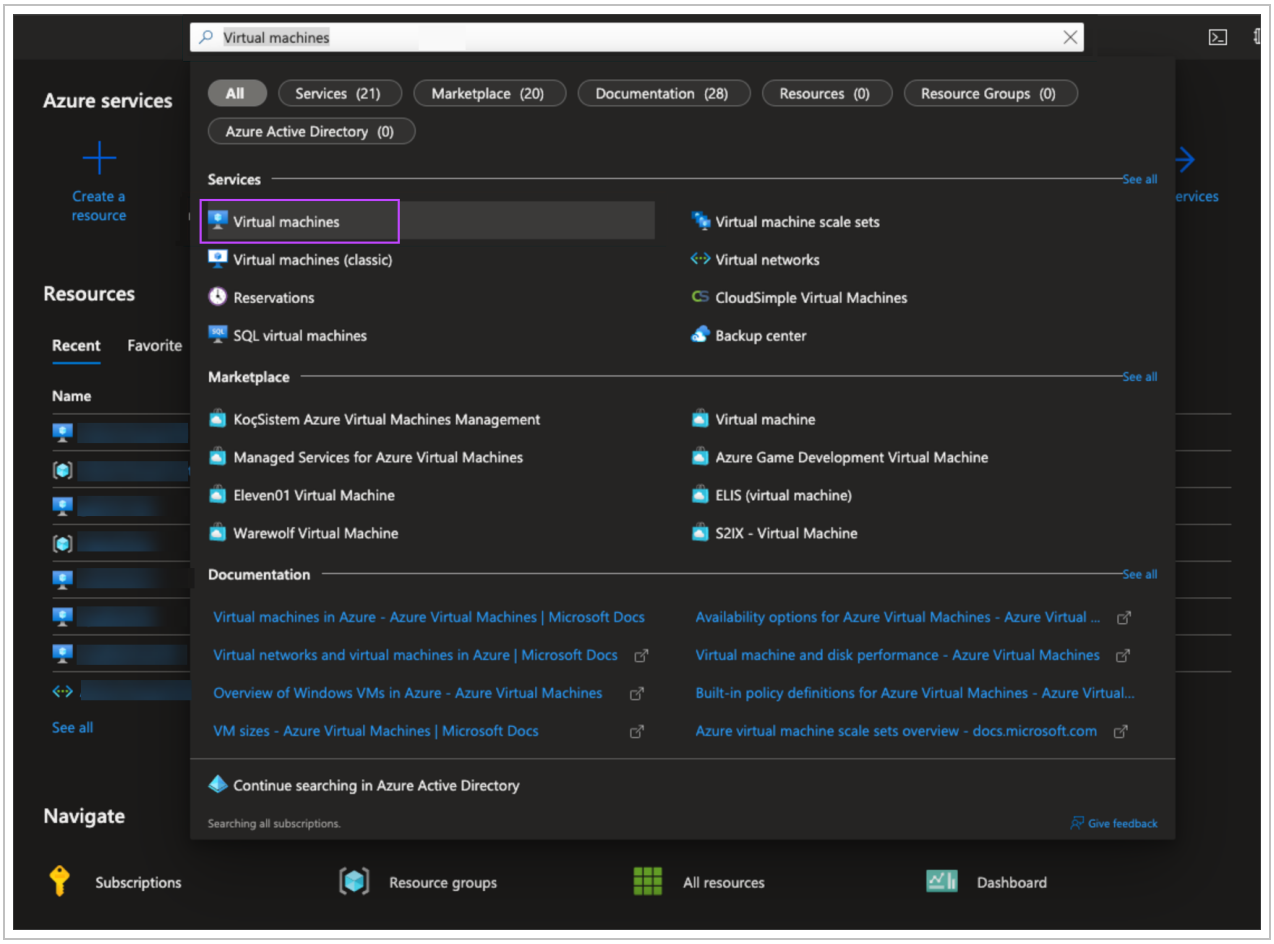


Step 3: Assign Permissions to the Recovery Location VM

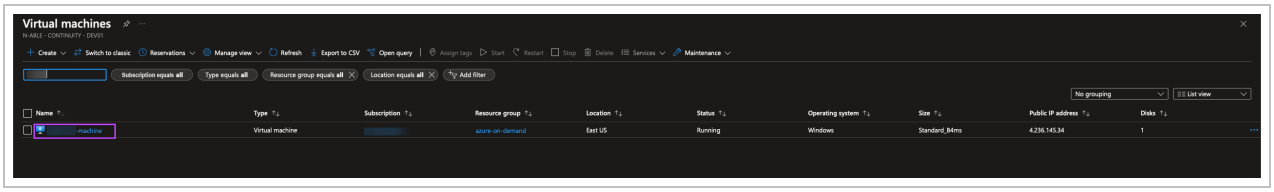
In order for restores to successfully create Virtual Machine's in Azure, Owner permissions must be given to the Recovery Location VM.

> Without these permissions, the restores will start, but will fail when the recovery service attempts to manipulate Azure resources.

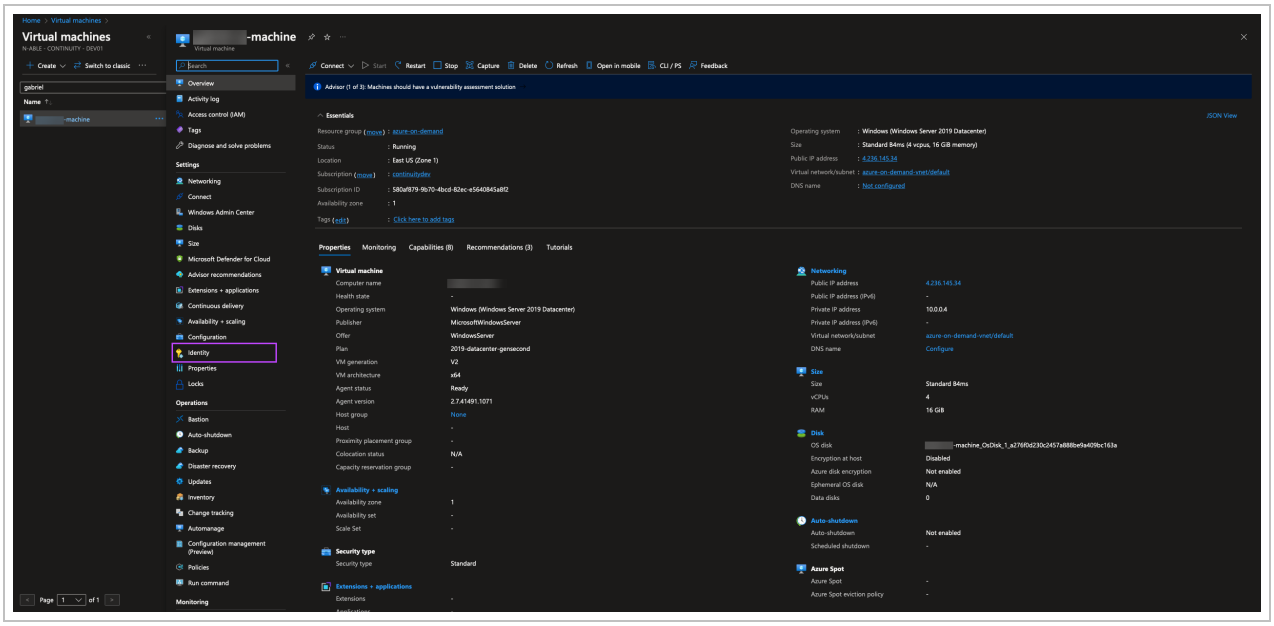
1. Login to the Azure portal
2. Using the search bar within the Azure Portal, type **Virtual Machines**, then select the **Virtual Machines service** from the results



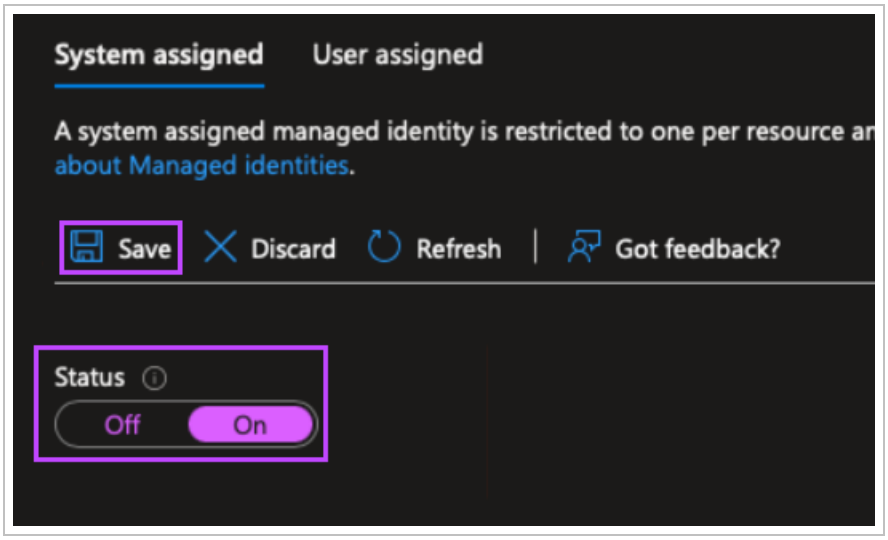
3. On the Virtual Machines page, find the virtual machine created in Step 2 where you will install the Recovery Agent in Step 4 and click the VM name



4. In the Virtual Machine, click the dropdown by the search bar and click **Identity**

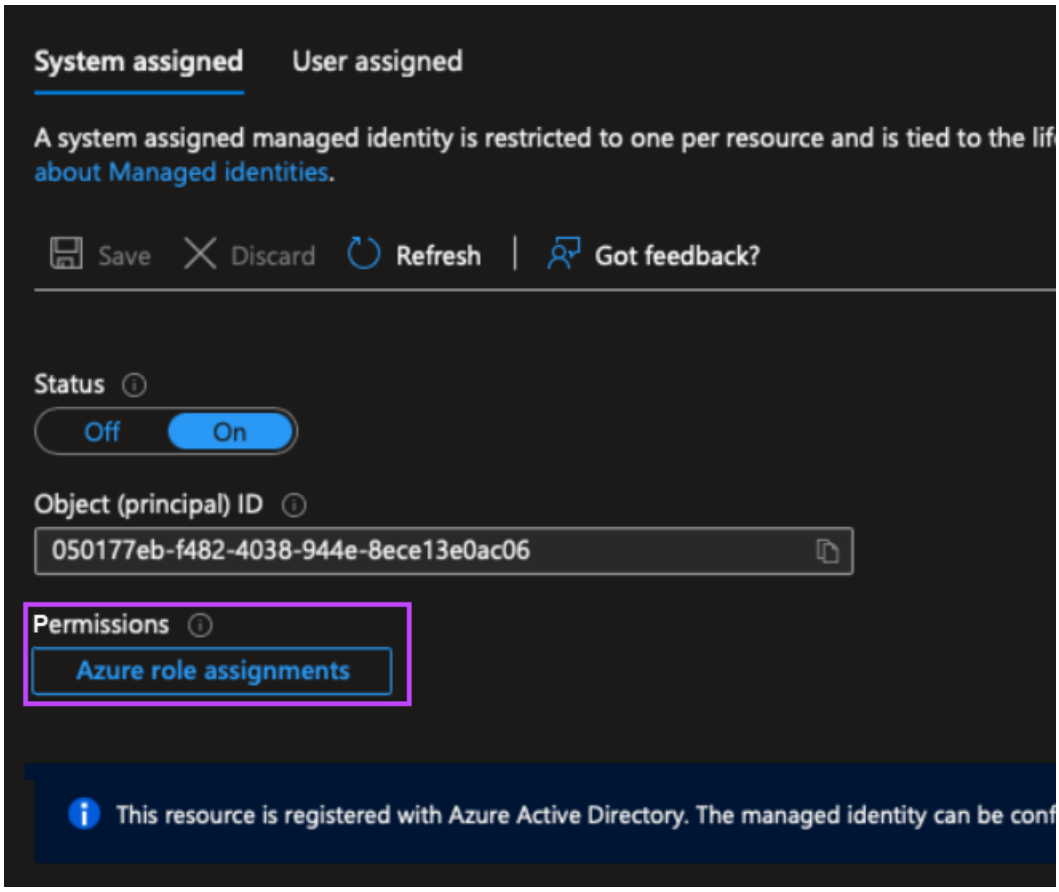


5. In the System Assigned tab, set the **Status** to **ON**



6. Click **Save**

7. Select **Azure role assignments**



8. Click **Add role assignment (Preview)** at the top of the page
9. In the Add role assignment (Preview) window, set the following:
   a. **Scope**: Resource Group
   b. **Subscription**: Select the subscription selected for the Recovery Location VM in Step 2: 4
   c. **Resource Group**: Select the resource group selected for the Recovery Location VM in Step 2: 4
   d. **Role**: Owner

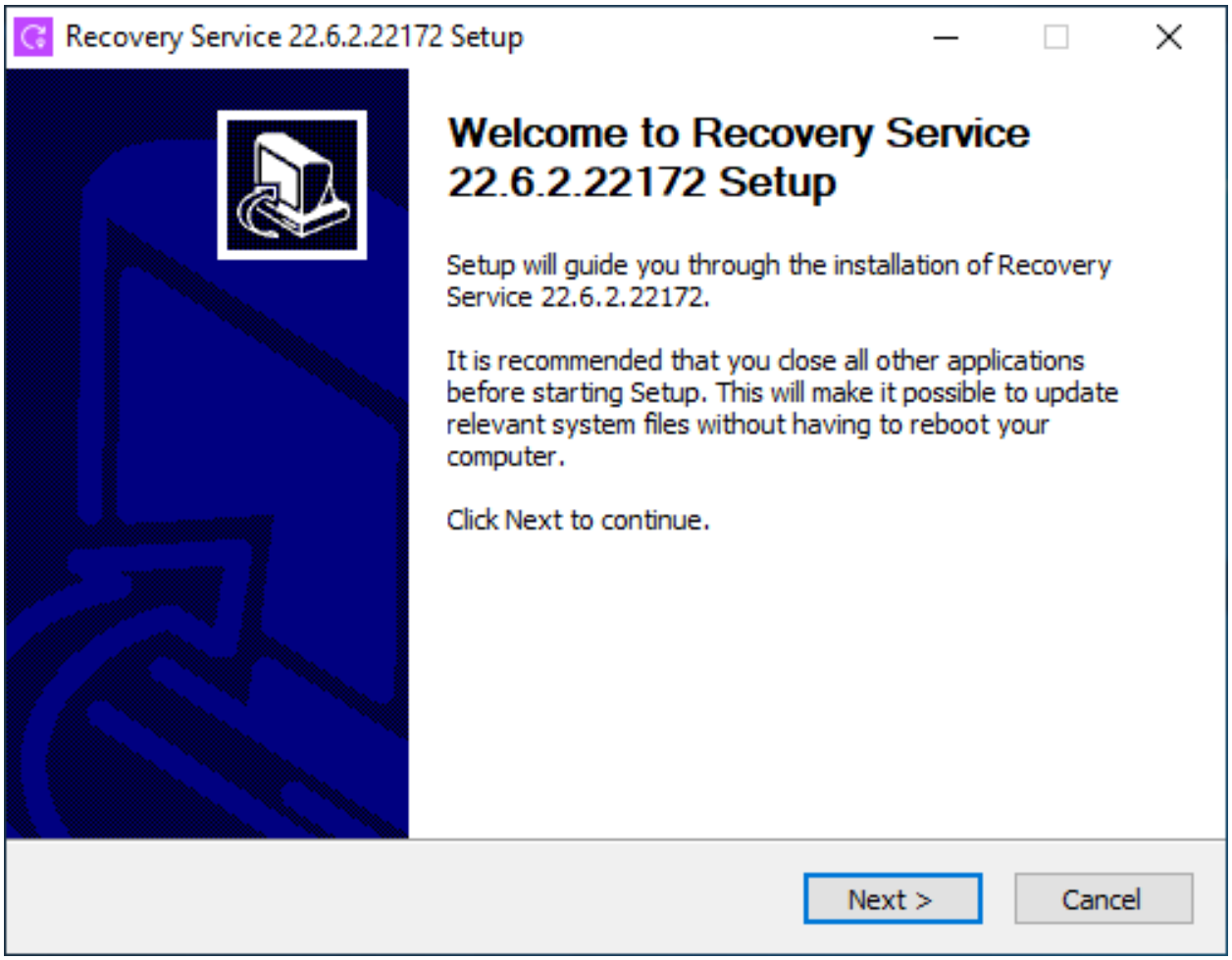
   > If you see a warning message that states "You don't have permissions to add role assignments…", please make sure you have the proper access right to assign roles to the VM.

10. Click **Save**
11. Once complete you will see the role assigned in the **Azure Role Assignments** table
12. To restore to resource groups other than the Recovery Location resource group, or to use virtual networks from other resource groups to place target VMs, you must add role assignments for those groups as well. To do this, repeat step 9 and step 10 for each group

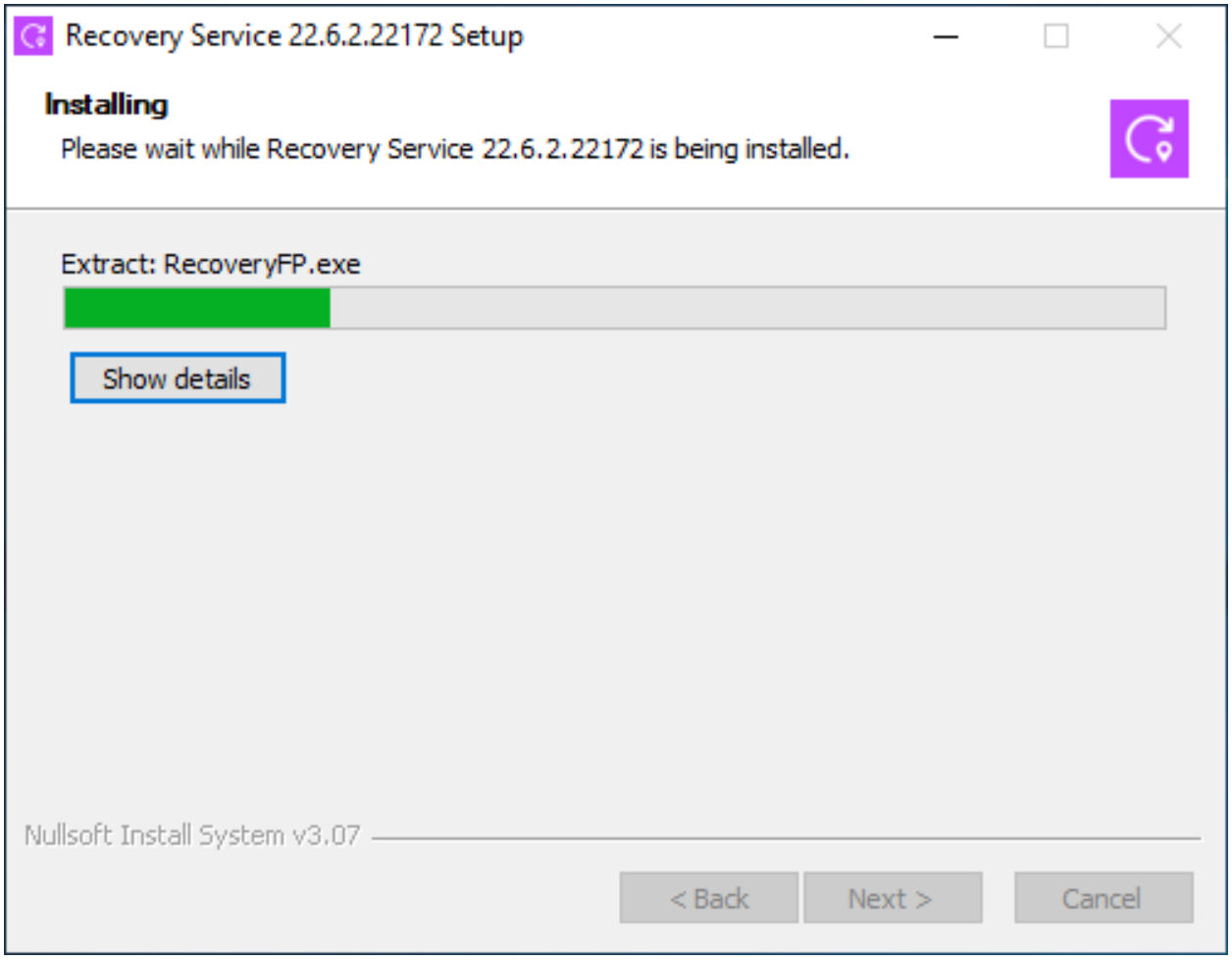
    > If you try to restore to a resource group without the role assignment the restore will fail

Step 4: Install the Recovery Service on the Recovery Location VM

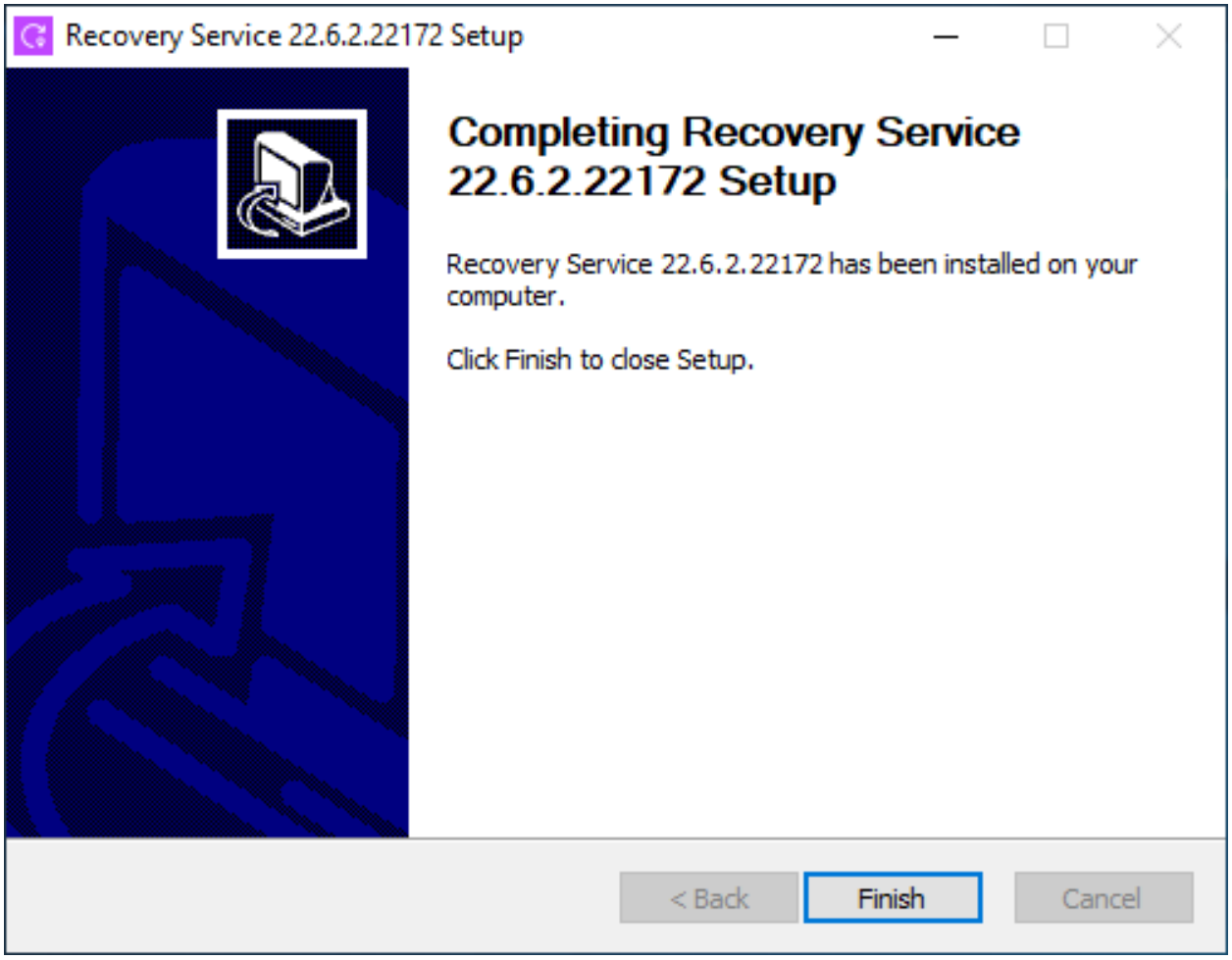
1. Connect to the Recovery Location VM created in Step 2 via RDP or Bastion
2. Copy the Recovery Service downloaded in Step 1:6 from it's location onto the VM
3. Double-click the executable on the Recovery Location VM to run
4. Click **Next** to begin setup



5. Wait for installation to complete



6. Finish the installation and close the wizard



7. After a few minutes, the Recovery Location will appear on the Management Console's Recovery Locations dashboard and can be used to in the One-Time Restore to restore data to Azure

Step 5: Add Antivirus Exclusions

To help speed up Azure restores by up to three times (3x), add the following processes and folders to your Antivirus Exclusions:

Processes

- **AuthTool.exe** - [file location] SYSTEM_DRIVE:\Program Files\Recovery Service*\AuthTool.exe
- **unified_entry.exe** - [file location]. SYSTEM_DRIVE:\Program Files\Recovery Service*\unified_entry.exe
- **RecoveryFP.exe** - [file location] SYSTEM_DRIVE:\Program Files\Recovery Service*\BM\RecoveryFP.exe
- **VdrAgent.exe** - [file] SYSTEM_DRIVE:\Program Files\Recovery Service*\BM\VdrAgent.exe
- **ProcessController.exe** - [file location] SYSTEM_DRIVE:\Program Files\Recovery Service*\BM\ProcessController.exe
- **RecoveryProcessController.exe** - [file location] C:\Program Files\Recovery Service*\BM\RecoveryProcessController.exe

- **ClientTool.exe** - [file location] SYSTEM_DRIVE:\Program Files\Recovery Service*\BM\ClientTool.exe
- **VdrTool.exe** - [file location] SYSTEM_DRIVE:\Program Files\Recovery Service*\VdrTool.exe

Folders

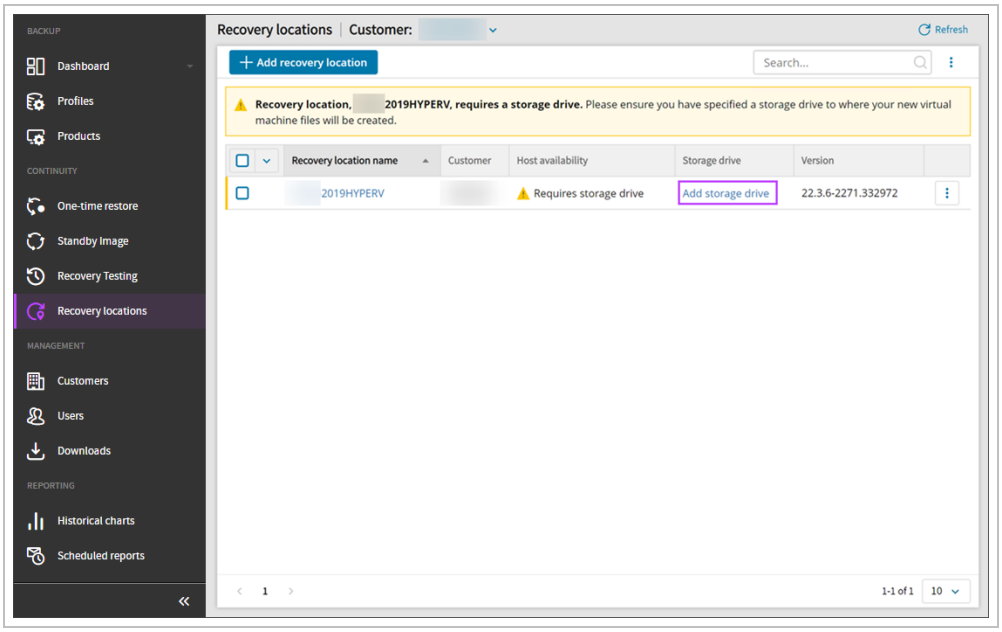
- **StandbyImage** - STORAGE_LOCATION_PATH\StandbyImage
- **OnDemandRestore** - STORAGE_LOCATION_PATH\OnDemandRestore

Step 6: Configure Recovery Location in Management Console

1. Login to the Management Console under a SuperUser account
2. Navigate to **Continuity** > **Recovery Locations**

   > The new recovery location will now be displayed in the list of locations under the customer selected in Step 1: 4

3. Enter the storage drive to assign where the target VM(s) metadata, needed for recovery, will be stored by clicking **Add storage drive** and entering the drive location. E.g. `C:\`



Check recovery location

When the Recovery Location set up is completed you will be able to find it in the drop-down at the first step of One-Time Restore wizard (or on the Recovery Locations Dashboard) and proceed with the restore: Configure One-Time Restore to AzureBefore starting a One-Time Restore to Azure, ensure you have checked all requirements and limitations, including setting up an Azure recovery location.From Backup DashboardLog in to the Management Console under a SuperUser accountIn the Backup Dashboard, tick the checkbox to the left of the device(s) to restoreClick One-Time Restore Select the Azure targetSelect the CustomerSelect the Azure Recovery Location for the restore or click + Add recovery Location to follow the steps to create a new Azure Recovery LocationIf adding a recovery location from here, you will be taken to the Add Azure Recovery Location wizard, where Azure will be automatically selected as the recovery type. Follow the Azure Recovery Location installation instructions from Step #4 onwards.Click NextConfirm compatibility of device(s) and click NextEnter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key -

Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereIf you are logged in as a security officer, this will be detected automatically.Click NextSelect the date and time of the backup session to restoreDuring this step, all available sessions for all devices listed will be loaded in the backup session column. Please allow time for these to load, if the load of sessions fails, a message stating so will be displayed with a refresh button to try again.If you wish to protect the device according to its existing backup schedule, enable Backup target VMIf the Backup Target VM option is enabled for one or more devices, be aware that if the backup agent is still running in backup mode on the source VM, this will lead to corrupted backup data for both the source and target VMs.If you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Supply the Azure VM settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk type Set to Premium SSD to speed up the Azure restore. This can be changed in Azure laterData disk(s) typeSet to Premium SSD to speed up the Azure restore. This can be changed in Azure laterVirtual NetworkSubnetStop target VM after recoveryAssign NSG and public IPClick NextClick Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowReview and confirm the restore details for each device and click ConfirmOnce the restore has been started, a green banner will be displayed and a notification in the top right-hand corner of the screen to confirm. Click Finish to close the restore wizard and return to the DashboardFrom One-Time Restore OverviewLog in to the Management Console under a SuperUser accountNavigate to the One-Time Restore overview by selecting Continuity > One-time Restore from the vertical menu on the left hand sideClick One-time restore from the top barThe wizard will open to target selection window, follow the above steps from Step #4 onwardsRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding:.

Configure N-able Recovery Service on ESXi Host Server

Installing the Recovery Locations recovery service on an ESXi Host Server requires additional configuration during the setup of the environment:

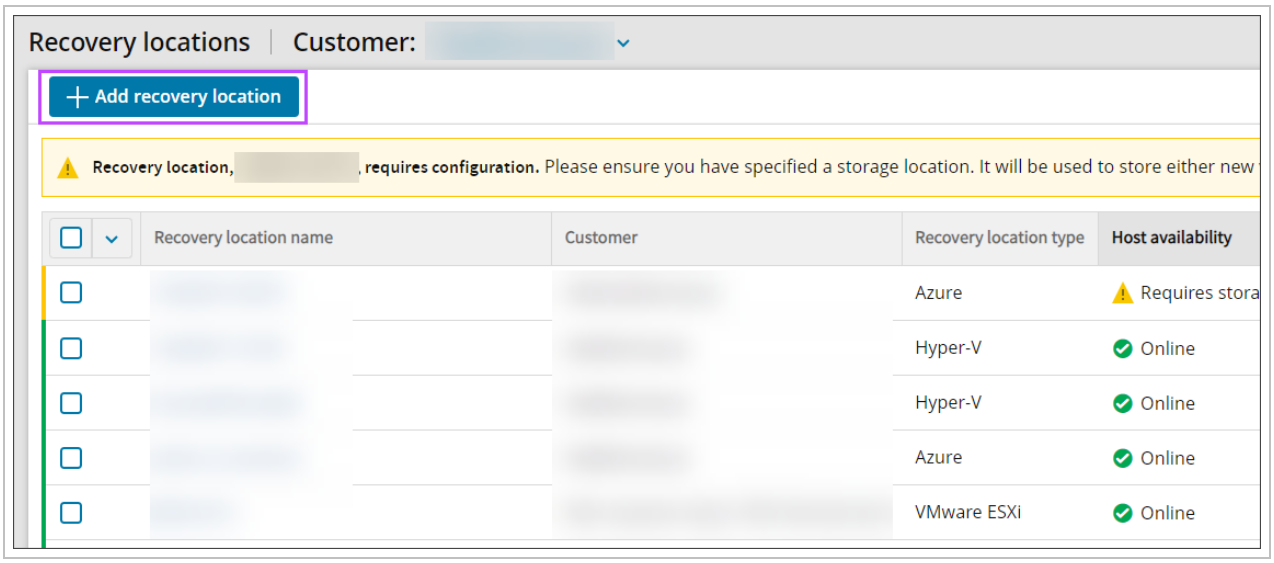
- Check the Requirements
- Configuration
  - Step 1: Download the Recovery Service
  - Step 2: Create vSphere Client User
  - Step 3: Create Recovery Location Virtual Machine
  - Step 4: Install Recovery Service On VM
  - Step 5: Add Storage Location and Server Connections
  - Step 6: Add device to Standby Image plan

Configuration

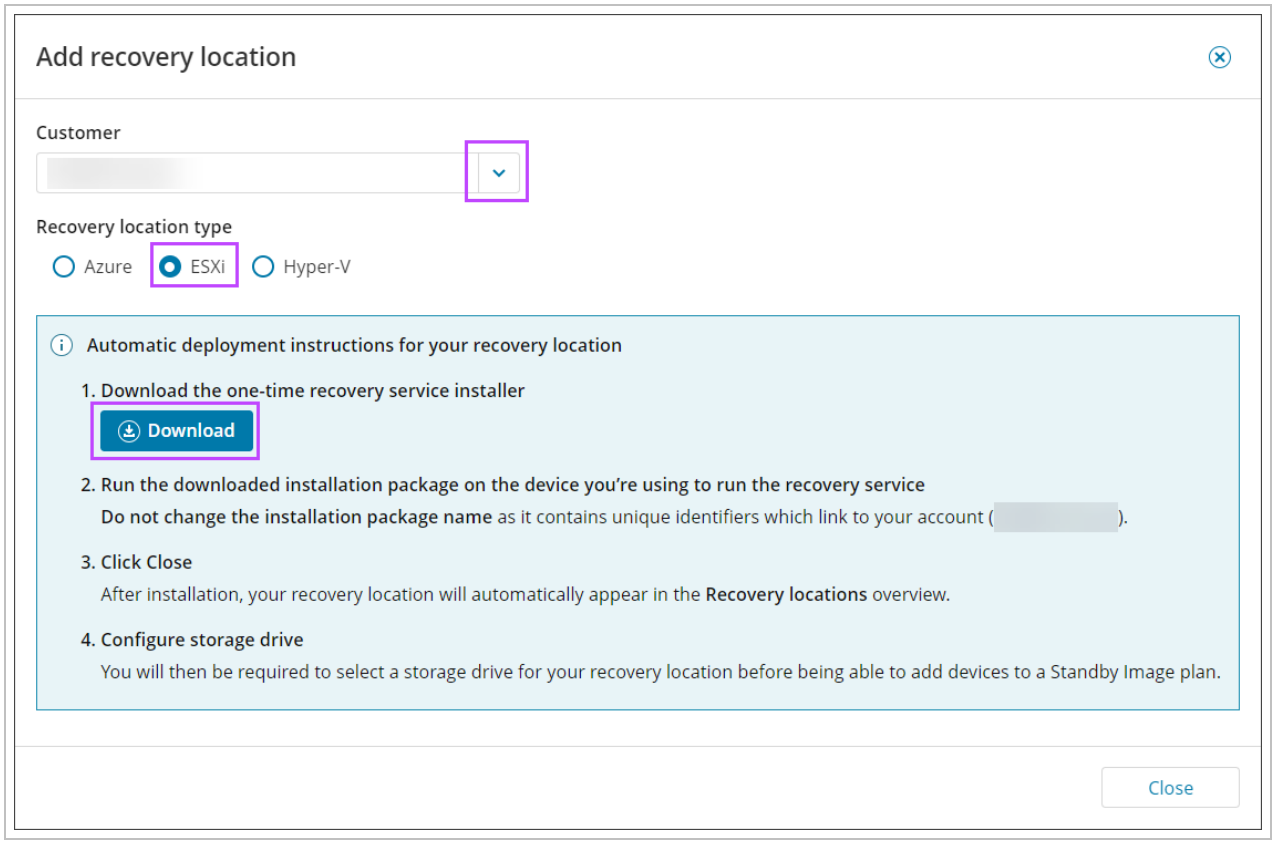
> It is important to follow the installation steps in the order below.

Step 1: Download the Recovery Service

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Click **Add recovery location** at the top of the page



4. In the **Add Recovery Location wizard**, select the customer to attribute the recovery location to from the dropdown



5. Select **ESXi** as the recovery location type
6. Download the recovery service installer

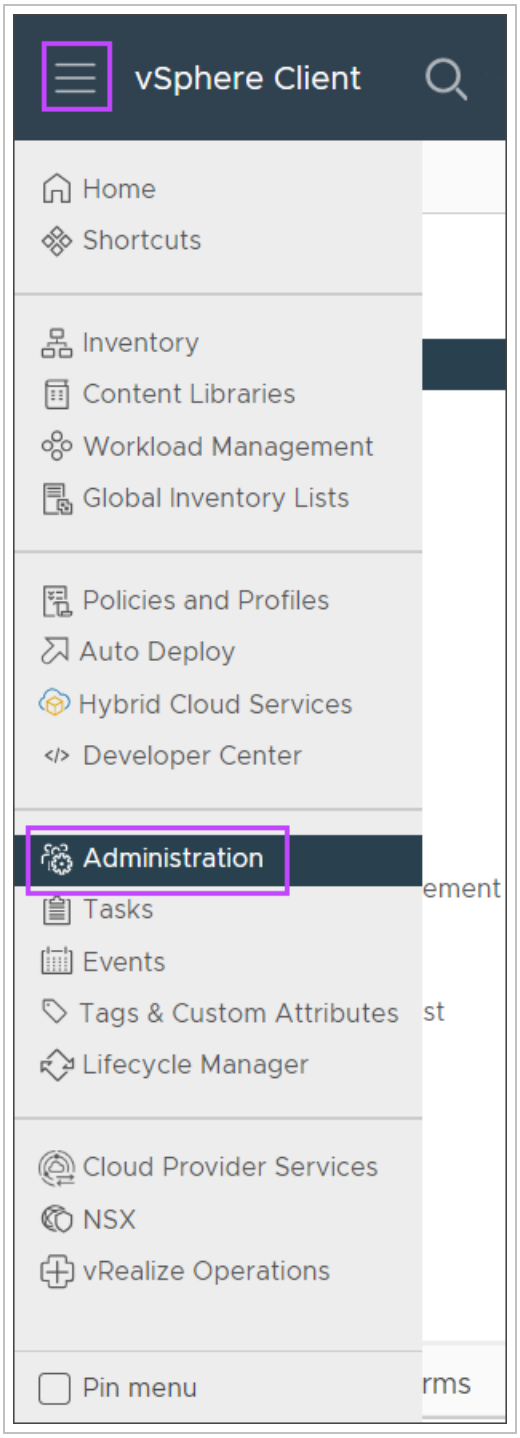
> Do **not** change the installation package name. The installation package name contains unique identifiers to your account.
>
> This is a one-time installer and can only be used to install a single instance of the recovery service. The installer will fail if you attempt to use the same package for another installation.

Do **not** run the installer at this point, there are additional changes that are required first.

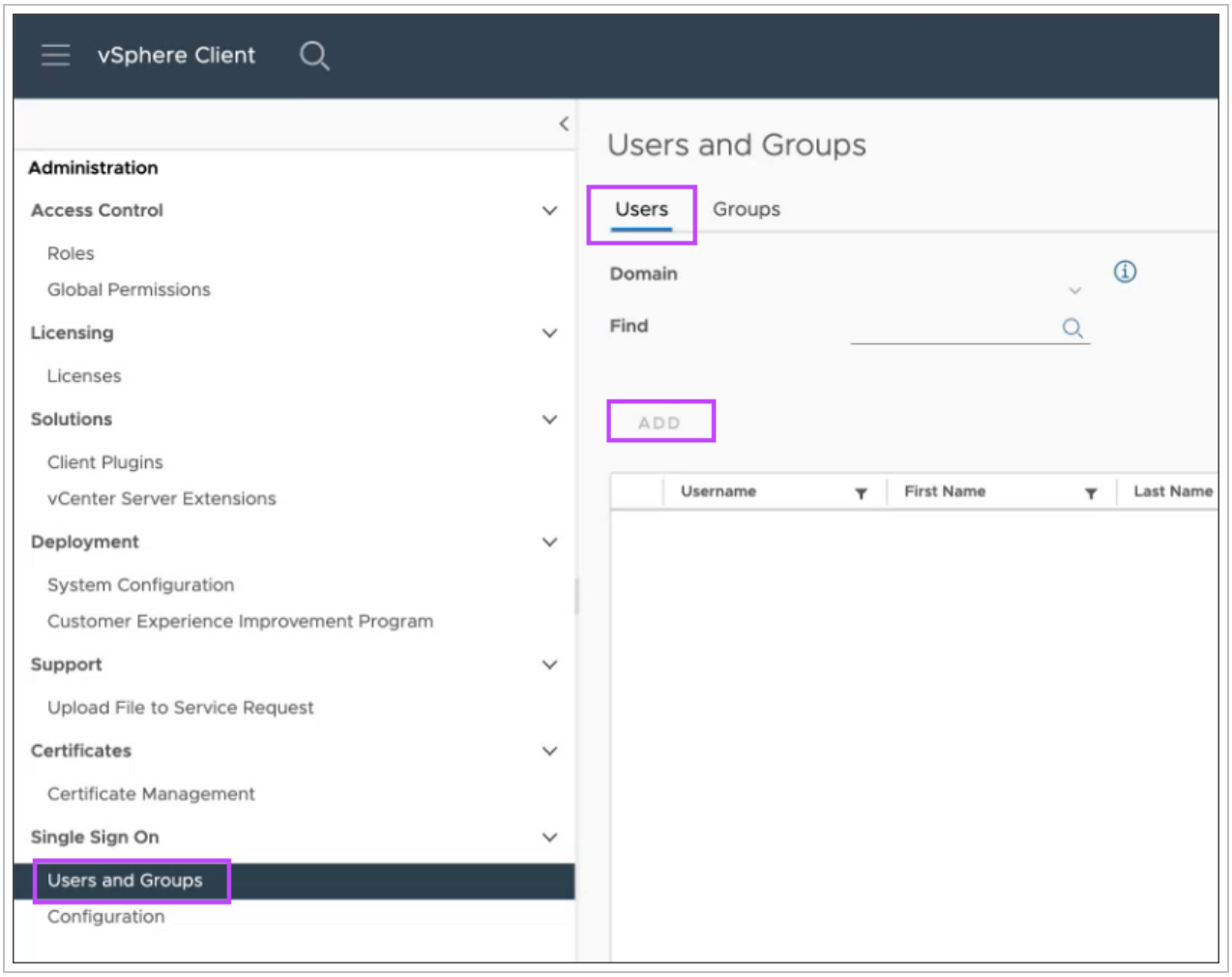
If you want to restore to Local VMDK format go now to Step 4. As you will not restore to an ESXi server, is not obligatory to configure vSphere Client user and Virtual Machine in vCenter.

Step 2: Create vSphere Client User

1. Login to the **vCenter Server** by using the **vSphere Client**
2. Open the menu and navigate to **Administration**



3. In the **Users and Groups** page, select the **Users** tab and click **Add**



4. Fill in the user details and **Save** the new user
5. Once the new user has confirmed access, assign the **Administrator** role to the user

> The user **must** be assigned the Administrator role for Standby Image to ESXi to function appropriately. Do **not** use a custom role with lesser privileges.

There are two options for where to install the Recovery Service:

1. Create a recovery location Virtual Machine within the ESXi server/host (recommended)

> This option is recommended as performance is increased as data doesn't have to transfer over the network during the restore

> To use this option, follow the instructions in Step 3: Create Recovery Location Virtual Machine

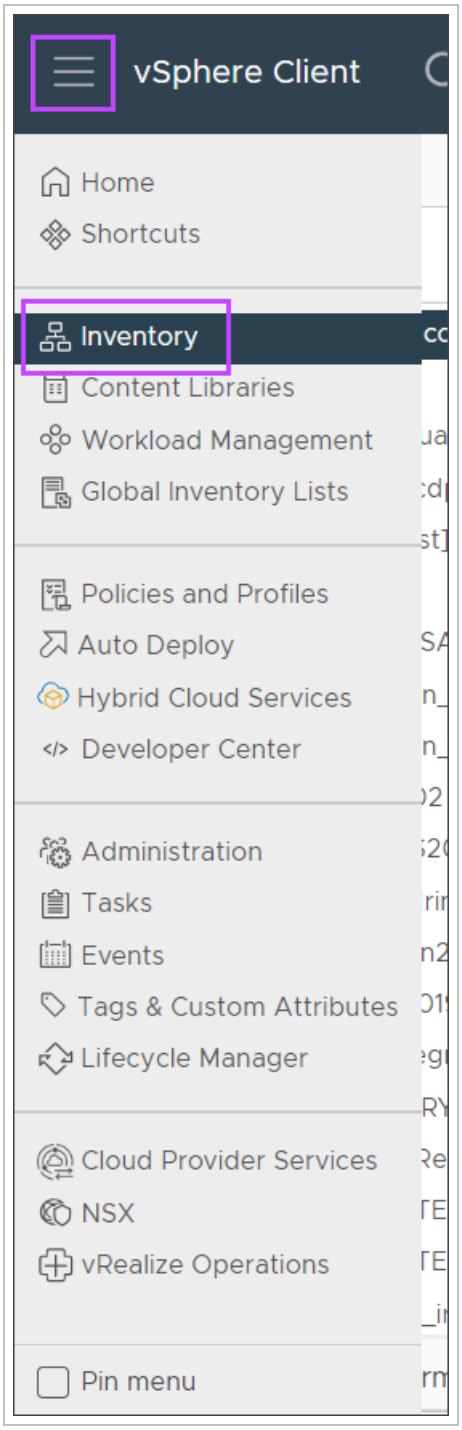
2. If you have multiple vCenter servers and want to restore to multiple ESXi servers/hosts directly (not to vSphere) it is recommended to create a recovery location on a dedicated server/host

   This option doesn't require the server to be stored anywhere but it **must** have access to vSphere

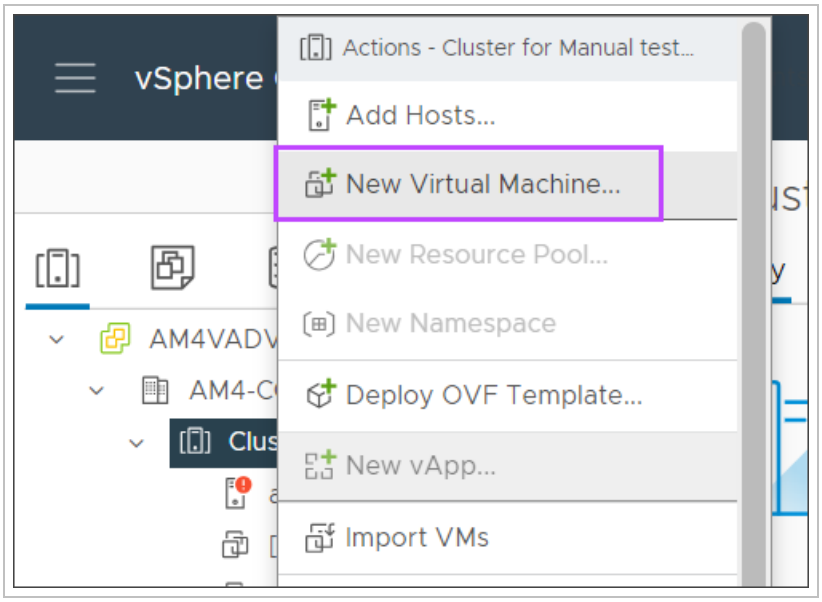
   To use this option, skip straight to Step 4: Install Recovery Service On VM

Step 3: Create Recovery Location Virtual Machine

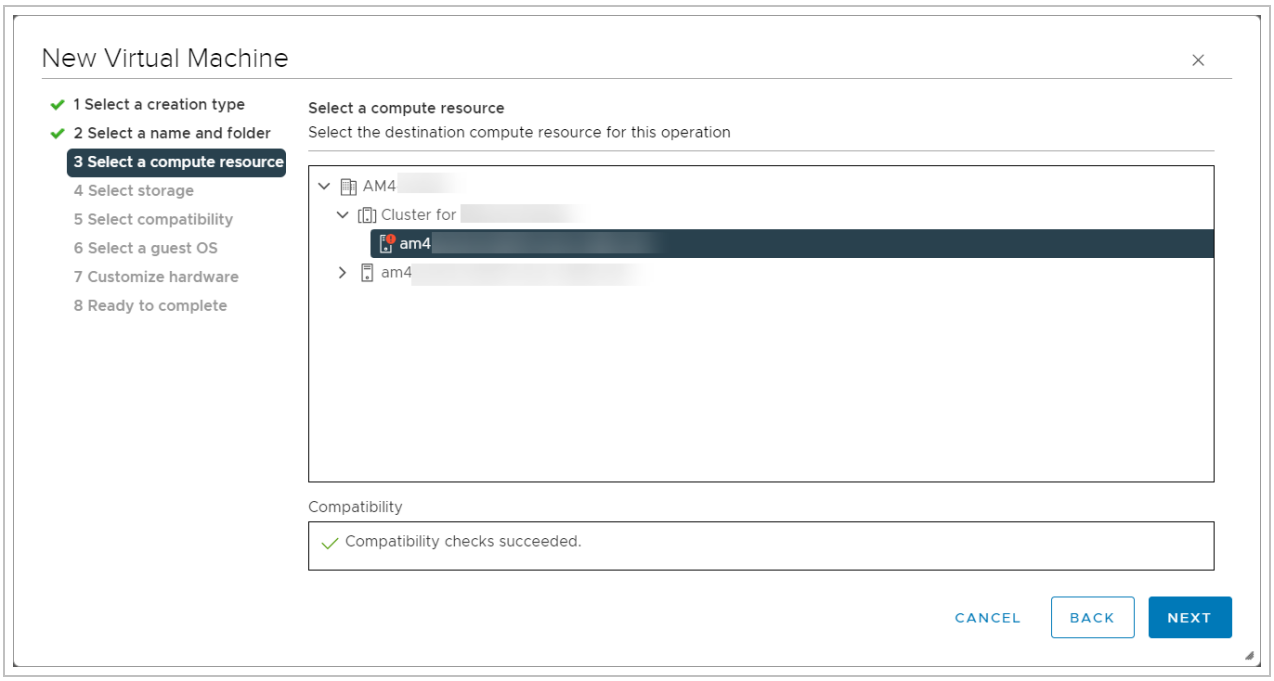
1. In the **vCenter Server** now navigate to **Inventory** in the menu



2. Right click the cluster and select **New Virtual Machine**

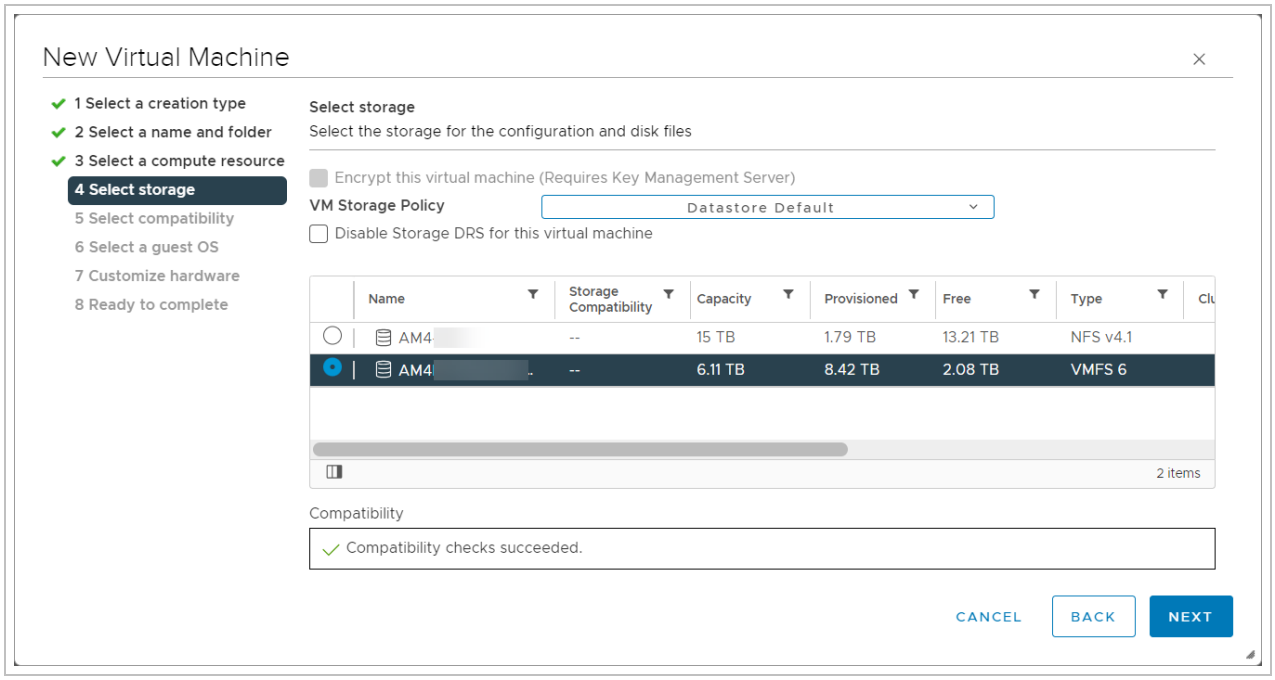


3. In the Creation Type list, select **Create a new virtual machine** then click **Next**
4. Give the Virtual Machine a name and select a location for the virtual machine from the resource tree
5. Click **Next**
6. From the resource tree, select a compatible destination compute resource and click **Next**



7. Select the data store from the available options for the configuration and disk files and click **Next**

> The selected storage **must** have enough capacity to run the restores and store Virtual Machine data



8. Select the ESXi version to ensure the new Virtual Machine is compatible with the host in your environment and click **Next**
9. Configure the guest Operating System from the dropdowns provided and click **Next**

> **Microsoft Windows Server 2019** is recommended

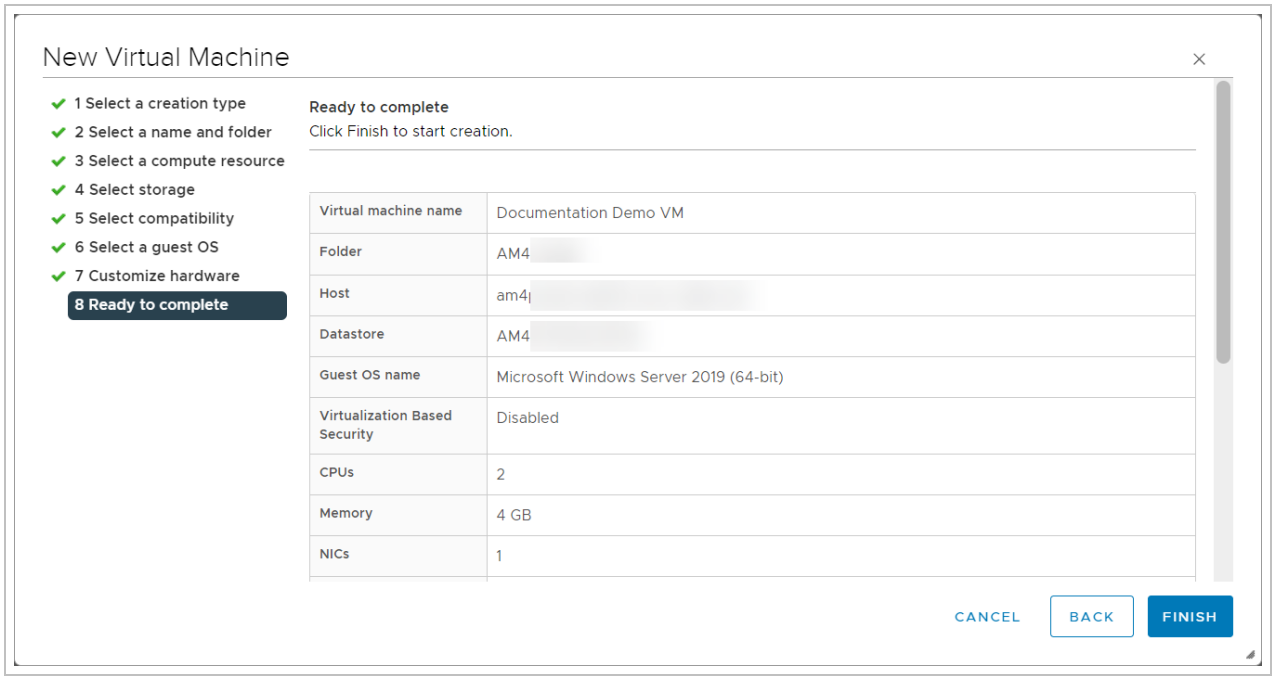
10. Customize the virtual hardware as per our requirements:

> See the Minimum Requirementsfor our default hardware configuration recommendations

> It is possible to run multiple parallel restores so long as the virtual hardware is configured to handle this amount of traffic

11. Click **Next**

12. Confirm the details of the new Virtual Machine and click **Finish** to begin creation of the new Virtual Machine



Step 4: Install Recovery Service On VM

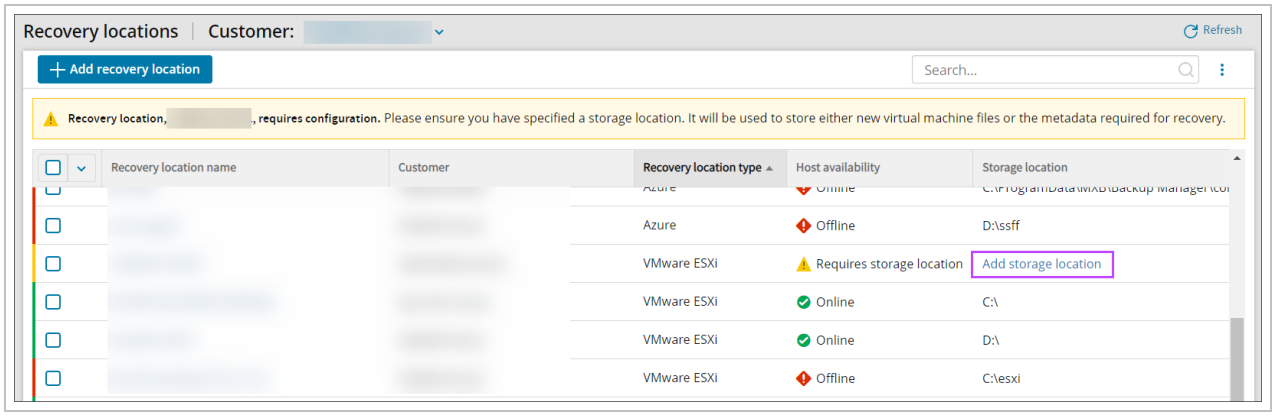
1. Select the newly created Virtual Machine from Step 3 in the **Inventory** list, power it on and click **Launch remote console** or move to the dedicated server/host if restoring to the ESXi server/host directly
2. Transfer the downloaded recovery service file to the machine
3. Run the installation package

> The recovery location will appear in the list on the Management Console after installation is complete

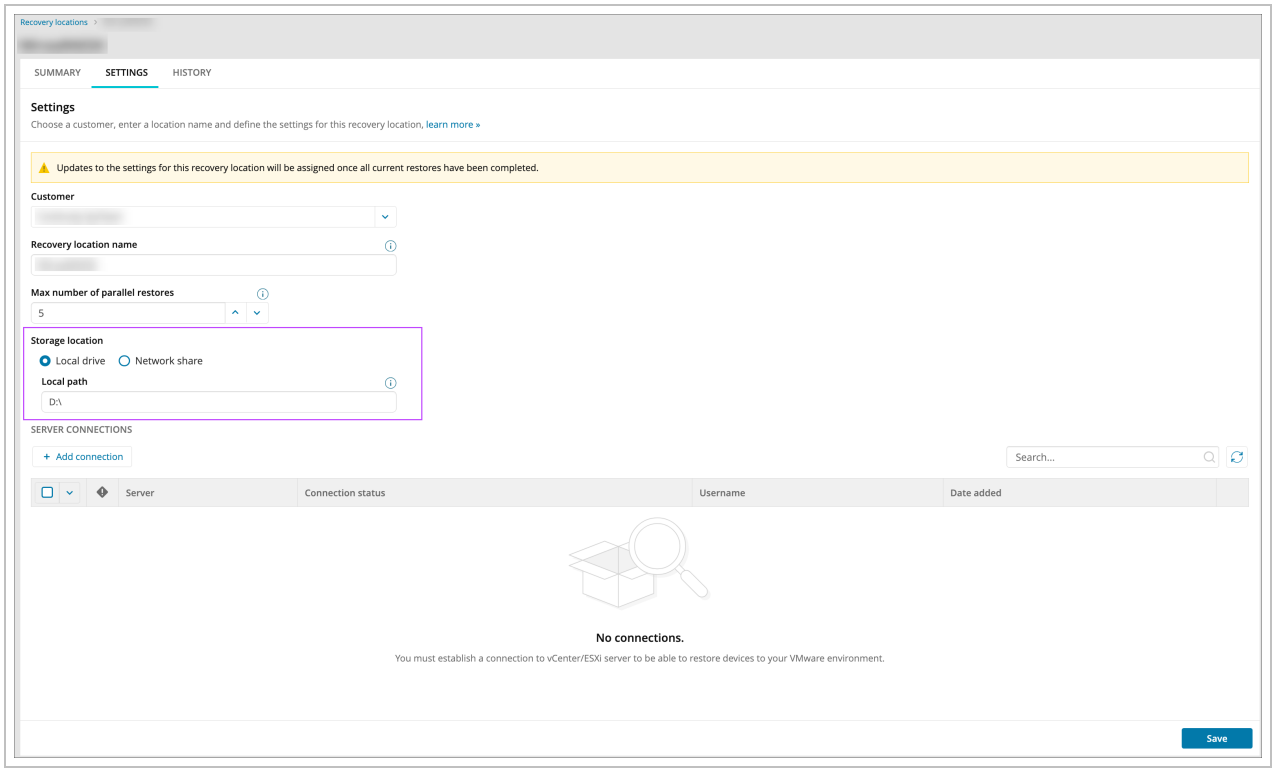
Step 5: Add Storage Location and Server Connections

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**

3. Find the new recovery location in the list and click **Add storage location**

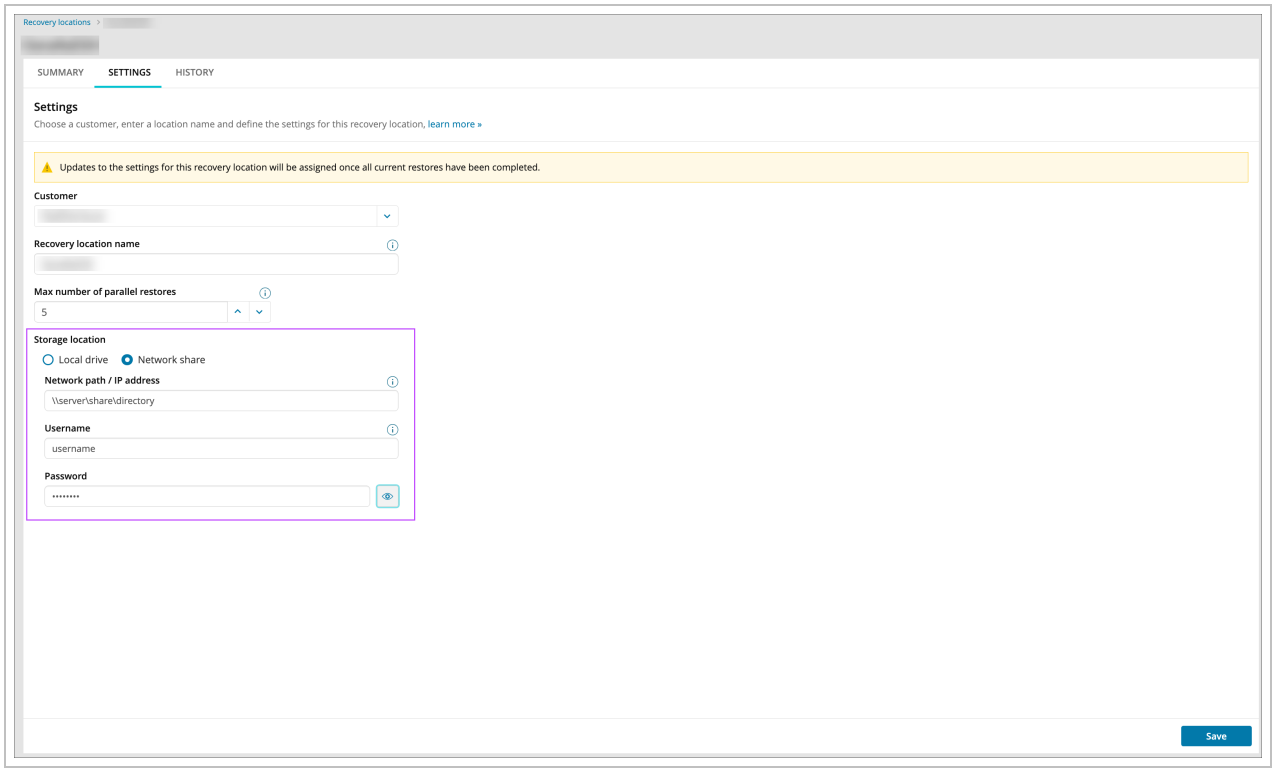


4. Provide local file path for the storage location
   - Local Drive (only available for Hyper-V and ESXi locations):



> Without a storage location, connections **cannot** be made to any of the added servers. If you want to restore to Local VMDK is not obligatory to configure server connections. The VMDK file will be restored directly to the storage path, and not on the ESXi server.

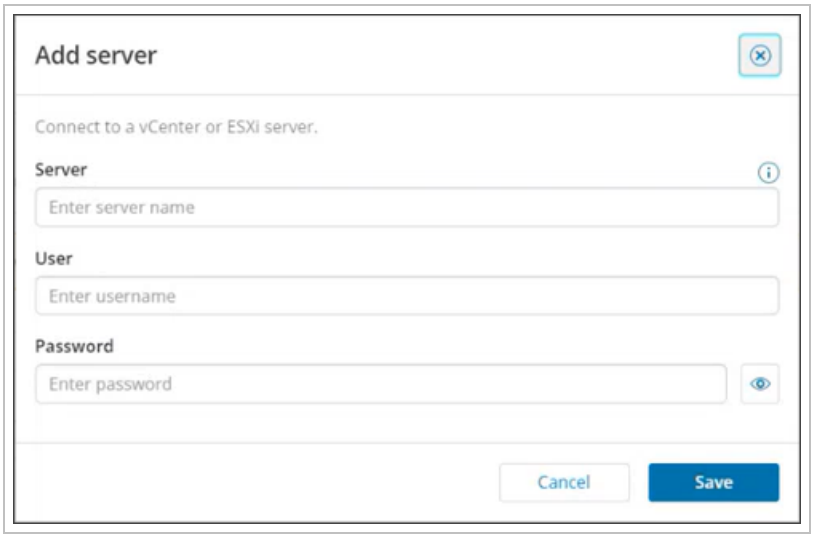
- Network Share:



> Recovery Locations using **Network Shares** will **not** see the option to configure any server connections as the restore will not be done on an ESXi server, and will be done on the Network Share to a Local VMDK restore format.

5. Click **Add Connection** to connect to the vCenter or ESXi server

> If using a connection to the vCenter server, you will be able to restore to any ESXi host connected to the vCenter server



6. Enter the vCenter or ESXi **server name** or **IP address**, and your username and password for this
7. Click **Save**

> Multiple server connections can be added to the recovery location, but must be done one at a time. Doing so will allow you to connect and restore to several ESXi hosts which are not connected to one vCenter Server

> You must click the **refresh** button to above the list of server connections to update the status from 'connecting' to 'connected'. The connection may take a few minutes.

Step 6: Add device to Standby Image plan

Once the server connections are added, you may now add devices to the Standby Image to ESXi recovery plan by following the instructions in Top bar menu

Configure N-able Recovery Service on Hyper-V Server 2019

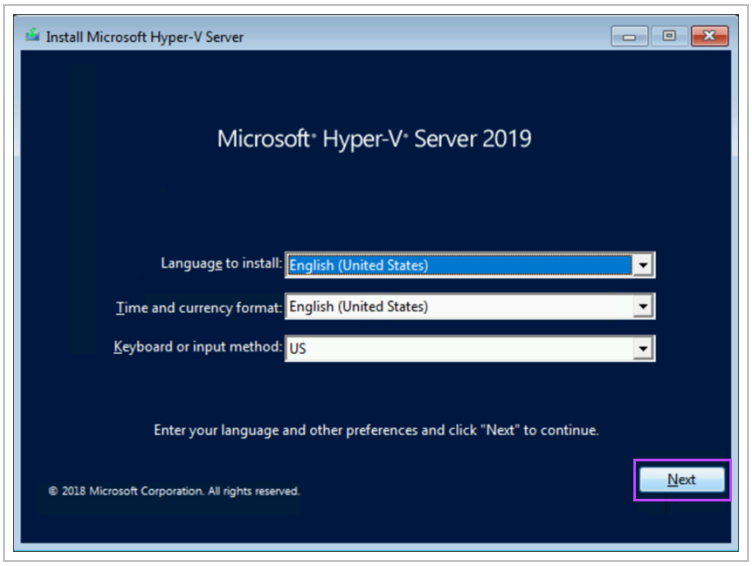
Installing the Recovery Locations recovery service on a Hyper-V Server 2019 requires additional configuration during the setup of the Hyper-V:

- Check the Requirements
- Configuration
  - Step 1: Install the Hyper-V Server
  - Step 2: Configure the Hyper-V Server
  - Step 3: Download the Recovery Service
  - Step 4: Add a role for Hyper-V
  - Step 5: Install and Configure the Recovery Location

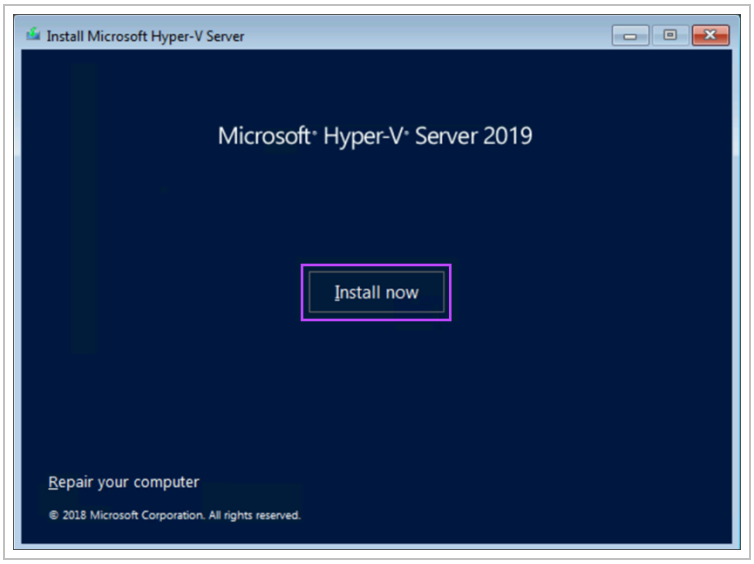
Configuration

Step 1: Install the Hyper-V Server

1. Open the Microsoft Evaluation Center
2. Download the **Hyper-V Server 2019** ISO
3. Create bootable media (e.g. USB drive)
4. Ensure the recovery machine will boot from the bootable media
5. Begin the installation of Hyper-V Server 2019
6. Select your preferred language, time and currency format and keyboard or input method, then click **Next**

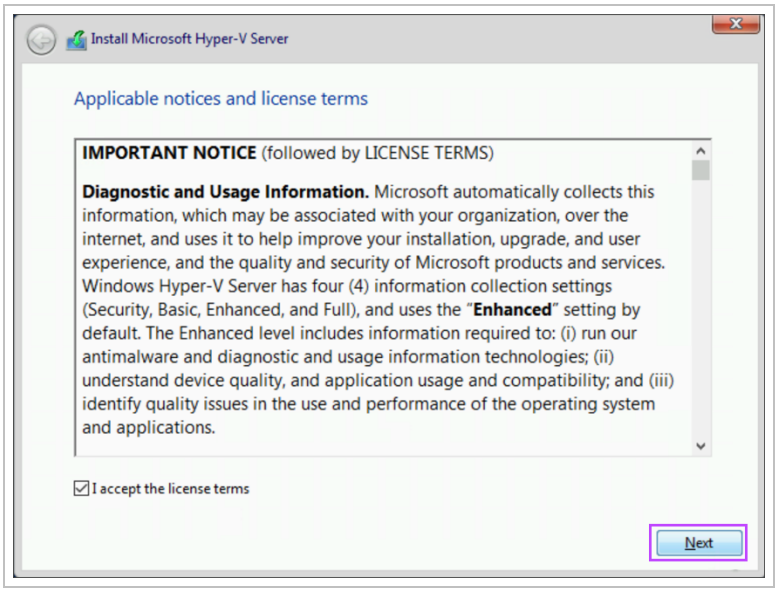


7. Click **Install Now**

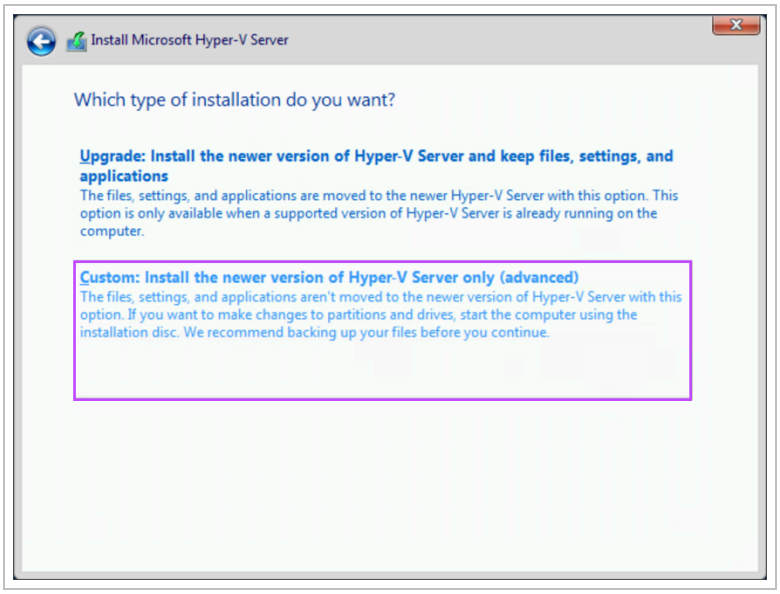


8. Accept the notices and license terms

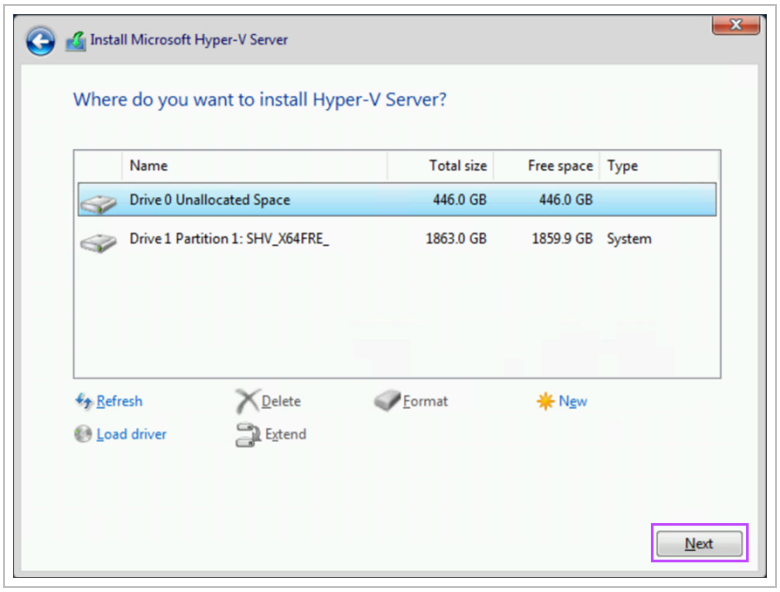
9. Click **Next**



10. On the Installation type screen, select **Custom**



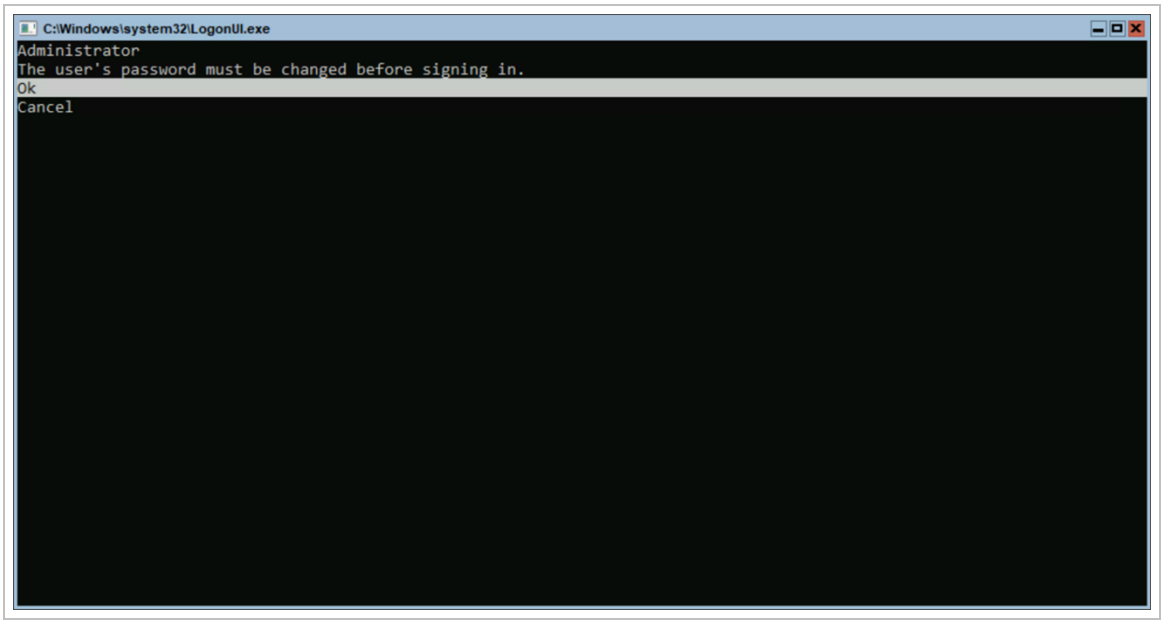
11. Select the drive you want top install the Hyper-V Server on



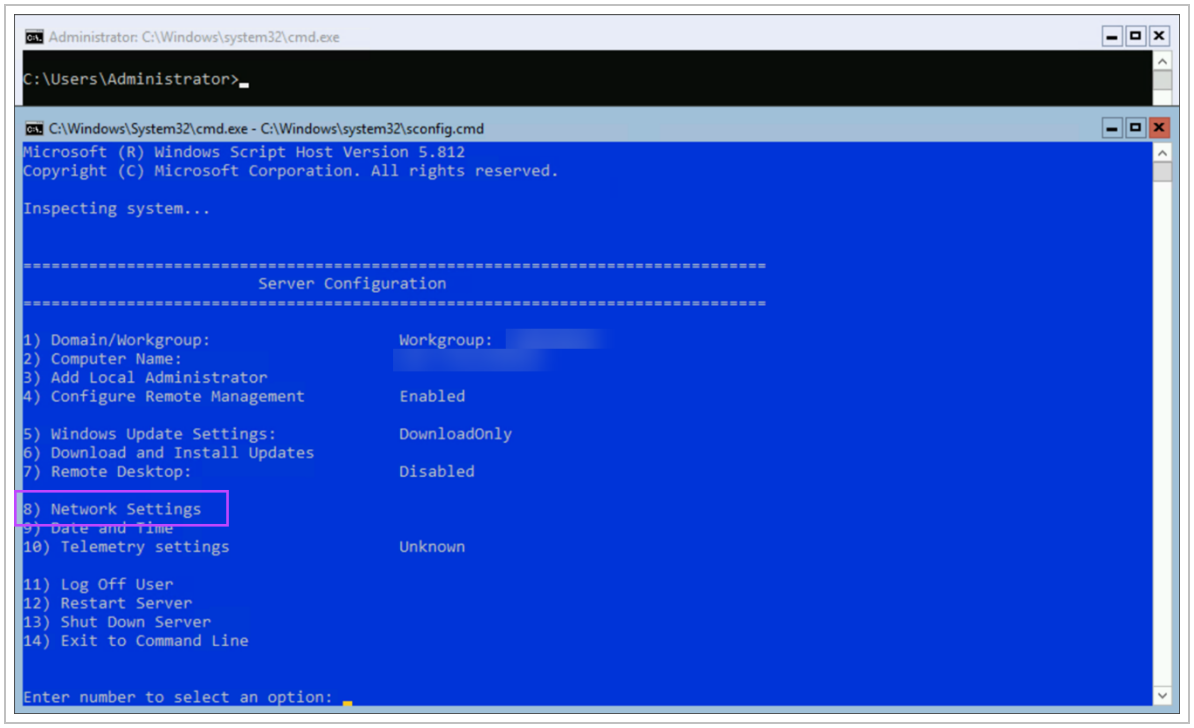
12. The installation will now run, the machine will restart to finalize the installation

Step 2: Configure the Hyper-V Server

1. When the machine boots after Hyper-V Server installation, follow the instructions on screen to set an Administrator Password

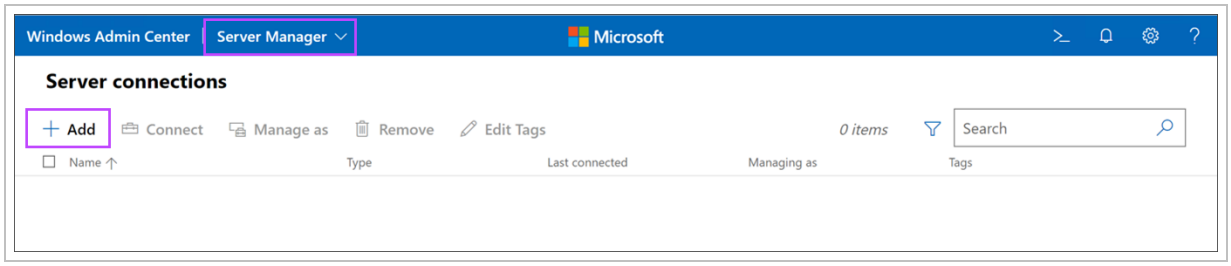


2. Ensure the Network Settings are configured correctly. These can be found under **option 8** of the Server Configuration



> Setup of the recovery service will **not** be successful without an internet connection

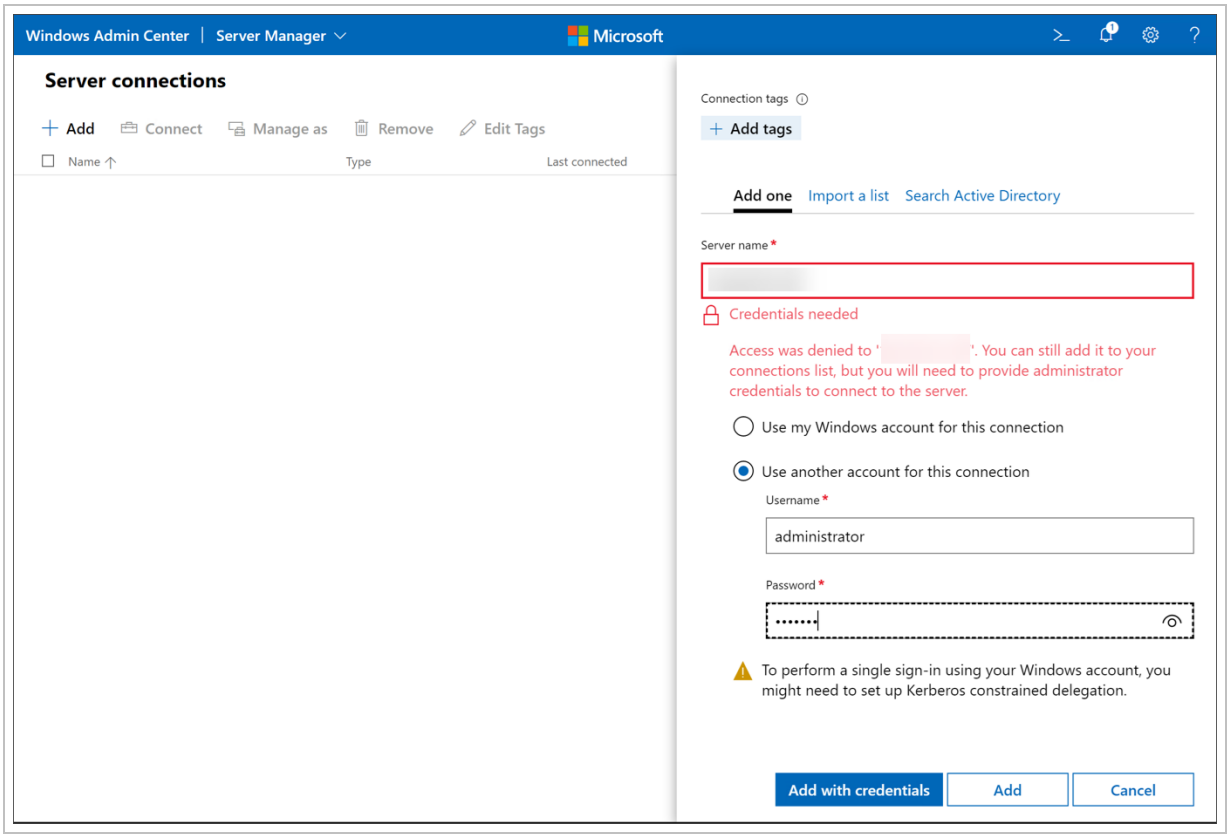
3. Use **option 14** to exit the command line once all configuration has been completed
4. Start the **Windows Admin Center** on the management machine
5. Navigate to **Server Manager** then into **Server Connections**
6. Click **Add** to add the Hyper-V Server



7. Enter the details of the Hyper-V server:
   - **Server Name:** Enter the IP address of the Hyper-V Server

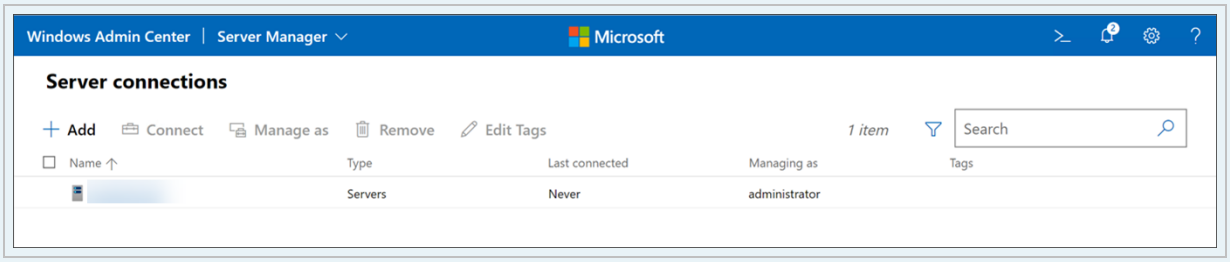
     > You will be required to provide access credentials to connect to the server, click **Use another account for this connection**

   - **Username:** Enter Administrator
   - **Password:** Enter the password configured in Step 2:1



8. Click **Add**

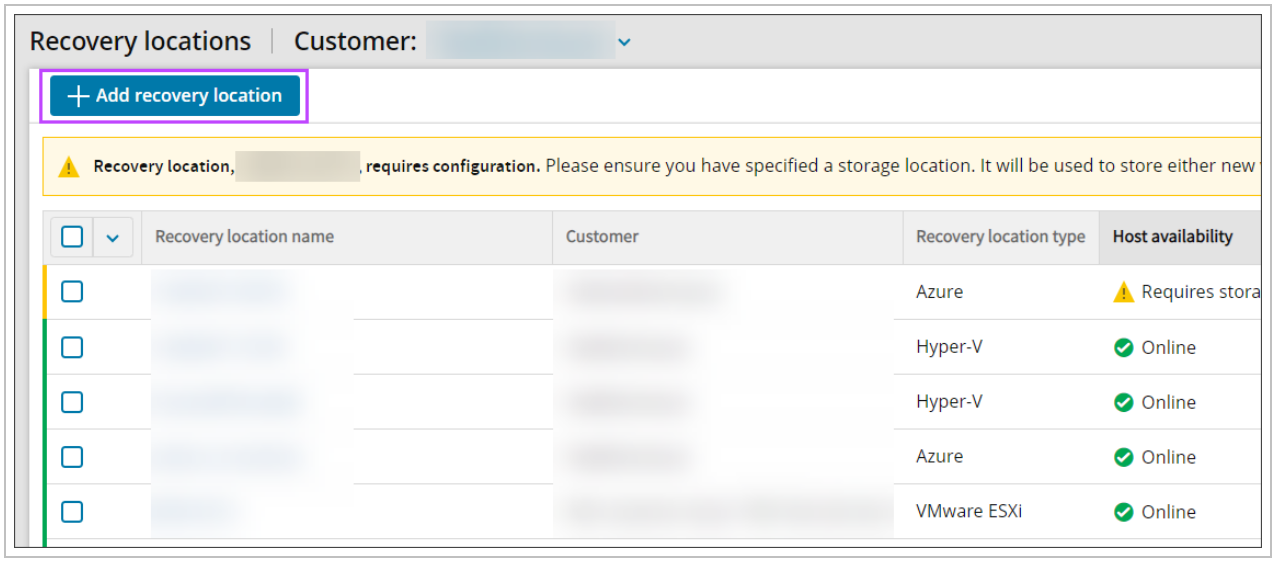
> Once added, the Hyper-V Server will be displayed in the list of connections



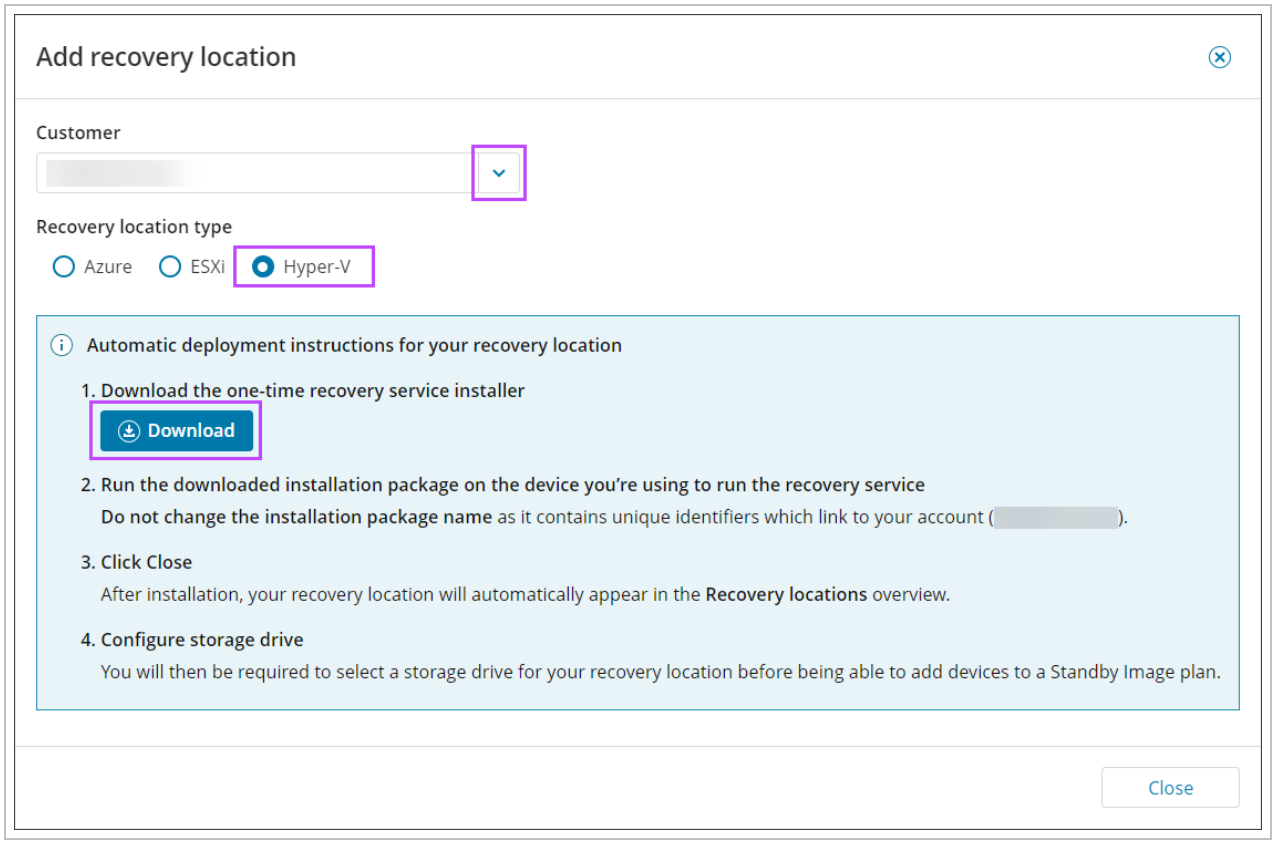
> You can view an overview of information related to the device by clicking the server name/IP address in the list.

Step 3: Download the Recovery Service

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Recovery** > **Recovery Locations**
3. Click **Add recovery location** at the top of the page



4. In the **Add Recovery Location wizard**, select the customer to attribute the recovery location to, from the dropdown



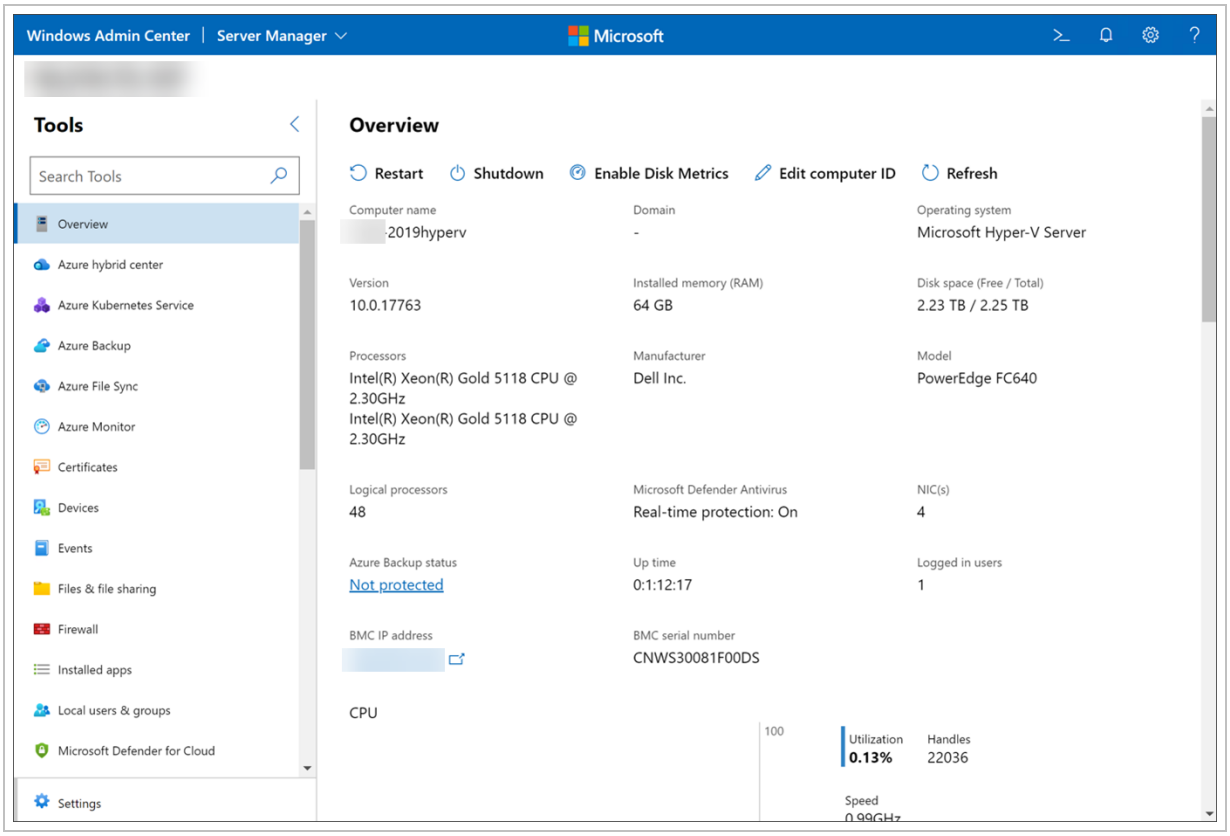
5. Download the recovery service installer and save it to your USB drive

> Do **not** change the installation package name. The installation package name contains unique identifiers to your account.
>
> This is a one-time installer and can only be used to install a single instance of the recover service. The installer will fail if you attempt to use the same package for another installation.

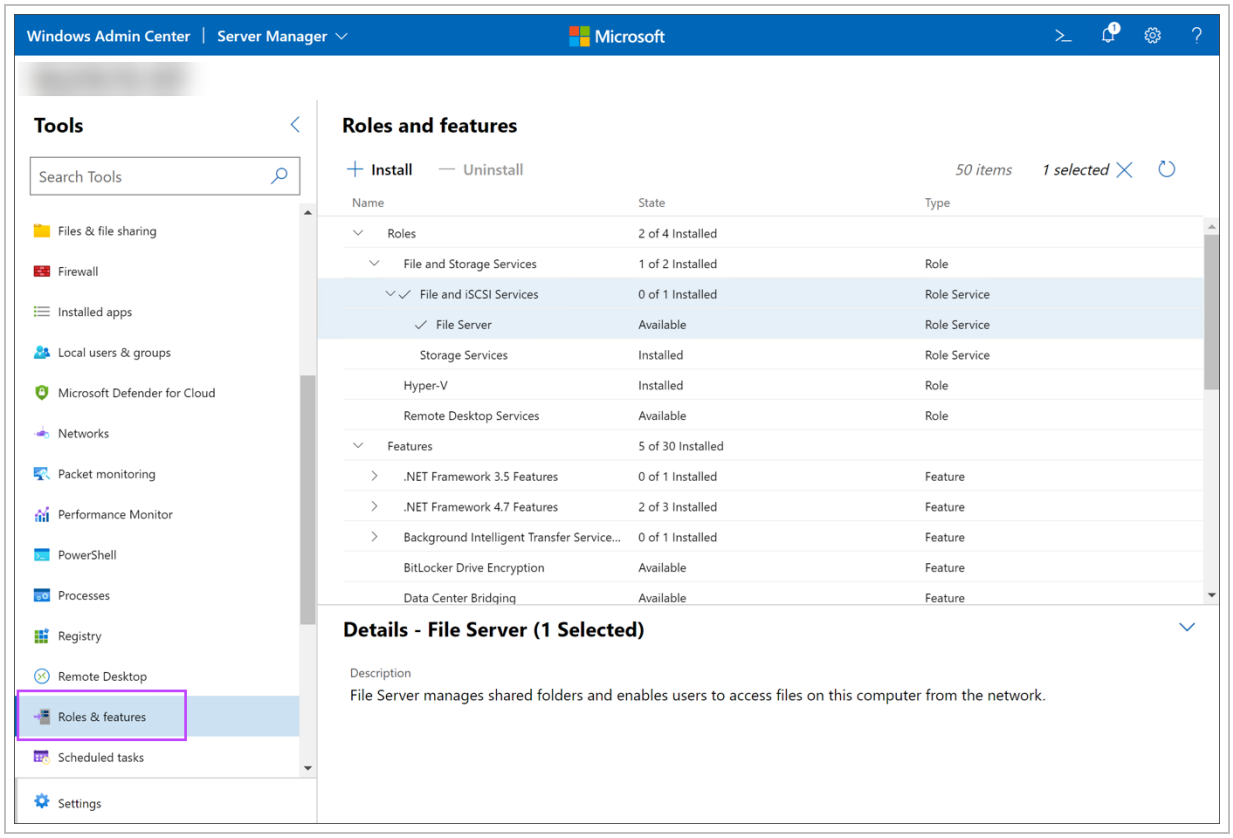
> Do **not** run the installer at this point, there are additional changes that are required first.

Step 4: Add a role for Hyper-V

1. Return to the **Windows Admin Center** on the management machine
2. Navigate to **Server Manager** then into **Server Connections**
3. Open the overview the Hyper-V server from the list of connections by clicking the server name/IP address in the list

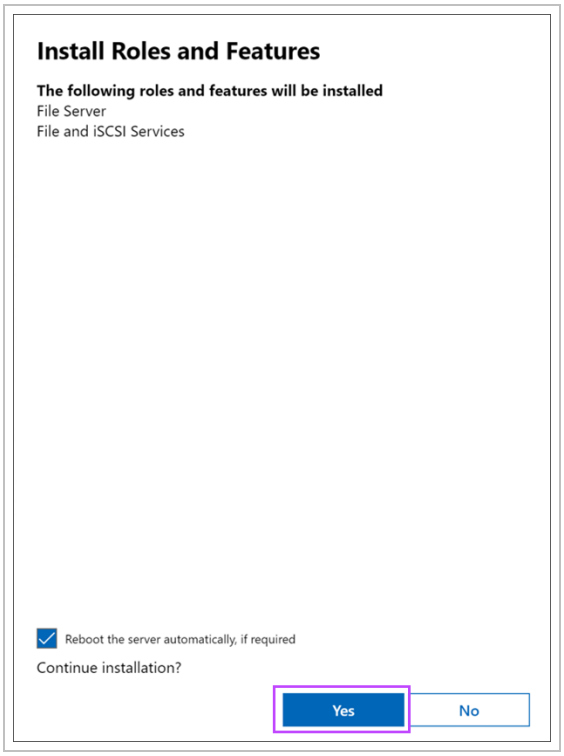


4. In the left-hand **Tools** menu, select **Roles and features**



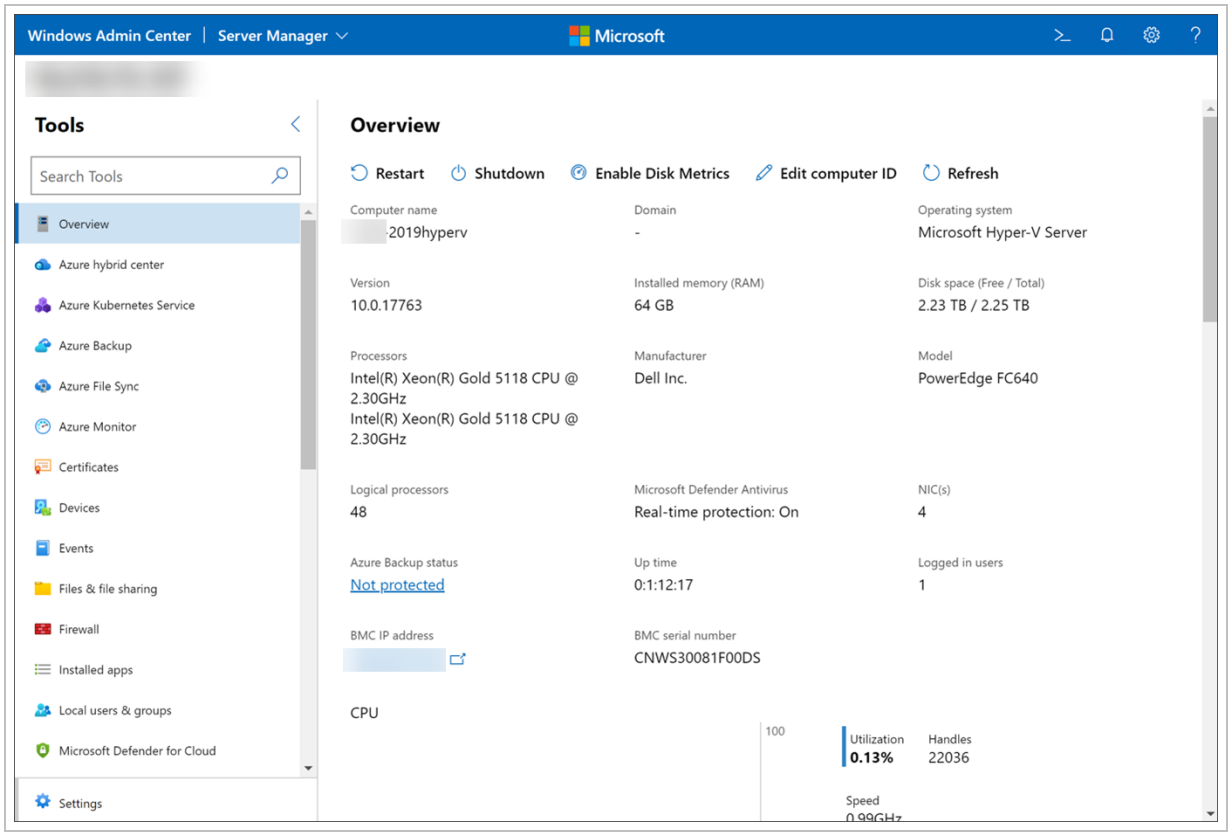
5. Expand **Roles > Files and Storage Services**, select **File abd iSCSI Services**
6. Click **Install**

7. Confirm role installation



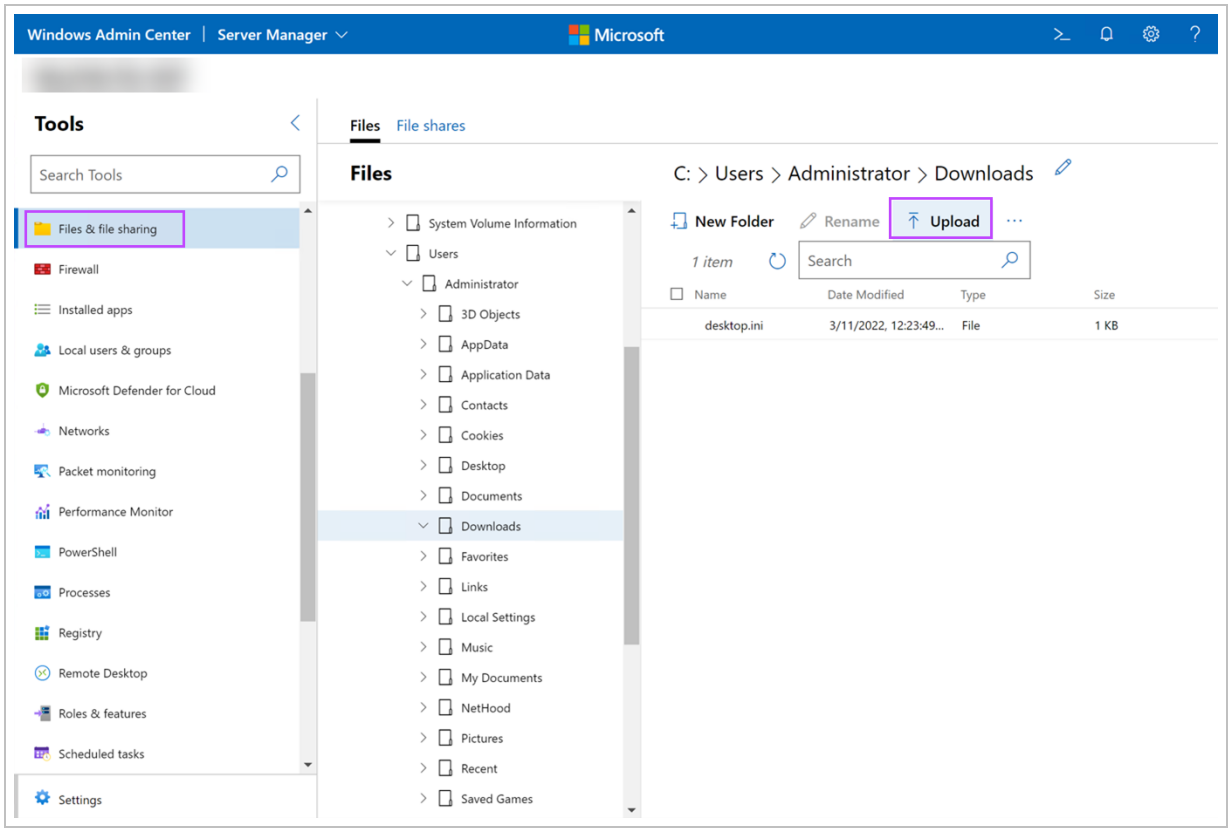
Step 5: Install and Configure the Recovery Location

1. In the **Windows Admin Center**, navigate to **Server Manager** then into **Server Connections**
2. Open the overview the Hyper-V server from the list of connections by clicking the server name/IP address in the list



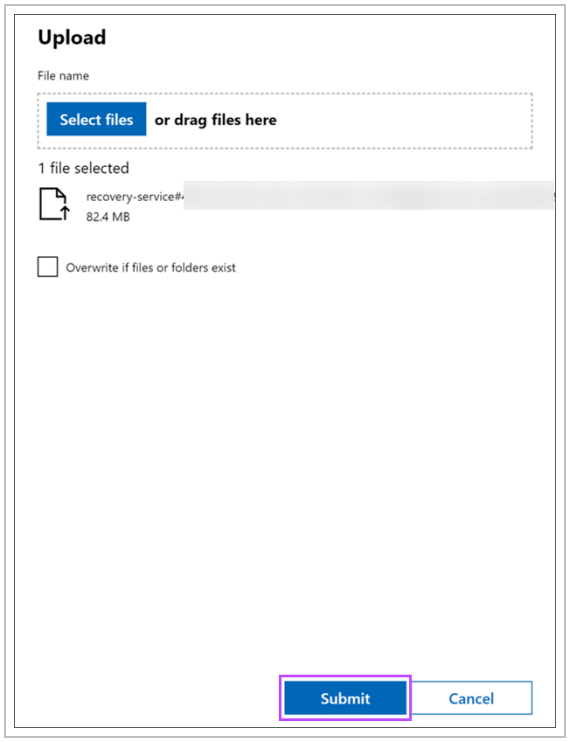
3. In the left-hand **Tools** menu, select **Files & file sharing**

4. Using the file structure, browse to the folder you want to upload the Recovery Location's recovery service installer to on the Hyper-V Server



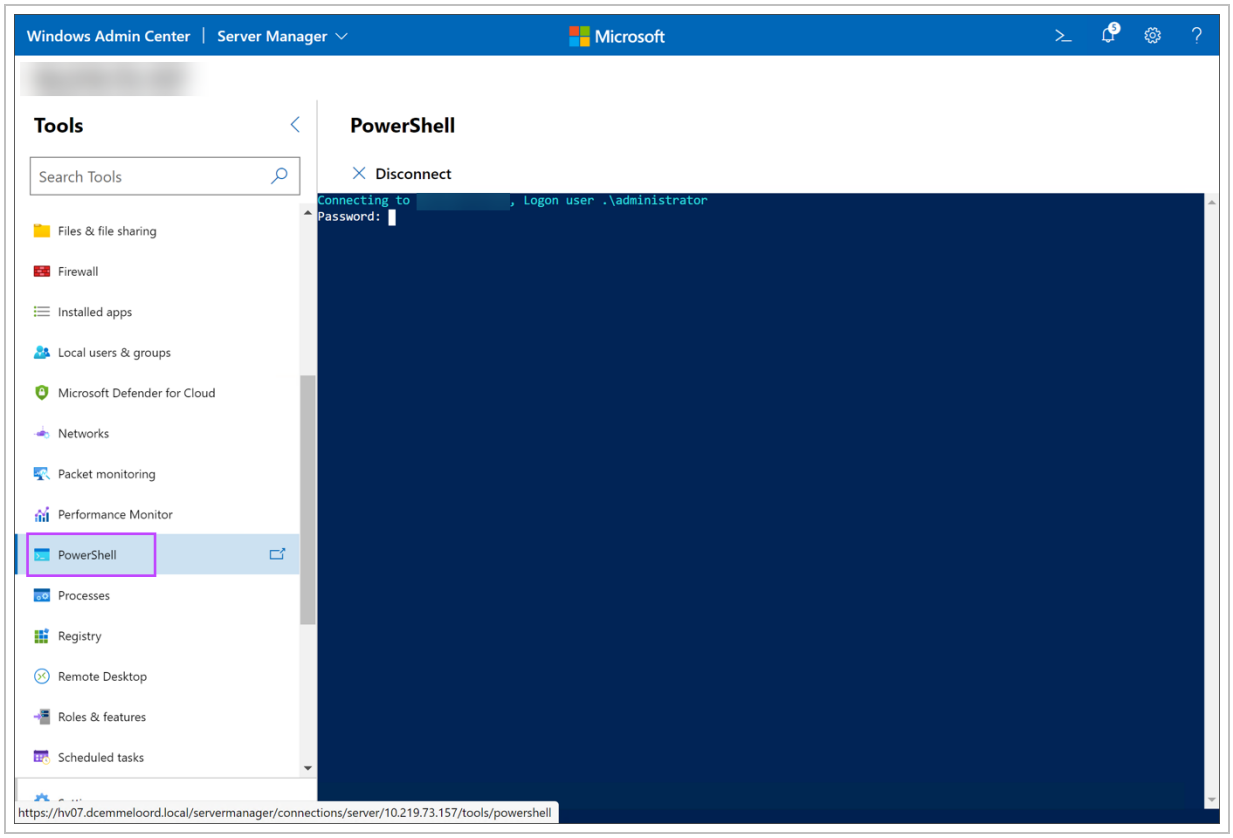
5. Click **Upload**
6. Browse to the downloaded installer file from Step 3:5 and click **Open** to begin the upload to the Hyper-V server

7. Once the file appears in the upload window, click **Submit**



8. Once the upload completes, select **PowerShell** from the left-hand **Tools** menu

9. Login using the **Administrator** credentials



10. Browse to the directory selected in the upload in Step 5:4 using the `cd` command
11. Enter the installer filename

> You can enter `.\re` and press **TAB**, this will populate the full name automatically, so long as no other file in this location begins with `re`

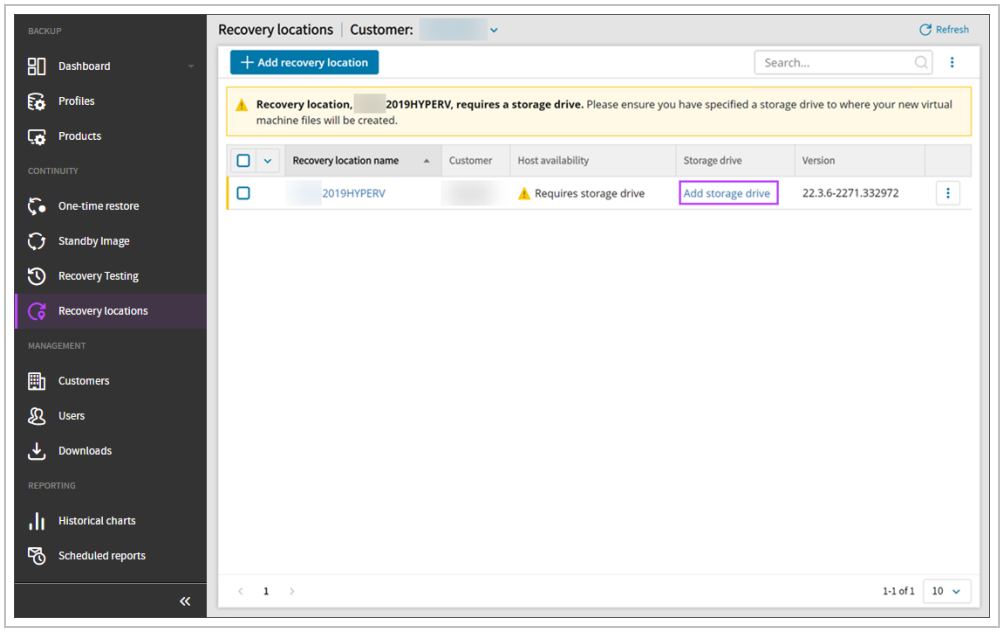
12. Make sure to add `/S` (case sensitive) after the installer filename, or the installation will not complete
13. Press **Enter**

> Once the execution of the installer has been confirmed, PowerShell will return to the standard prompt (`PS C:\Users\Administrator\Downloads>`).

> Depending on the performance of the machine, this can take between a few seconds and a few minutes. Do not try to speed up the process by hitting enter multiple times or closing out of the PowerShell.

14. Exit the PowerShell and navigate to **Installed Apps** in the left-hand **Tools** menu. **Recovery Service** will be listed in the Installed Apps page
15. Log in to the Management Console under a **SuperUser** account

16. Navigate to **Recovery** > **Recovery Locations**. The new Recovery Location will now be displayed in the list of locations under the customer selected in Step 3:4
17. Enter the storage drive to assign where the Standby Images are going to be restored to by clicking **Add storage drive** and entering the drive location. E.g. `D:\`



18. You can now add devices using the Standby Image plan using this Recovery Location

Manage Recovery Locations

> Permissions to modify storage locations to a Network Share are available for Reseller level and lower, for SuperUsers with Security Officer permissions *only*.

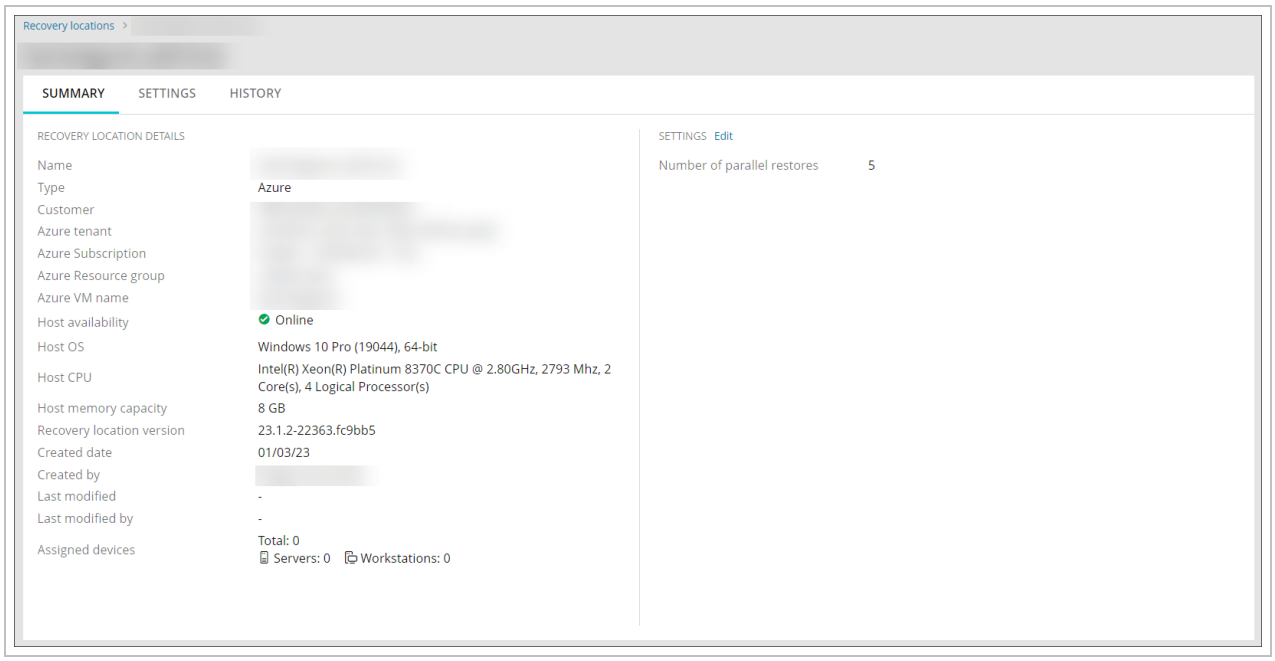
View Recovery Location Summary

A summary of information relating to each Recovery Location can be viewed one at a time from the **Continuity** > **Recovery Locations** page using one of four methods for both Self-hosted (for Standby Image) and Azure location types.

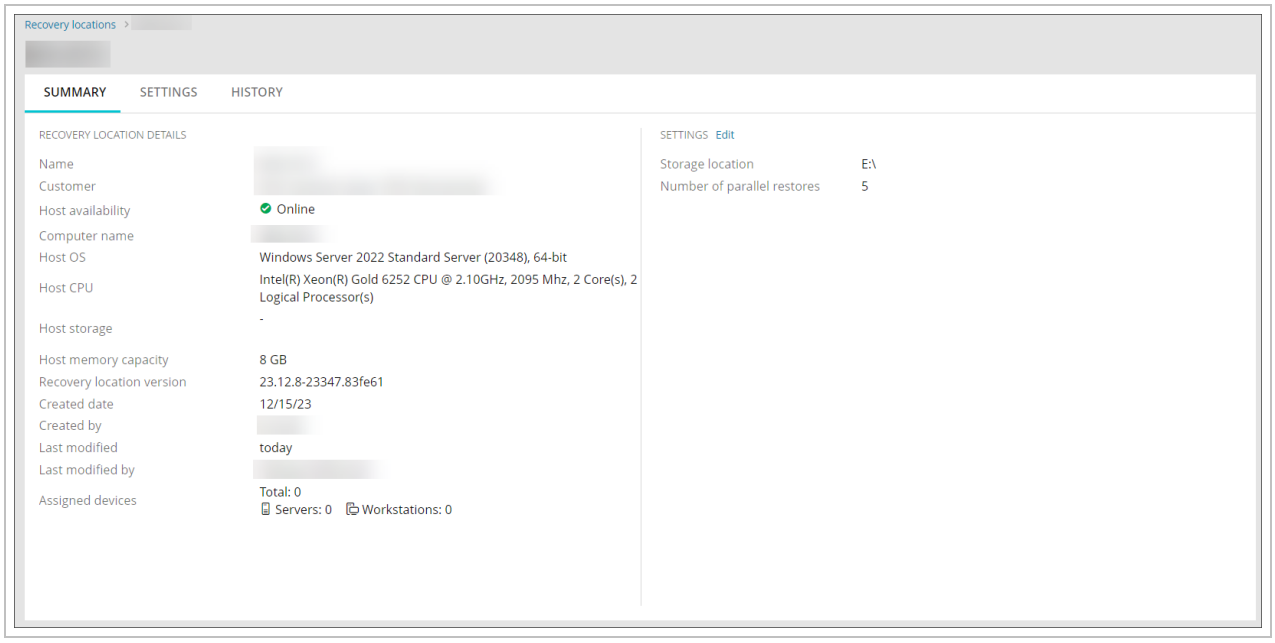
1. Recovery Location name
   a. Select the recovery location name to open the Summary page
2. Top bar menu
   a. Select the checkbox for the Recovery Location
   b. At the top of the Recovery Locations page, select **Edit**
   c. Switch to the **Summary** tab
3. Location context menu
   a. Right-click on the Recovery Location to edit
   b. Select **Edit**
   c. Switch to the **Summary** tab

4. Right hand menu
    a. Click the action menu for the Recovery Location, seen as three dots in a vertical line to the right of the location's version
    b. Select **Edit**
    c. Switch to the **Summary** tab

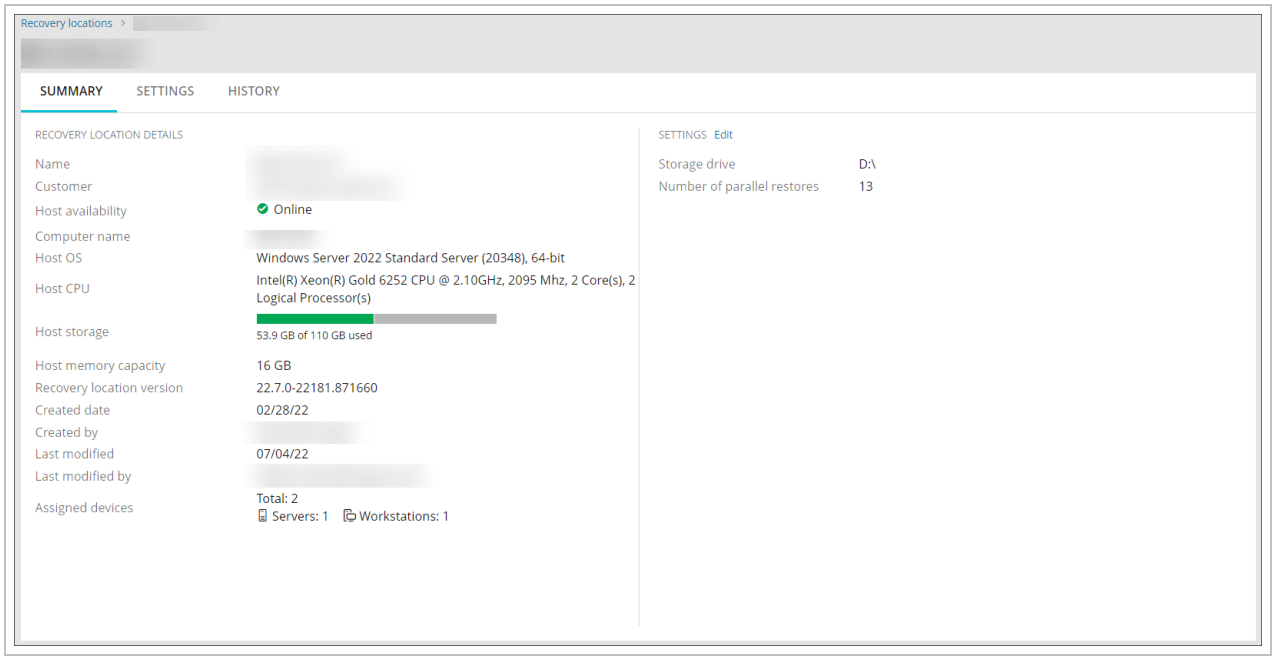
Azure:



ESXi:



Hyper-V:

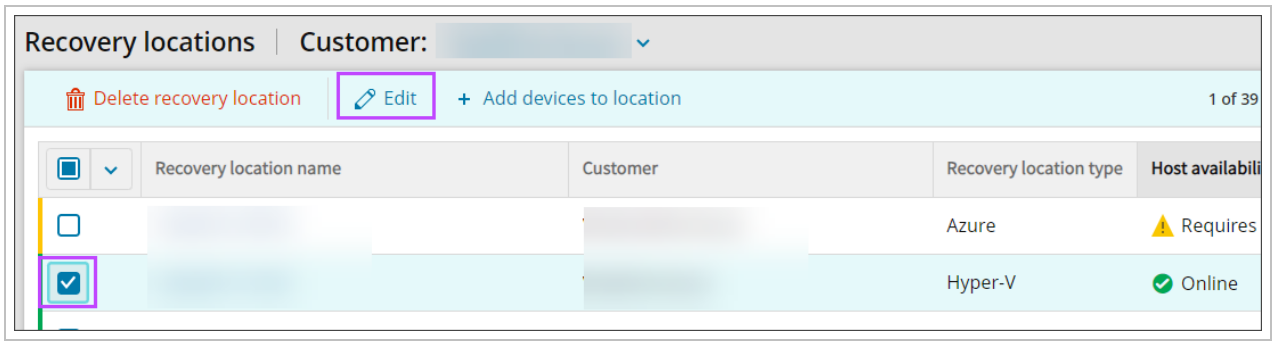


Edit Recovery Location

Recovery Locations can be edited one at a time from the **Continuity** > **Recovery Locations** page using one of four methods for Azure, ESXi and Hyper-V location types.

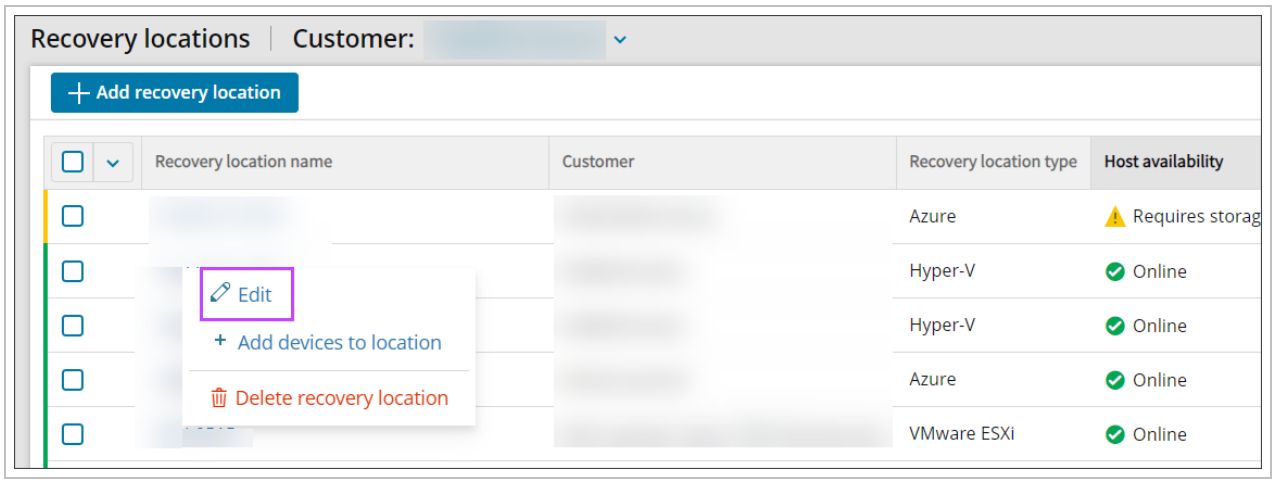
1. Recovery Location name
    a. Select the recovery location name to open the Summary page
    b. Switch to the **Settings** tab
    c. Make any required changes to the following aspects of the recovery location:
        - **Customer** - change the customer the storage location belongs to
        - **Recovery Location Name** - change the name of the machine or server used to store your device restores
        - **Max number of parallel restores** - manage the workload on the recovery machine by limiting the number of concurrent restores that can take place
        - **Storage Location** - set the recovery location to the appropriate type
            - **Local Drive** - The local path to the folder where your virtual machine files will be stored. This can be either a location at a drive, Cluster Shared Volume, or the drive itself. Examples:
                - C:\Virtual_Machines
                - D:\
            - **Network Share**(available only for Hyper-V and ESXi) - Only available if all devices assigned to this recovery location are being restored to Local VHDX / Local VMDK files, remove any devices restoring to Hyper-V or ESXi on the recovery location to use Network Share
                - Network path / IP address
                - Username
                - Password
        - **Server Connections** (Available only for ESXi) - see Step 5: Add Storage Location and Server Connections for instructions on connecting to the vCenter or ESXi Server
    d. Click **Save**

2. Top bar menu
   a. Select the checkbox for the Recovery Location to edit
   b. At the top of the Recovery Locations page, select **Edit**



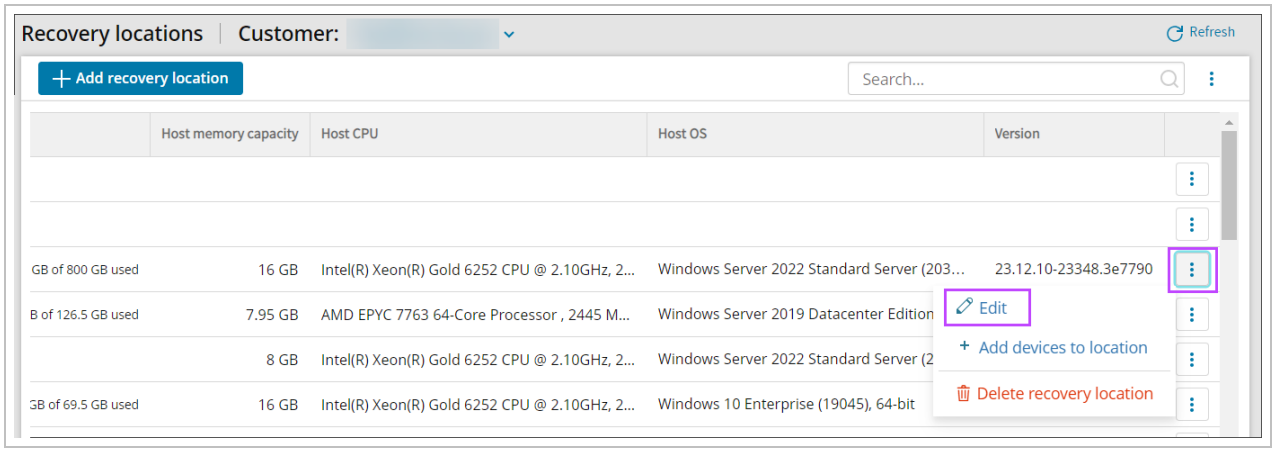
   c. Make any required changes to the following aspects of the recovery location:
      - **Customer** - change the customer the storage location belongs to
      - **Recovery Location Name** - change the name of the machine or server used to store your device restores
      - **Max number of parallel restores** - manage the workload on the recovery machine by limiting the number of concurrent restores that can take place
      - **Storage Location** - set the recovery location to the appropriate type
        - **Local Drive** - The local path to the folder where your virtual machine files will be stored. This can be either a location at a drive, Cluster Shared Volume, or the drive itself. Examples:
          - C:\Virtual_Machines
          - D:\
        - **Network Share**(available only for Hyper-V and ESXi) - Only available if all devices assigned to this recovery location are being restored to Local VHDX / Local VMDK files, remove any devices restoring to Hyper-V or ESXi on the recovery location to use Network Share
          - Network path / IP address
          - Username
          - Password
      - **Server Connections** (Available only for ESXi) - see Step 5: Add Storage Location and Server Connections for instructions on connecting to the vCenter or ESXi Server
   d. Click **Save**

3. Location context menu
   a. Right-click on the Recovery Location to edit
   b. Select **Edit**



   c. Make any required changes to the following aspects of the recovery location:
      - **Customer** - change the customer the storage location belongs to
      - **Recovery Location Name** - change the name of the machine or server used to store your device restores
      - **Max number of parallel restores** - manage the workload on the recovery machine by limiting the number of concurrent restores that can take place
      - **Storage Location** - set the recovery location to the appropriate type
        - **Local Drive** - The local path to the folder where your virtual machine files will be stored. This can be either a location at a drive, Cluster Shared Volume, or the drive itself. Examples:
          - C:\Virtual_Machines
          - D:\
        - **Network Share**(available only for Hyper-V and ESXi) - Only available if all devices assigned to this recovery location are being restored to Local VHDX / Local VMDK files, remove any devices restoring to Hyper-V or ESXi on the recovery location to use Network Share
          - Network path / IP address
          - Username
          - Password
      - **Server Connections** (Available only for ESXi) - see Step 5: Add Storage Location and Server Connections for instructions on connecting to the vCenter or ESXi Server
   d. Click **Save**

4. Right hand menu
   a. Click the action menu for the Recovery Location, seen as three dots in a vertical line to the right of the location's version
   b. Select **Edit**

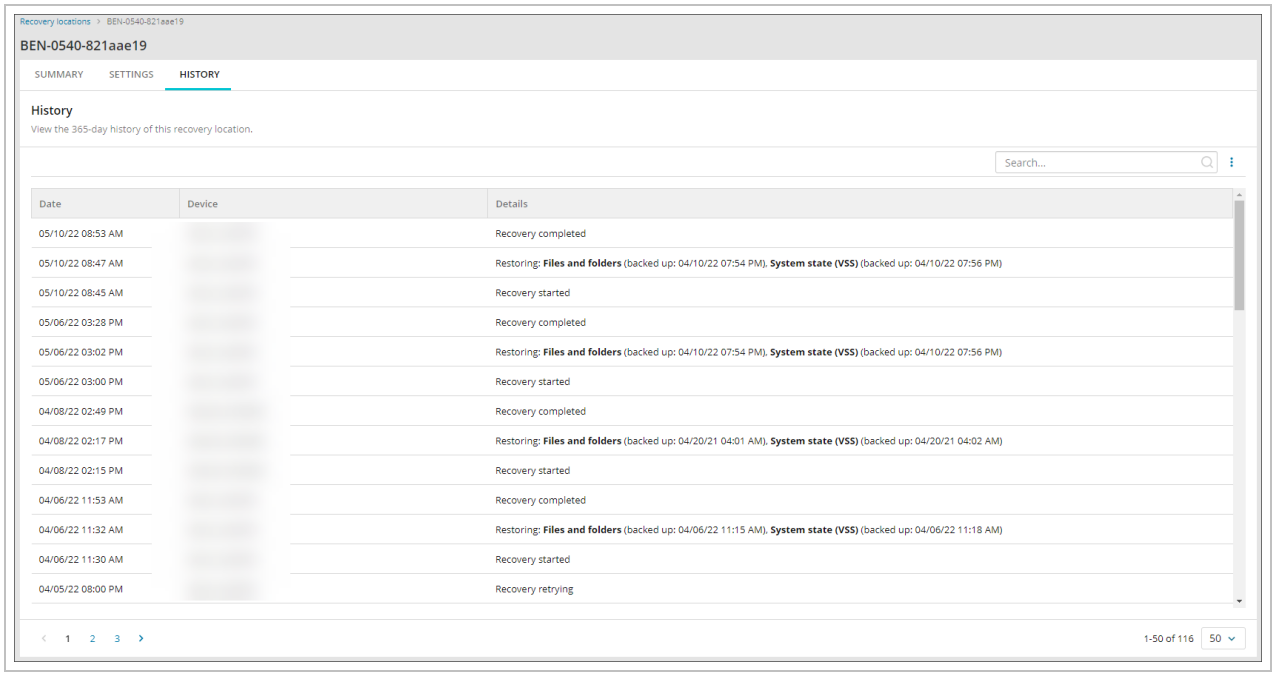


   c. Make any required changes to the following aspects of the recovery location:
      - **Customer** - change the customer the storage location belongs to
      - **Recovery Location Name** - change the name of the machine or server used to store your device restores
      - **Max number of parallel restores** - manage the workload on the recovery machine by limiting the number of concurrent restores that can take place
      - **Storage Location** - set the recovery location to the appropriate type
        - **Local Drive** - The local path to the folder where your virtual machine files will be stored. This can be either a location at a drive, Cluster Shared Volume, or the drive itself. Examples:
          - C:\Virtual_Machines
          - D:\
        - **Network Share**(available only for Hyper-V and ESXi) - Only available if all devices assigned to this recovery location are being restored to Local VHDX / Local VMDK files, remove any devices restoring to Hyper-V or ESXi on the recovery location to use Network Share
          - Network path / IP address
          - Username
          - Password
      - **Server Connections** (Available only for ESXi) - see Step 5: Add Storage Location and Server Connections for instructions on connecting to the vCenter or ESXi Server
   d. Click **Save**

View and Search Recovery Location History

A history of restores relating to each Recovery Location can be viewed one at a time from the History tab when looking from **Continuity** > **Recovery Locations**.

1. Open the Recovery Location by clicking the Recovery Location name
2. Switch to the **History** Tab



3. Using the search bar, it is possible to search by the content in the **Device** column

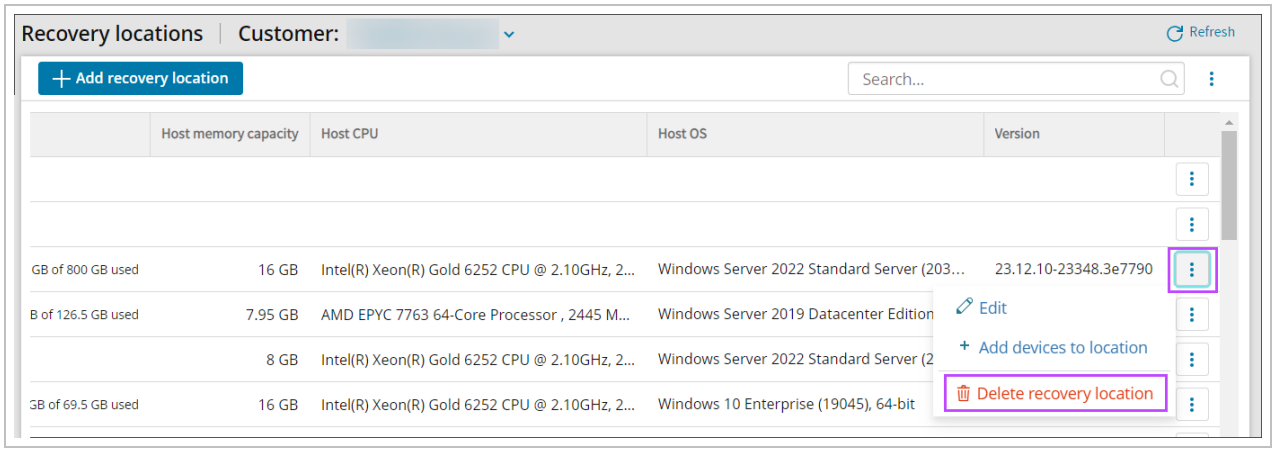
Delete Recovery Location

> Deleting a recovery location will **uninstall** the recovery service and all devices which were using the deleted recovery location will be **unassigned** from the Standby Image plan.

To delete a single recovery location:

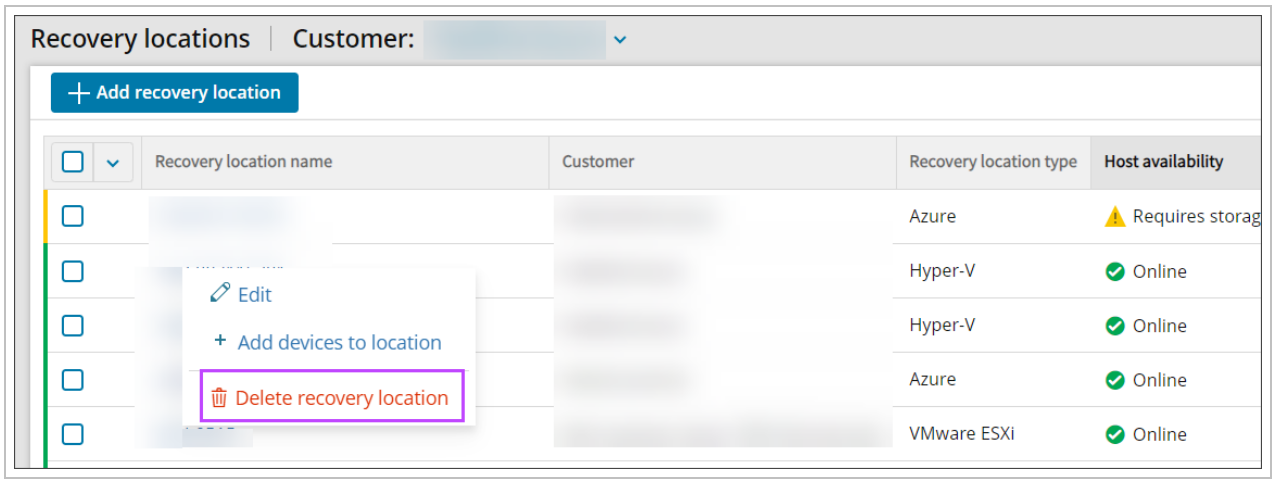
1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Click the action menu for the Recovery Location, seen as three dots in a vertical line to the right of the location's version, or right-click the recovery location to view the context menu

4. Select **Delete recovery location**



Or,

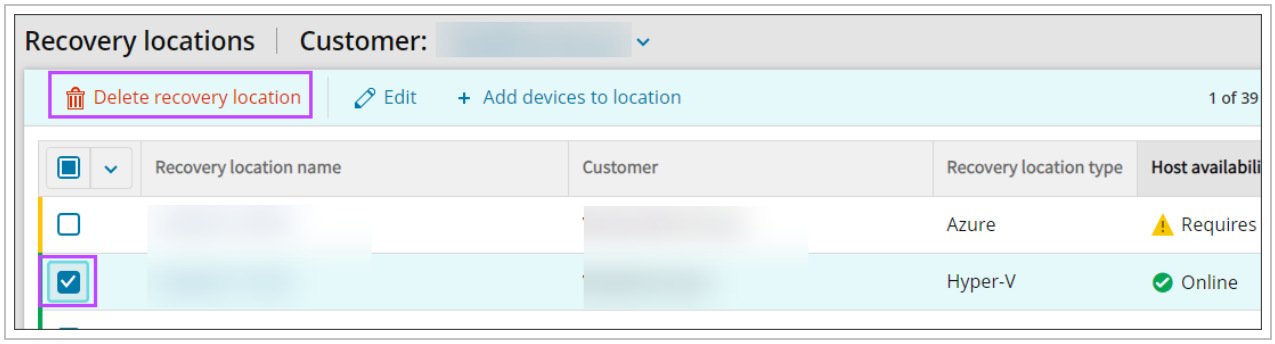
1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Right-click on the Recovery Location to remove
4. Select **Delete recovery location**



Or to delete single or multiple recovery locations:

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Select the checkboxes of any locations you wish to delete

4. At the top of the page click **Delete recovery location**



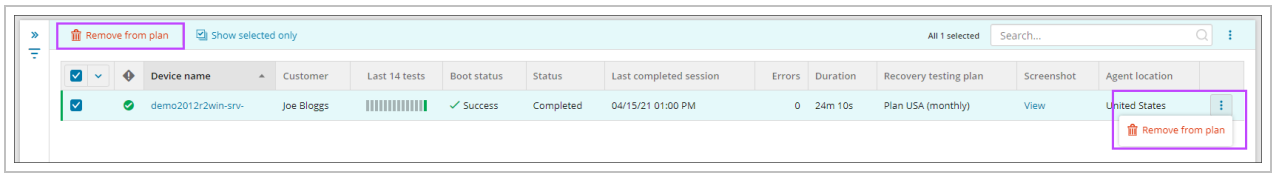
> Deleting a Recovery Location does **not** delete previously stored data. This restored data is kept on the device until manually deleted by the user.

Disabling Recovery Services

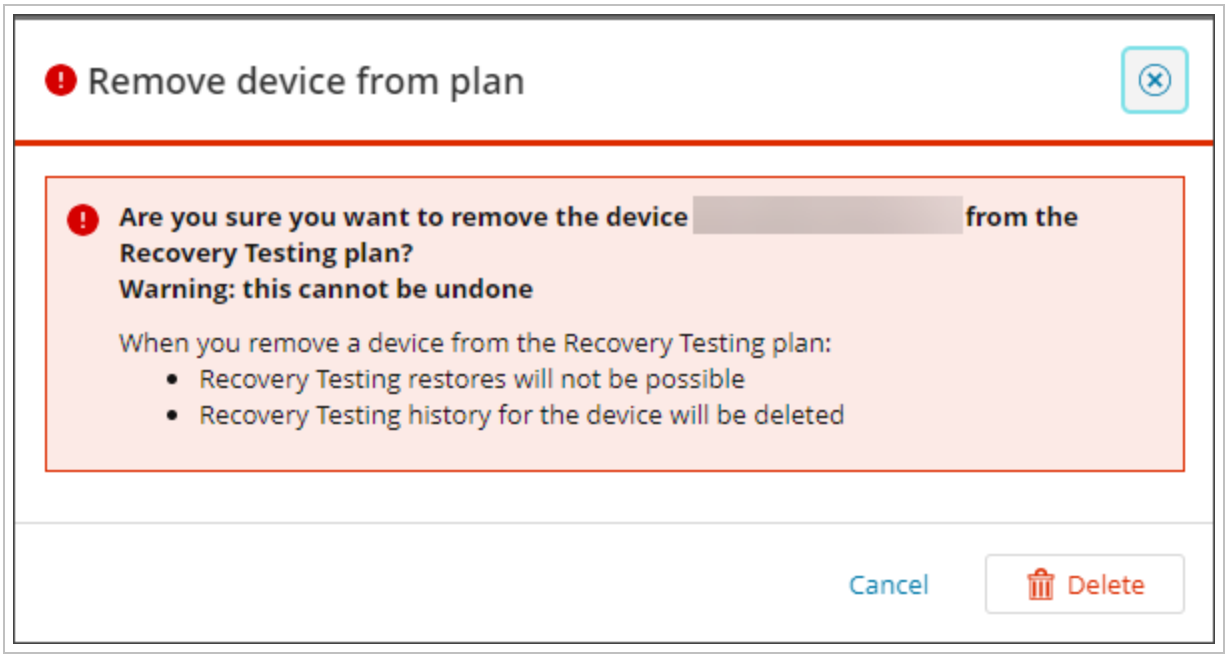
> Removing a plan does not affect previously restored data.

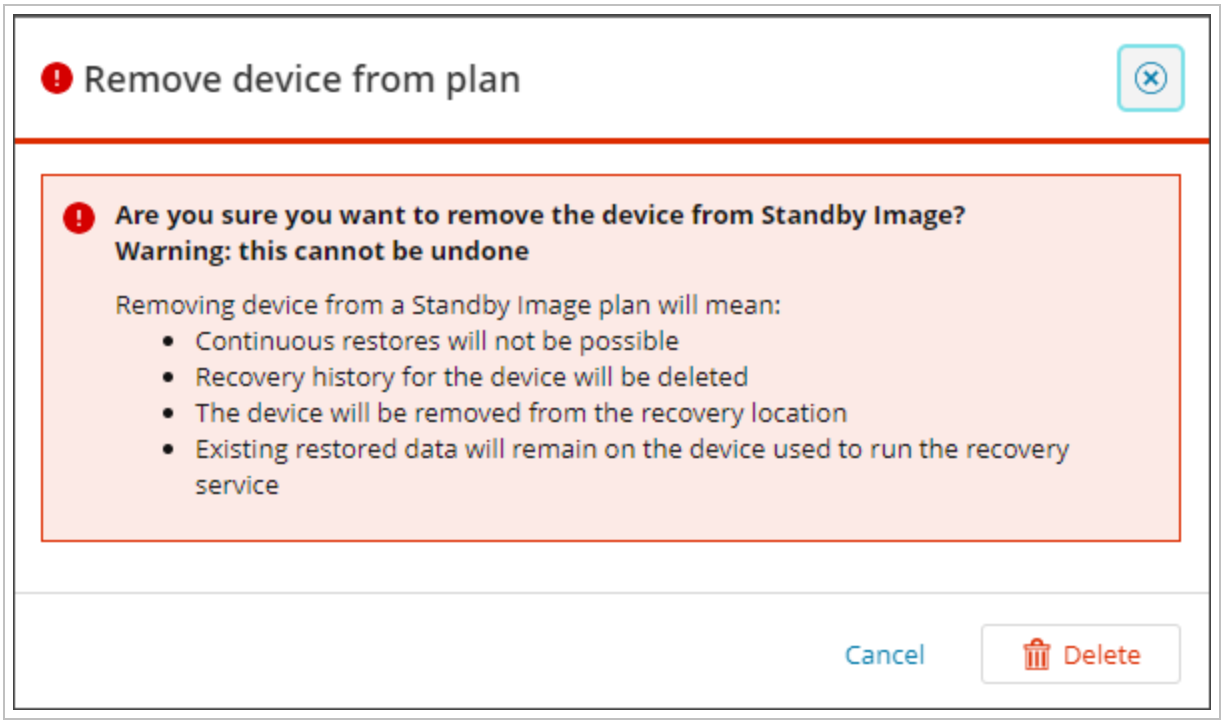
Removing devices from Recovery Testing or Standby plans can be done from the dedicated Recovery Testing and Standby Image Overviews by following the below steps:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Recovery Testing/Standby Image**
3. Select the device(s) you wish to remove the plan from using the checkboxes to the left of the device name, right clicking the device name or use the three dots to the far right of the screen to open the action menu
4. Select **Remove from plan**



5. Confirm your intention to remove the device from the recovery plan by clicking **Delete**



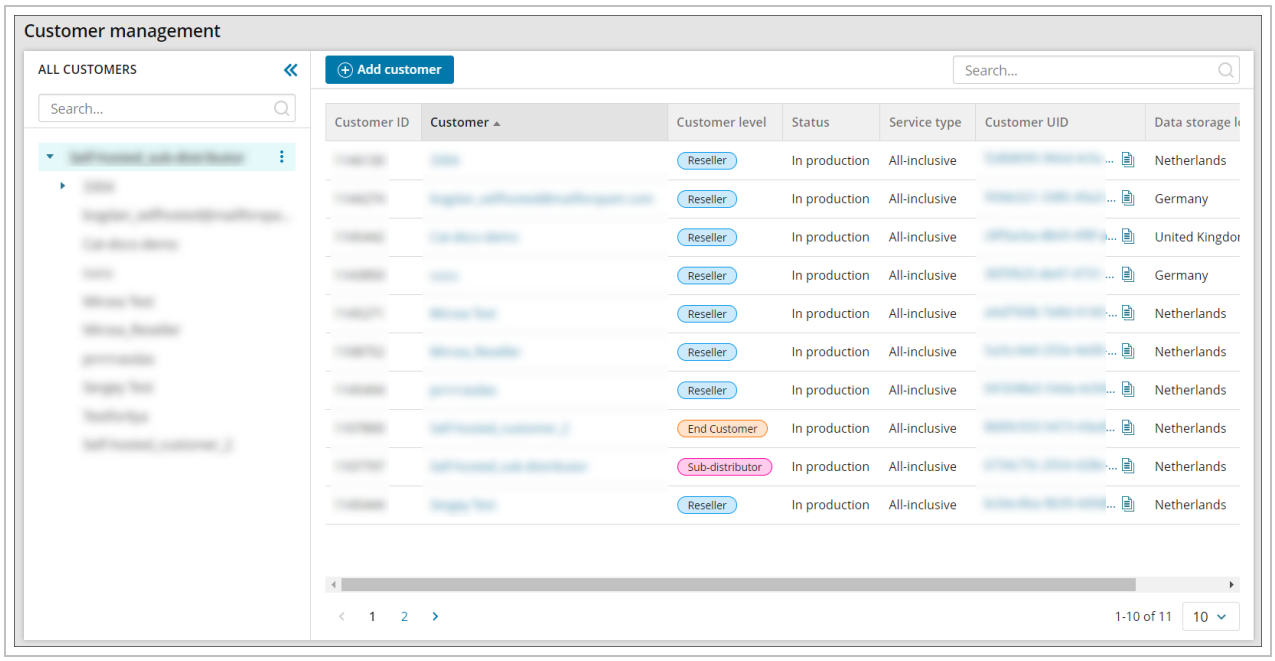


Customer management in Management Console

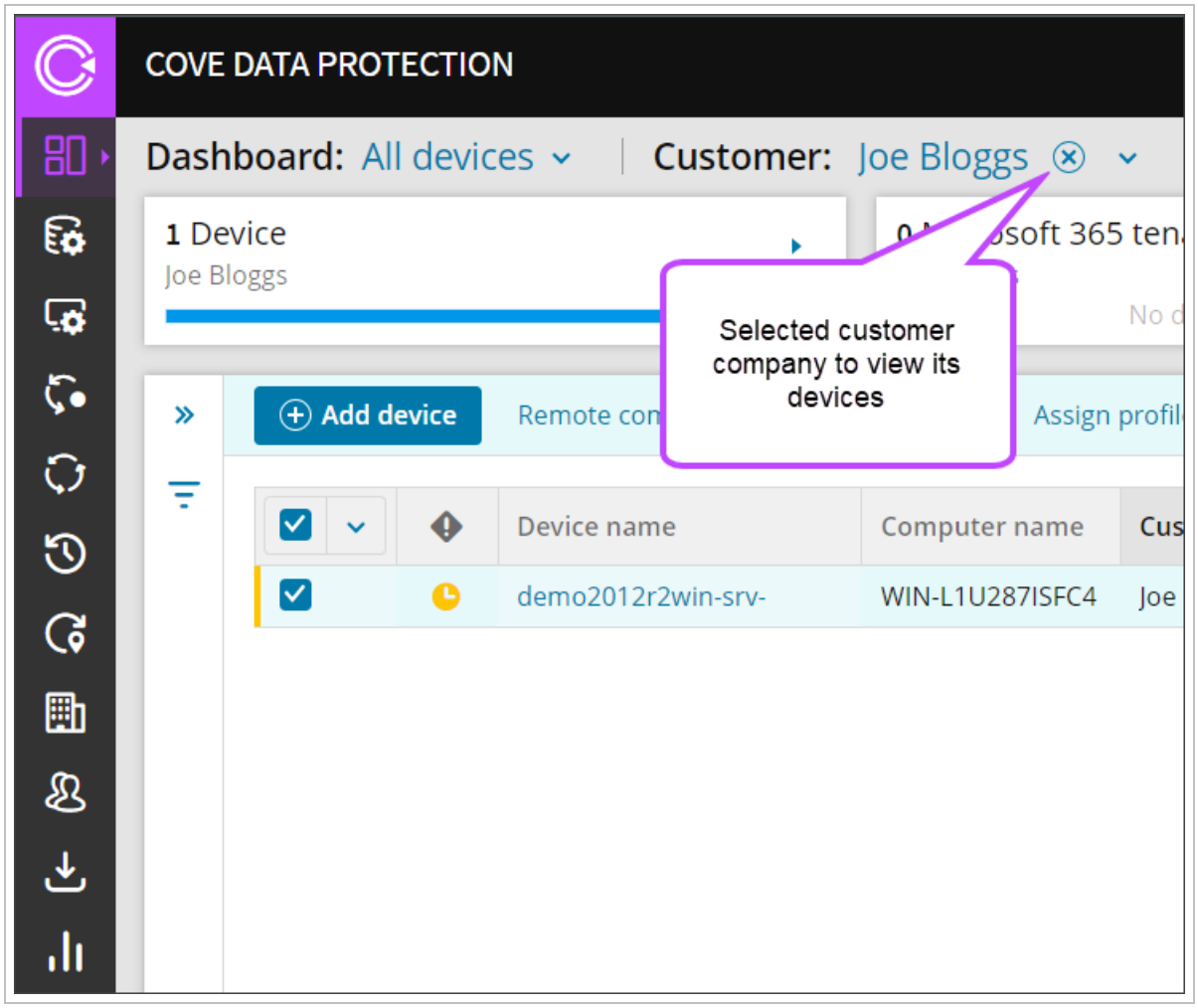
A customer in the Management Console is a general term for a company that provides, sells or consumes Cove Data Protection (Cove)'s backup services.

- If you are a service provider, customers are your **clients**
- If you are a system administrator, customers are **groups or departments** within your own company. Treat customers as a way to organize backup devices and control storage usage

When you open the **Customers** page in the Management Console, you will find your own company at the root level. Your customers are displayed below and all customers listed in the right-hand panel.



To view or manage devices belonging to a certain customer, go to **Backup > Dashboard** and select the customer from the **Customer** list at the top of the page.



Types of customer

Customers are organized in a hierarchy with Distributor at the top level.

Access to some modules in the Management Console is based on the type of customer. See the table below for the details.

Module or feature	Distributor	Sub-distributor	Reseller	End-customer	Site
Quick Installation and generating passphrases (in **Backup > Dashboard**)	Unavailable		Available		Available

<table>
<tr><th>Module or feature</th><th>Distributor</th><th>Sub-distributor</th><th>Reseller</th><th>End-customer</th><th>Site</th></tr>
<tr><td>Profiles</td><td colspan="2" rowspan="8">Available</td><td colspan="2" rowspan="8"></td><td rowspan="3"></td></tr>
<tr><td>Products</td></tr>
<tr><td>Backup > Dashboard (all features except for Quick Installation and generating passphrases)</td></tr>
<tr><td>Customers</td><td>Unavailable</td></tr>
<tr><td>Users</td><td rowspan="4">Available</td></tr>
<tr><td>Downloads</td></tr>
<tr><td>Historical charts</td></tr>
<tr><td>Scheduled Reports</td></tr>
</table>

Access to features within a module may require a certain user account type (learn more).

What's Next?

- Add Customers
- Manage Customers

Add Customers

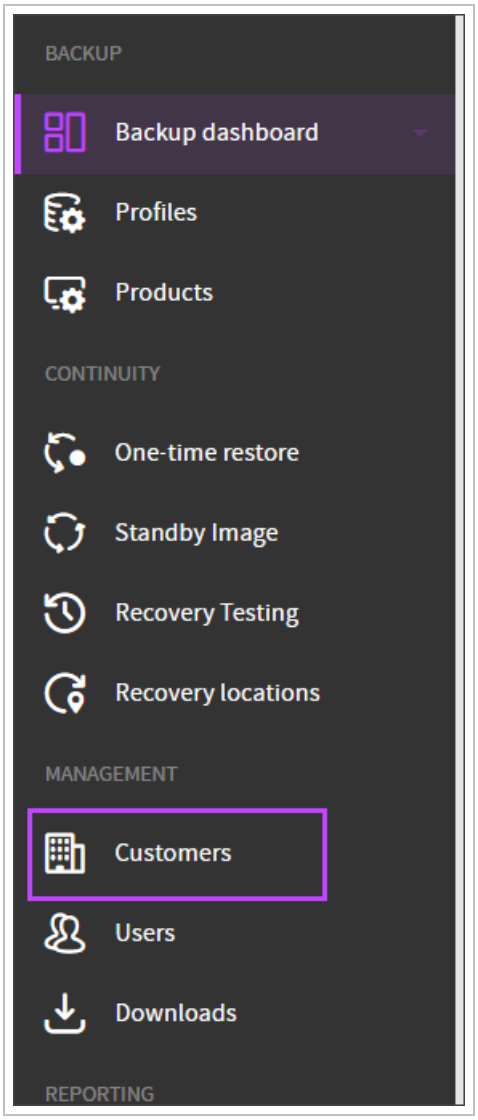
Adding customers differs depending on the customer level.

- See Customer management in Management Console for details on the types of customer
- See Manage Customers for how to edit or delete existing customers

Add a Distributor, Sub-Distributor or Reseller

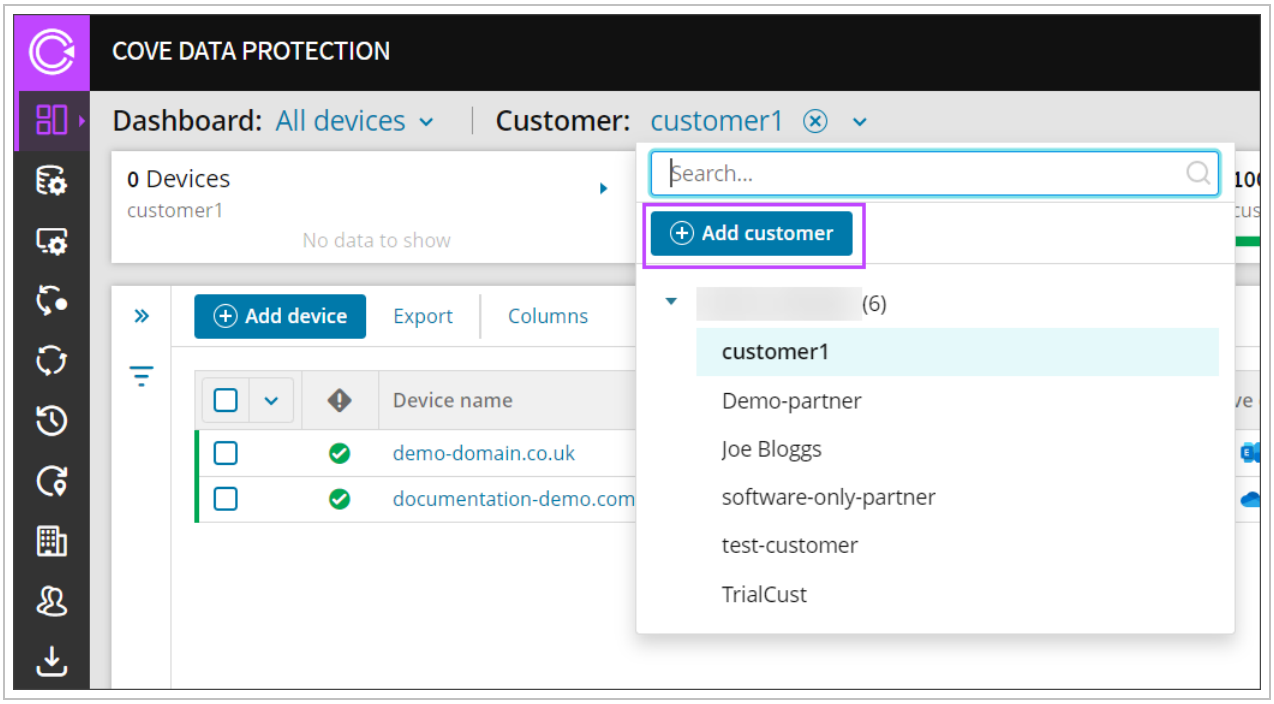
To add a new Distributor, Sub-Distributor or Reseller to the system, do the following:

1. Login to the Management Console
2. Navigate to the **Management** section of the vertical menu and click **Customers**



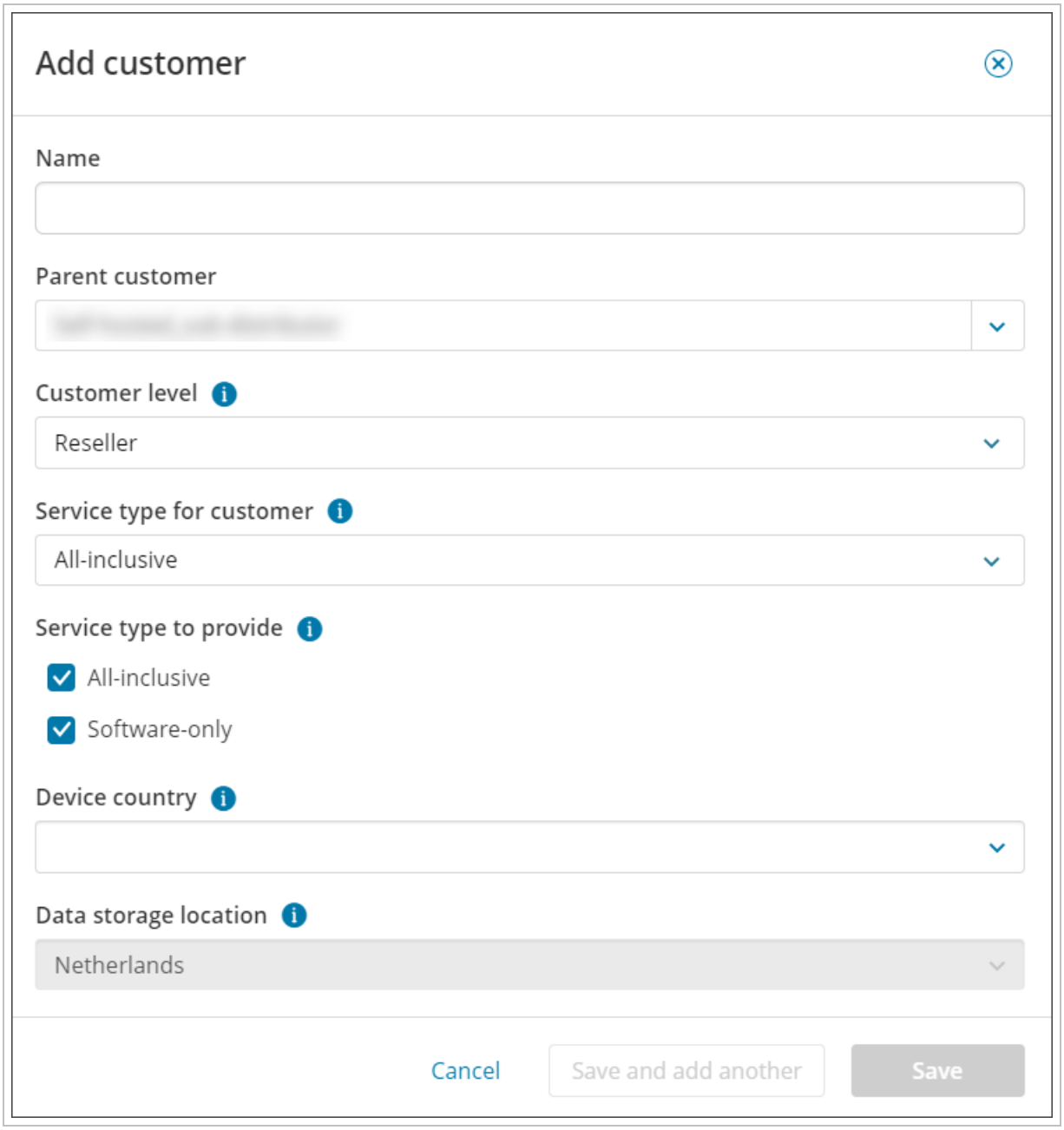
Or

3. From Backup > Dashboard, select the customer dropdown at the top of the page



4. Click **Add customer**

5. Fill out the details for the customer:



- **Name** - The name of the customer as you want it to show on the dashboard
- **Parent customer** - Using the dropdown, select the customer this new one should belong to
- **Customer Level** - Using the dropdown, select the level of customer
- **Service type for customer** - Use the dropdown to select either **All-Inclusive** or **Software-Only**. See our Storage management guide for more information on the service types.

- **Service type to provide** - Use the checkboxes to select which services the new customer will be able to provide to their customers, with a choice of **All-Inclusive** and **Software-Only**. See our Storage management guide for more information on the service types.
- **Device country** - Use the dropdown to select the country the devices will be located
- **Data storage location**[1] - If you have selected a country where we host storage, this will be automatically selected in the Data Storage Location dropdown and you will be unable to change it. However, if you have selected a country where we do not have storage, use the dropdown to select your preferred storage location
  - The following data center locations are available, and are subject to change without notice:

Australia	Belgium	Brazil	Canada	Denmark	France
Germany	Italy	Netherlands	Norway	Portugal	South Africa
Spain	Sweden	Switzerland	United Kingdom	United States	

6. Click **Save**

> You must assign the country **at the time of customer creation**. Changing the country for existing customers has no influence on the storage location.

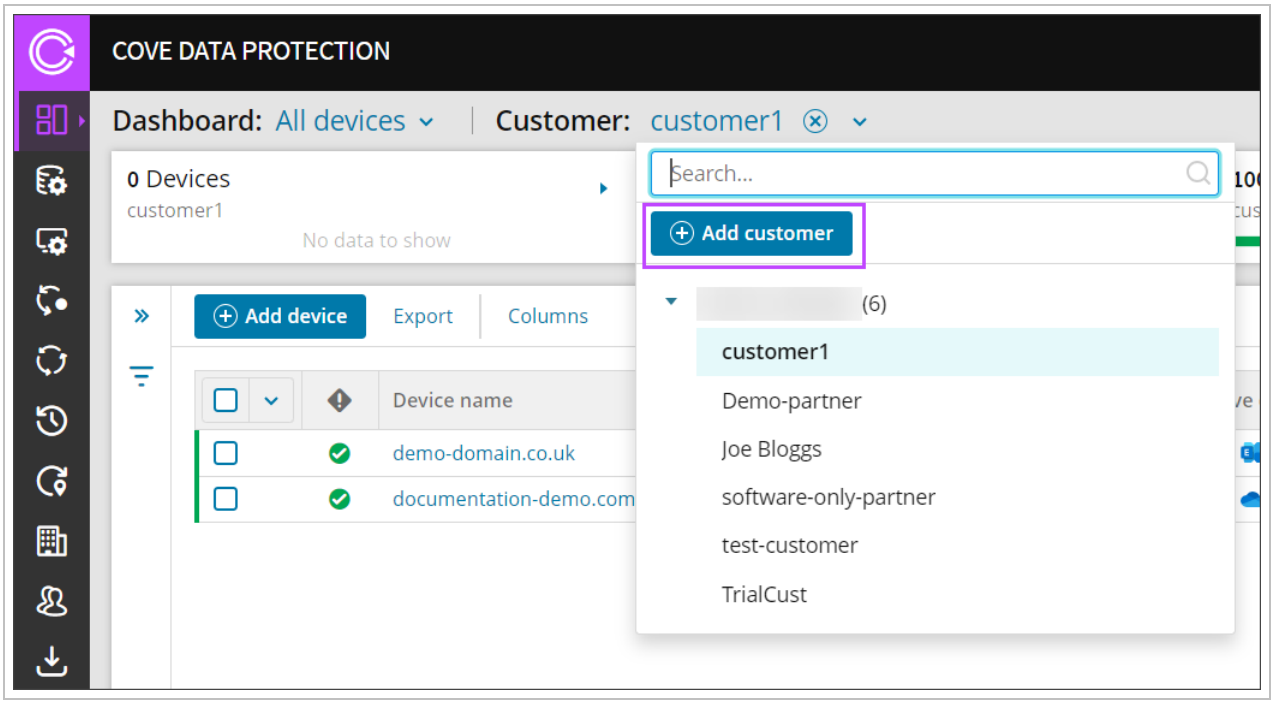
> Once the **storage location** has been selected, you will not be able to change this yourself and must contact support if you wish to change this.

Adding End-Customer or Site

To add a new End-Customer to the system, they must be added as a child to a Reseller or to add Site to the system, they must be added as a child to an End-Customer.

1. In the Management section of Management Console's vertical menu, click **Customers** to open the **customer Management** window or from Backup > Dashboard, select the customer dropdown at the top of the page

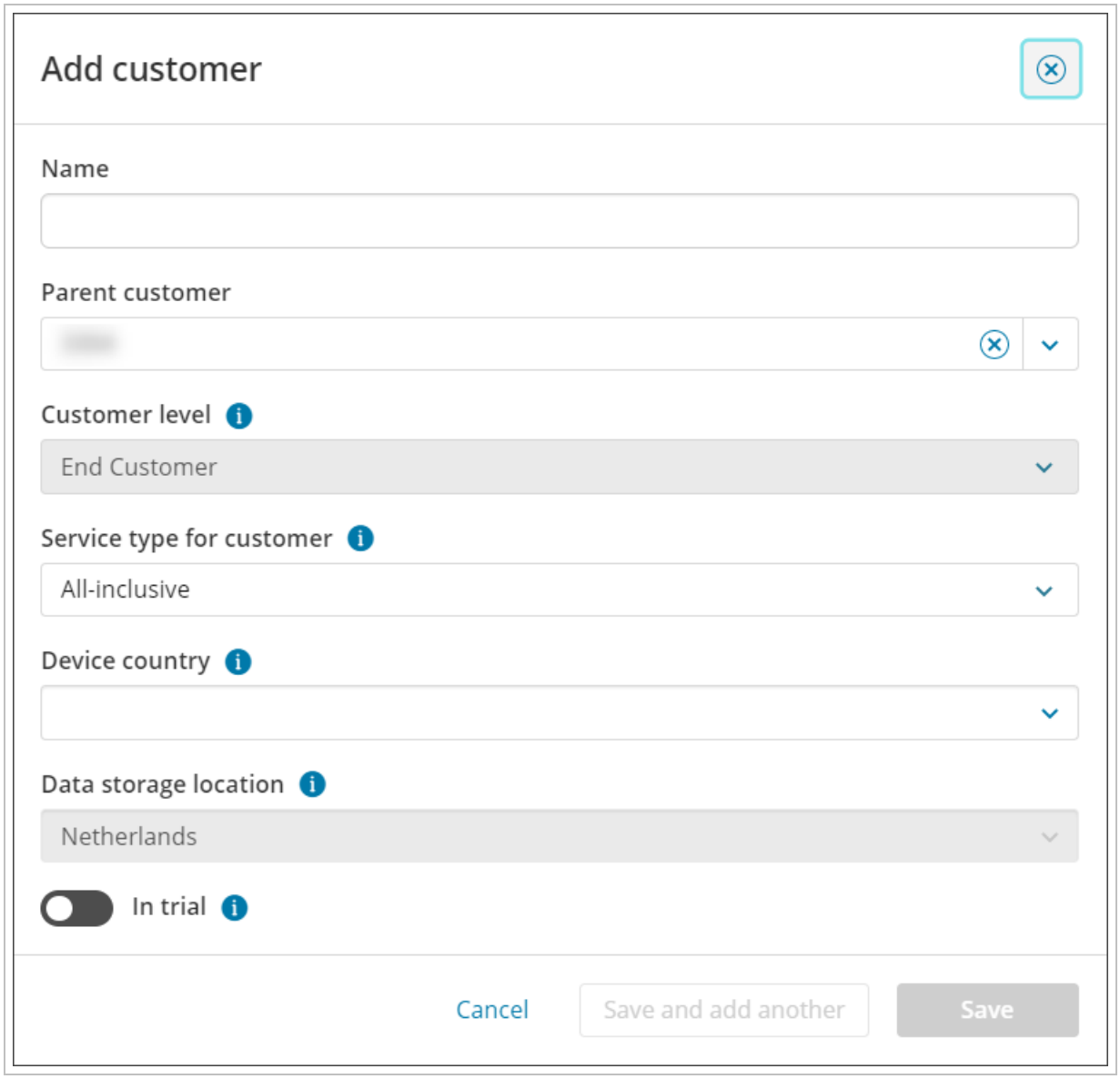
[1] The region where a customer's backup data is stored.



2. Ensure you are in the Reseller or End-Customer you wish the End-Customer or Site should be in
3. Click **Add customer**

4. Add the details for the:

a. End-Customer:



- **Name** - Provide an easily identifiable name for the End-Customer
- **Parent customer** - Using the dropdown, select the Reseller the End-Customer should belong to
- **Customer Level** - This will automatically be set to End customer and cannot be changed
- **Service type for customer** - Use the dropdown to select either **All-Inclusive** or **Software-Only**. See our Storage management guide for more information on the service types.
- **Device Country** - Using the dropdown, select the country the Site is based in

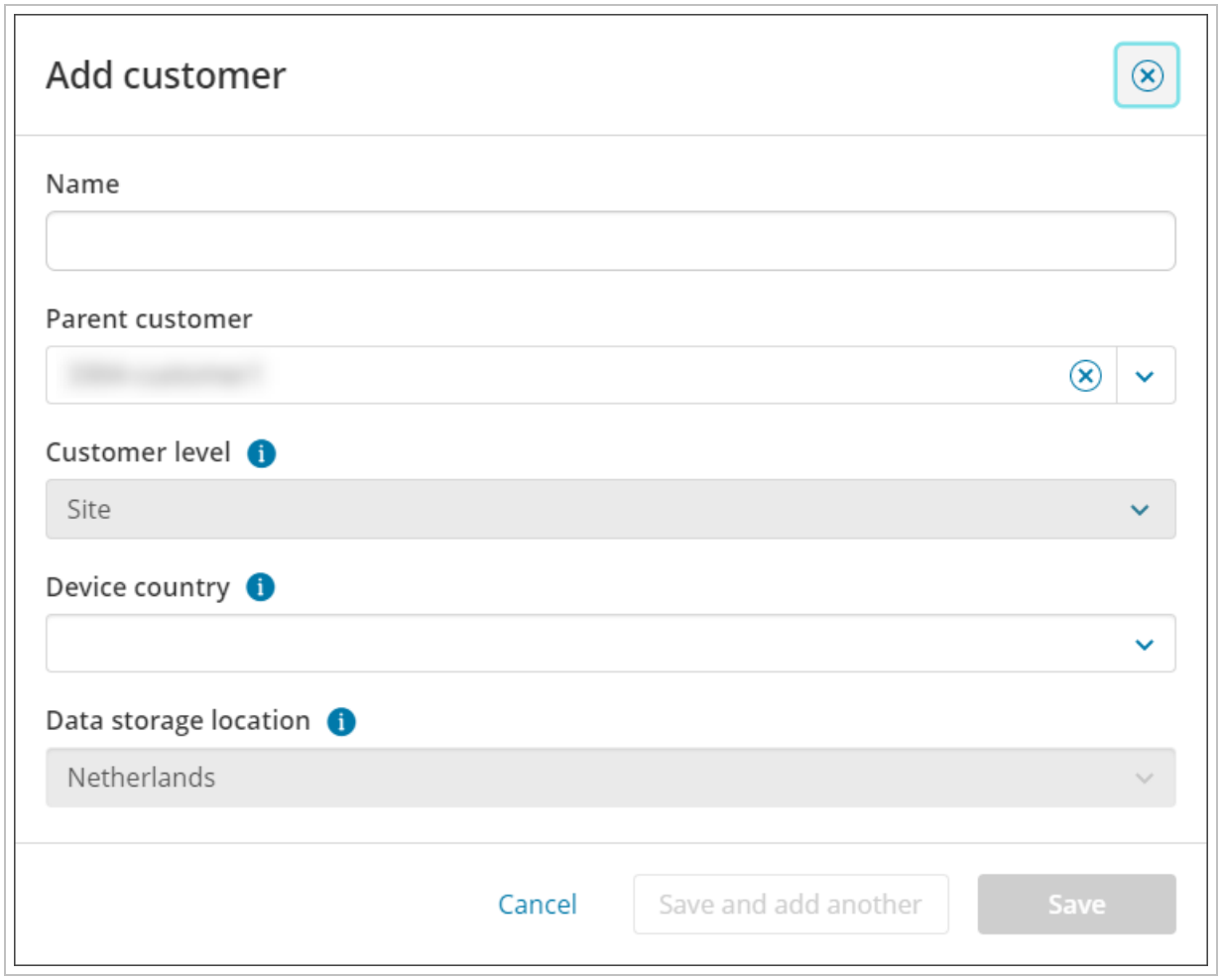
- **Data storage location**[1] - If you have selected a country where we host storage, this will be automatically selected in the Data Storage Location dropdown and you will be unable to change it. However, if you have selected a country where we do not have storage, use the dropdown to select your preferred storage location
  - The following data center locations are available, and are subject to change without notice:

Australia	Belgium	Brazil	Canada	Denmark	France
Germany	Italy	Netherlands	Norway	Portugal	South Africa
Spain	Sweden	Switzerland	United Kingdom	United States	

- **In trial** - If selected, the customer will be added as a trial for 30 days and will not be invoiced during this period. The customer will automatically go into Production when the trial is over.

[1] The region where a customer's backup data is stored.

b. Site:



- **Name** - Provide an easily identifiable name for the Site
- **Parent customer** - Using the dropdown, select the End-Customer the Site should belong to
- **Customer Level** - This will automatically be set to Site and cannot be changed
- **Device Country** - Using the dropdown, select the country the Site is based in

- **Data storage location**[1] - If you have selected a country where we host storage, this will be automatically selected in the Data Storage Location dropdown and you will be unable to change it. However, if you have selected a country where we do not have storage, use the dropdown to select your preferred storage location
  - The following data center locations are available, and are subject to change without notice:

Australia	Belgium	Brazil	Canada	Denmark	France
Germany	Italy	Netherlands	Norway	Portugal	South Africa
Spain	Sweden	Switzerland	United Kingdom	United States	

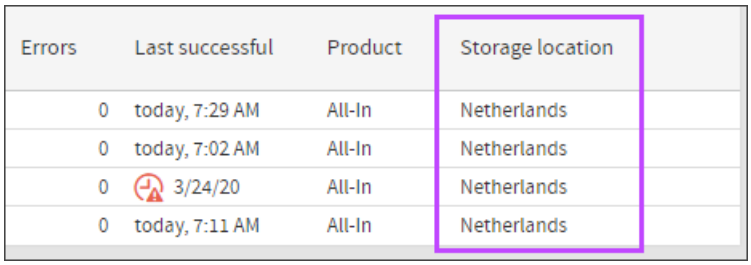
5. Click **Save**

After customer is Added

Further steps you can take:

- Give the customer **access to the Console**. For this purpose you need to create user accounts for people (or teams) from the customer company. You can create all necessary accounts yourself or create one administrator account and let in-house administrators create the rest
- Give the customer **access to the backup and recovery service**. You need devices for this purpose. You may add these yourself or an administrator from the customer company can do this through **Backup > Dashboard**

To make sure the customer has the desired storage location assigned, add a test device for this customer and check the country in the **Storage location** column. If you do not see the column, you will need to add it to the view (more on view management).



Errors	Last successful	Product	Storage location
0	today, 7:29 AM	All-In	Netherlands
0	today, 7:02 AM	All-In	Netherlands
0	3/24/20	All-In	Netherlands
0	today, 7:11 AM	All-In	Netherlands

> Local data centers are not available for every country, so your selection could route your data to a different region. Consult your dedicated account manager for the current listing of regional data centers. New data center availability and the associated routing are subject to change without notice.

Manage Customers

Customer management allows users to update or remove existing customers.

- See Customer management in Management Console for details on the types of customer
- See Add Customers for how to add a new customers

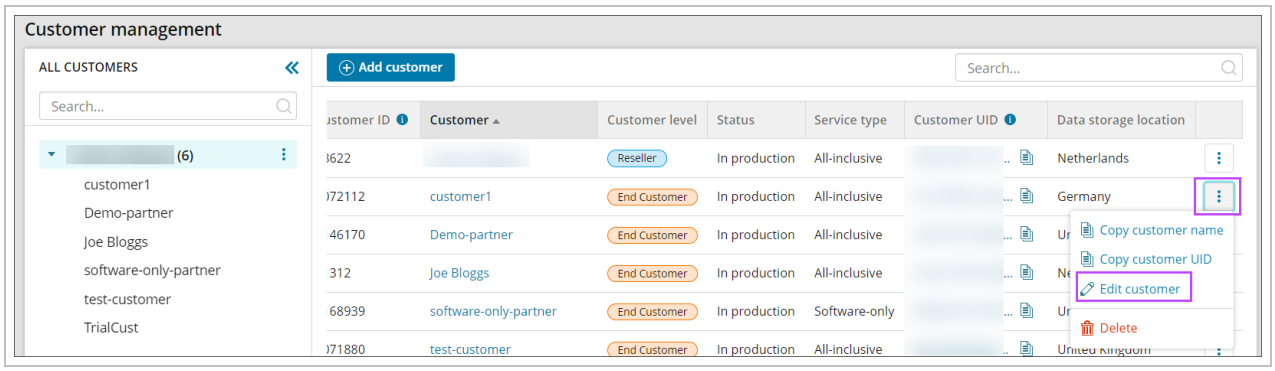
---

[1] The region where a customer's backup data is stored.

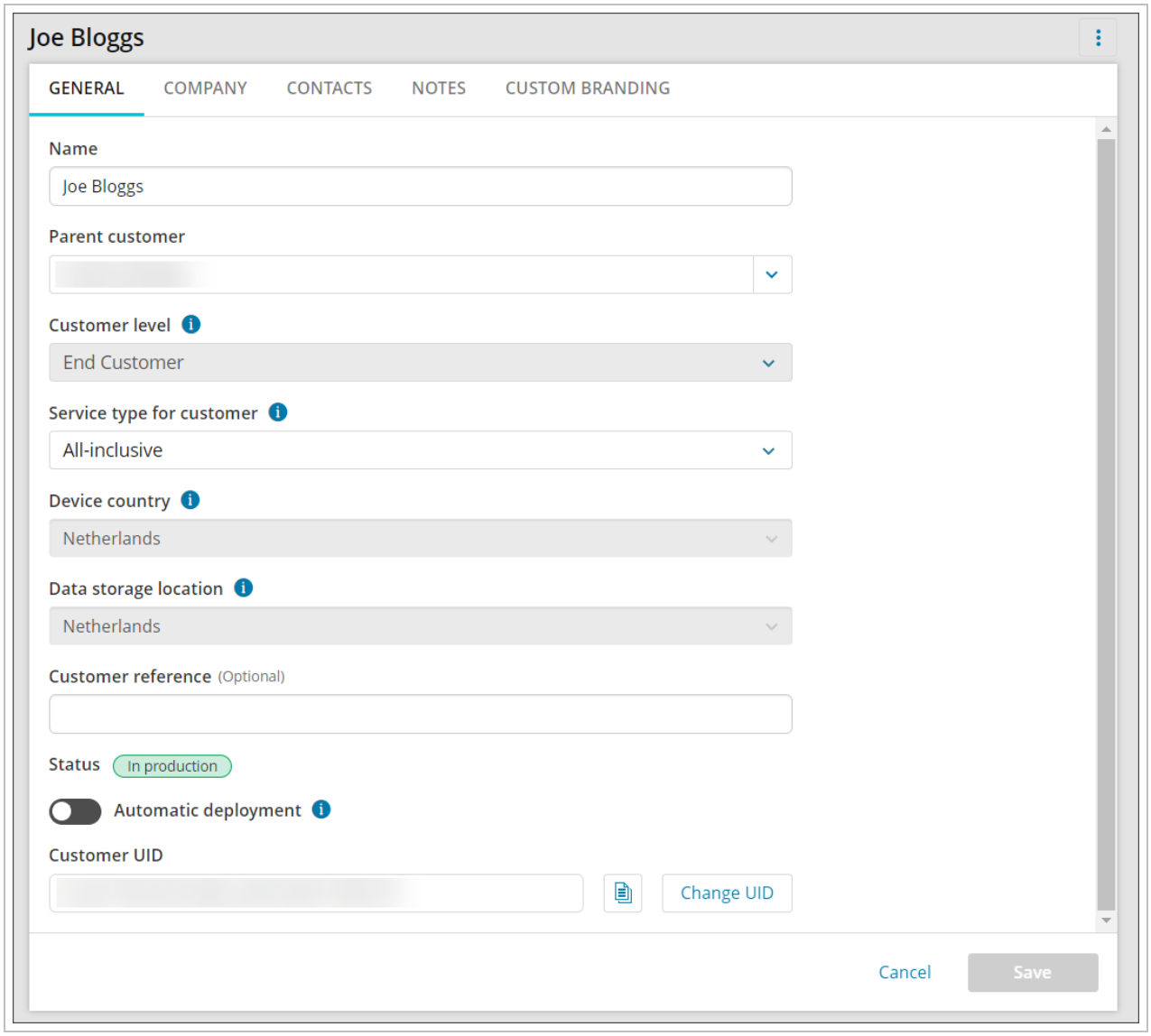
Editing customers

To access customer editing options, this must be done from the Customer Management window:

1. Log on to the Management Console
2. In the Management section of the vertical menu, click **Customers** to open the **customer Management** window
3. Find the name of the customer to edit
4. Scroll to the right of the Customer and click the three vertical dots to open the action menu



5. Click **Edit customer**
6. Make any changes as detailed below
7. Click **Save**



You can change the settings that you configured when creating the customer and access additional settings on the numerous tabs:

General

- **Name** - You may rename the Customer, but please keep in mind that customer names are sometimes required for authorization. So users from the customer company will need to update their access credentials for the Cloud
- **Parent Customer** - Move the Customer to a different parent Customer
- **Customer Level** - Change the customer to a different customer level
- **Service type for customer** - Use the dropdown to select either **All-Inclusive** or **Software-Only**. See our Storage management guide for more information on the service types.

- **Service type to provide** - Use the checkboxes to select which services the new customer will be able to provide to their customers, with a choice of **All-Inclusive** and **Software-Only**. See our Storage management guide for more information on the service types.
- **Customer Reference** - Add additional information to identify the Customer
- **Automatic Deployment** - Enable or disable Automatic Deployment for devices under this partner
    - This feature allows unattended installation of the Backup Manager through the command line on Windows device. For full information see Enable Automatic Deployment in Management Console

Company

All fields in this tab are optional:

- Legal Name
- Website
- Country
- State
- Address
- Zip Code
- City
- District
- Phone number
- Fax number
- Camber of commerce #
- Vat #
- Bank Account #

Contacts

All fields in this tab are optional. Click **Add Contact** to add the names of people to contact and their details:

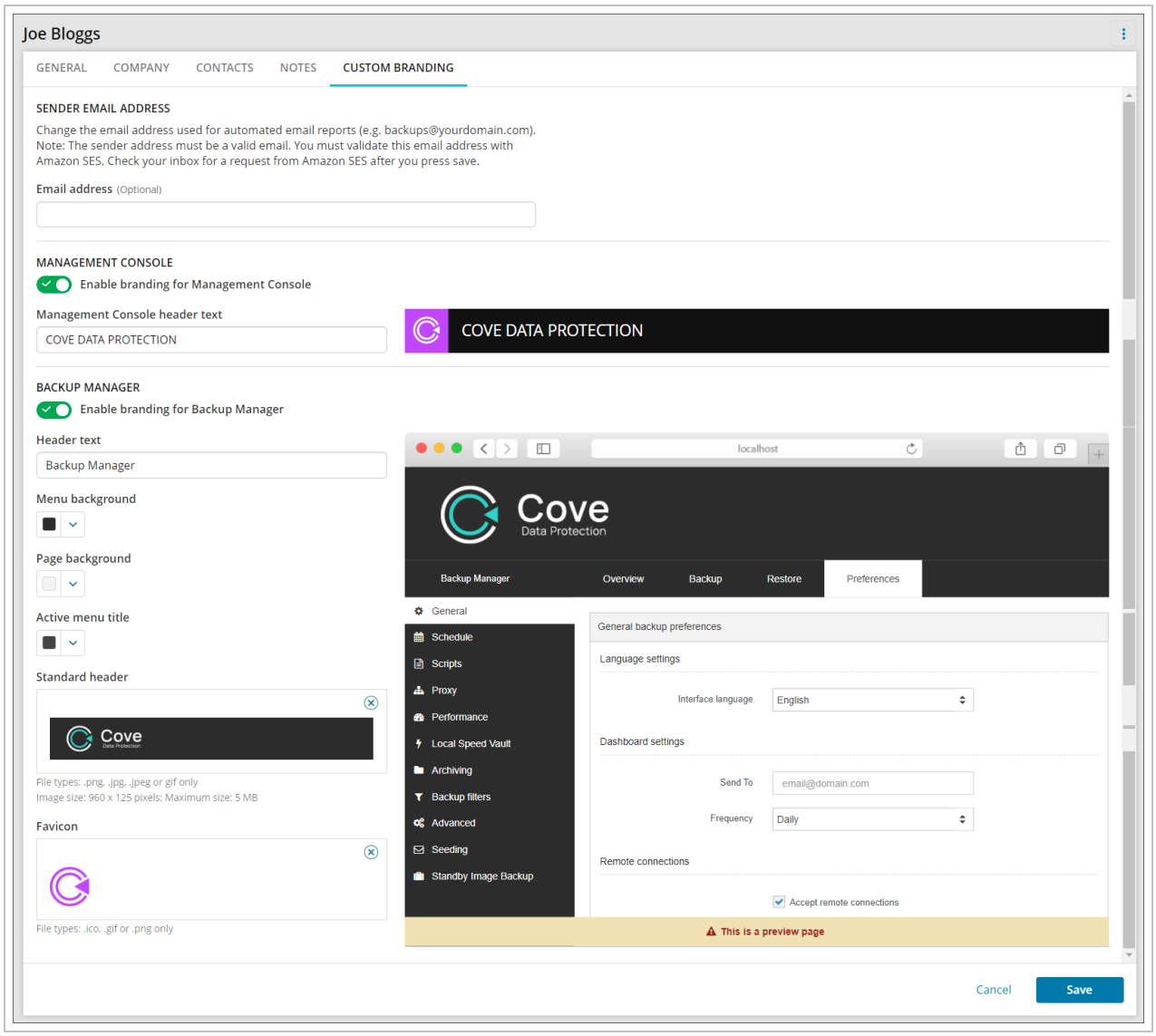
- Title
- First Name
- Last Name
- Position
- Email
- Phone Number
- Type:
    - Authorized signer
    - Administrative
    - Technical
    - Sales

Notes

Notes can only be added once a contact is created. Click **Add Note** to register past and upcoming communication activities, or relevant information regarding the Customer:

- Contact
- Type:
  - Phone
  - Email
  - Personal contact
  - Instant messenger
  - Contactless
- Status:
  - Planned
  - Done
- Date and Time
- Details

Custom Branding



- **Sender Email Address** - Change the email address used for scheduled reports (e.g. backup-reports@yourdomain.com). The default address is backup@n-able.com

  > Be aware if you use a custom sender address you will will need to verify the address by clicking on a verification link that arrives in the configured email address's inbox. If this does not happen then you will not receive any backup related emails (Let's get started, Backup daily Dashboards, reports, email views etc.).

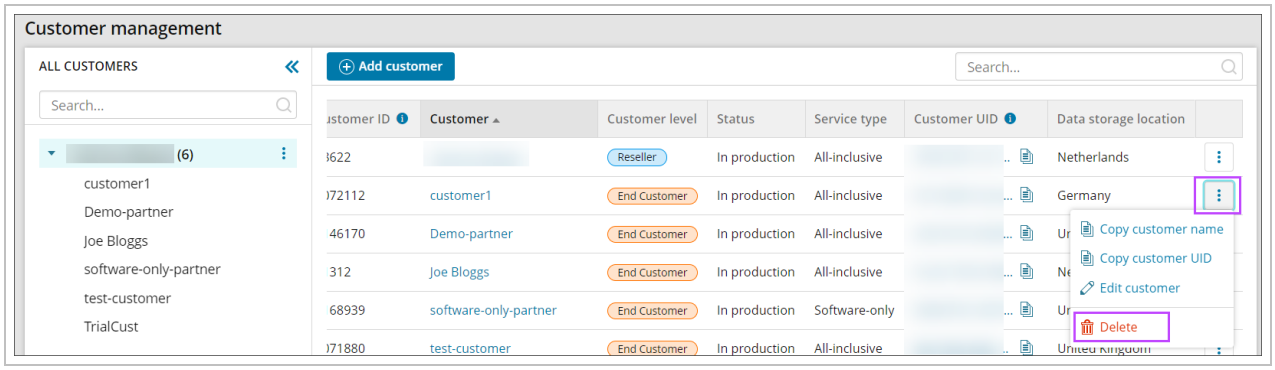
- **Enable Branding for Management Console** - Once enabled, the following additional option is given:
  - **Management Console header text** - this allows you to change the text shown in the header of the Management Console from the default of **Cove Data Protection** to something different in line with your custom branding

- **Enable branding for Backup Manager** - Once enabled, the following additional options are given:
  - **Header Text** - This allows you to change the text shown in the header of the Backup Manager tool from the default of **Backup Manager** to something different in line with your custom branding
  - **Menu Background** - use the colour picker, RGB, HSL or Hex code to select a colour matching your branding
  - **Page Background** - use the colour picker, RGB, HSL or Hex code to select a colour matching your branding
  - **Active Menu Title** - use the colour picker, RGB, HSL or Hex codes to select a colour matching your branding
  - **Standard Header** - remove the default Cove header image and drop or browse to add a custom header image
  - **Favicon** - remove the default Cove favicon image and drop or browse to add a custom favicon image

Delete customers

You can remove only those customers that do not have any devices or customers of their own, or with any recovery locations assigned to them. This must be done from the Customer Management window:

1. Log on to the Management Console
2. In the **Management** section of the vertical menu, click **Customers** to open the **customer Management** window
3. Find the name of the customer to remove
4. Scroll to the right of the Customer and click the three vertical dots to open the action menu



5. Click **Delete**
6. Confirm your intention to delete the customer

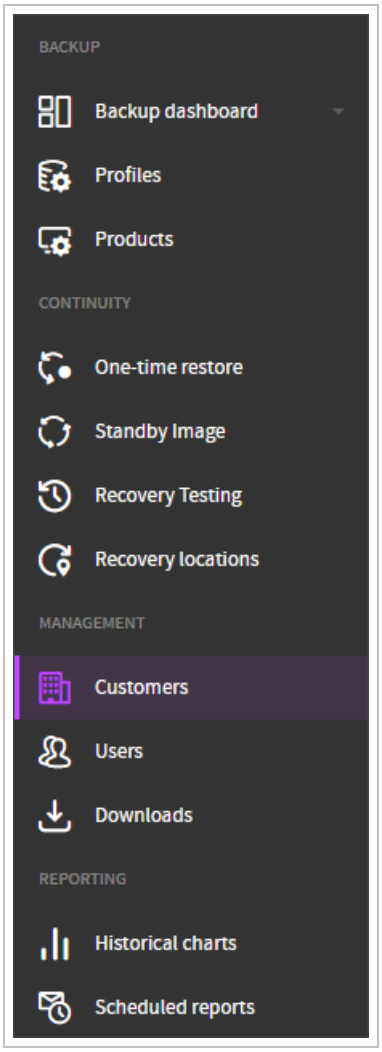
Enable Automatic Deployment in Management Console

This feature allows installation of the Backup Manager by automatic deployment. All that is required is to download the Backup Manager Installation package with the your customer UID and begin the installation on the system you wish to back up.

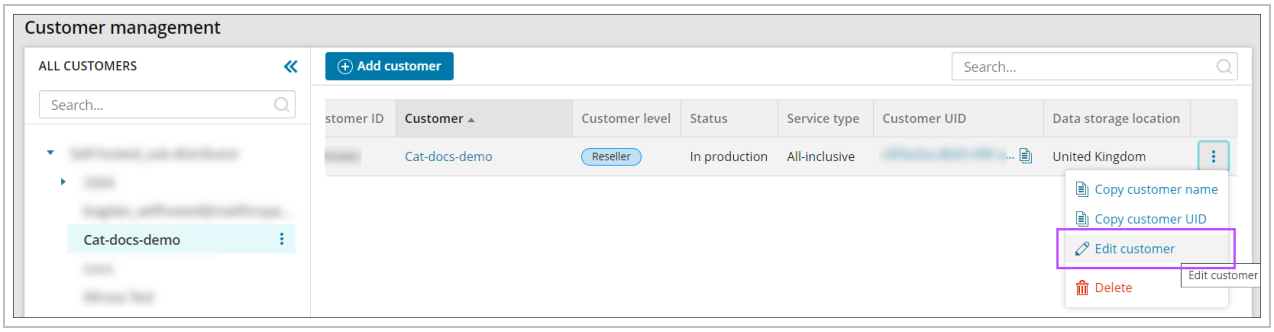
> The installation package can be used on multiple devices without the need to add a new device in the Management Console and downloading the installation files each time.

> Do **NOT** rename the installation package.

1. Log in to the Management Console
2. In the Management section of the vertical menu, click **Customers** to open the **Customer Management** window

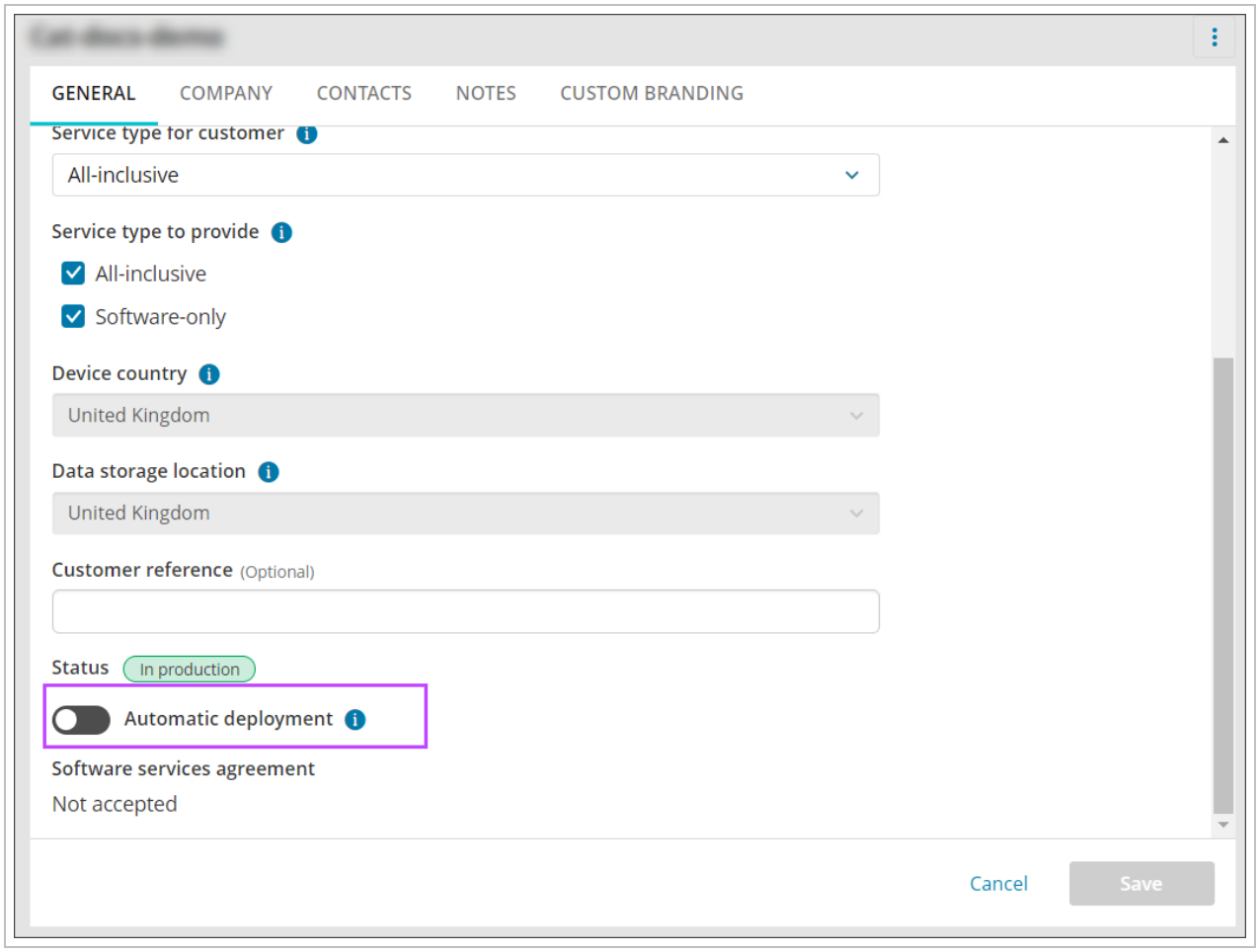


3. Find the Customer to edit
4. Scroll to the right of the Customer and click the three vertical dots to open the action menu



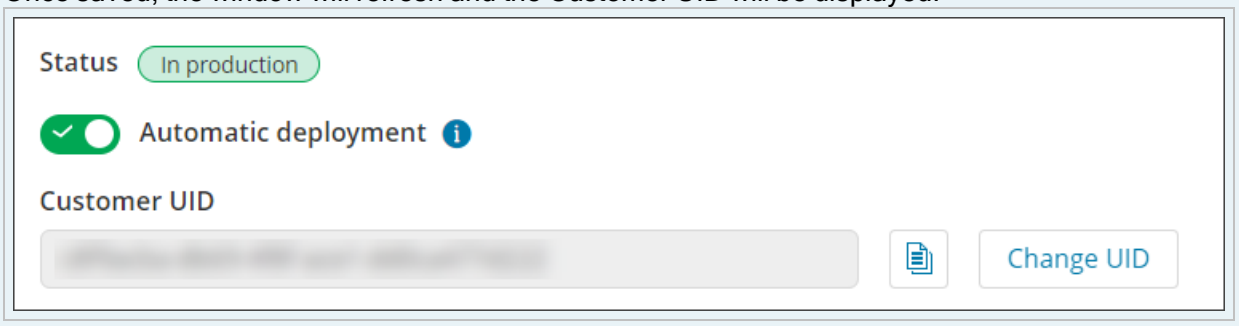
5. In the **Edit customer** window, select the **General** tab

6. Place a tick in the **Automatic Deployment** box



7. Click **Save**

Once saved, the window will refresh and the Customer UID will be displayed:



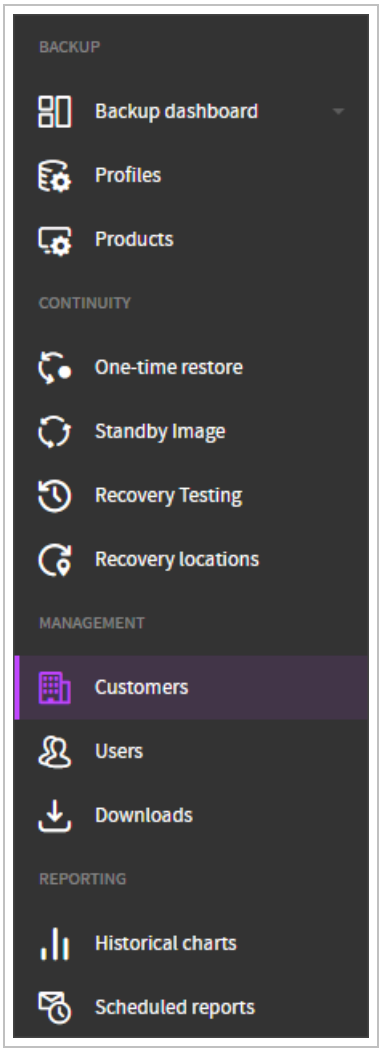
Customer UID

A Customer UID is a unique 36 character identifier generated for each partner when Automatic Deployment is enabled, which is required for authorization of the installation of Backup Manager.

Automatic Deployment must be enabled to be able to see and change the Customer UID. See Enable Automatic Deployment in Management Console for full details.

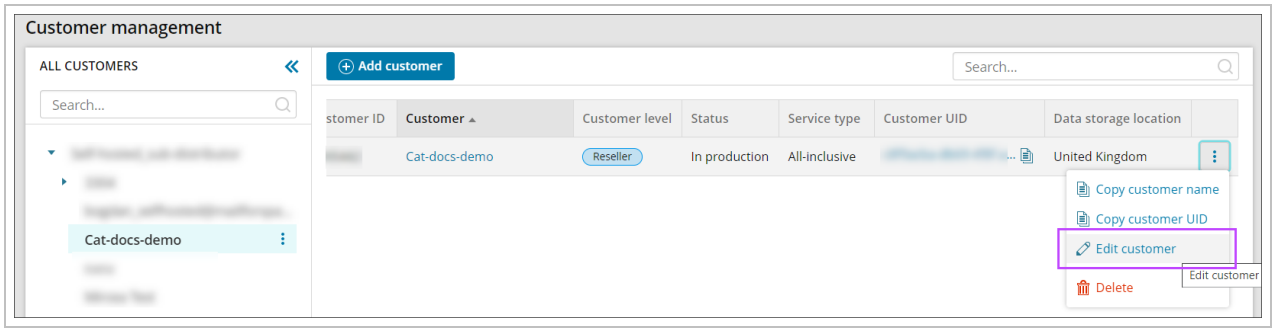
Find the Customer UID

1. Log in to the Management Console
2. In the Management section of the vertical menu, click **Customers** to open the **Customer Management** window

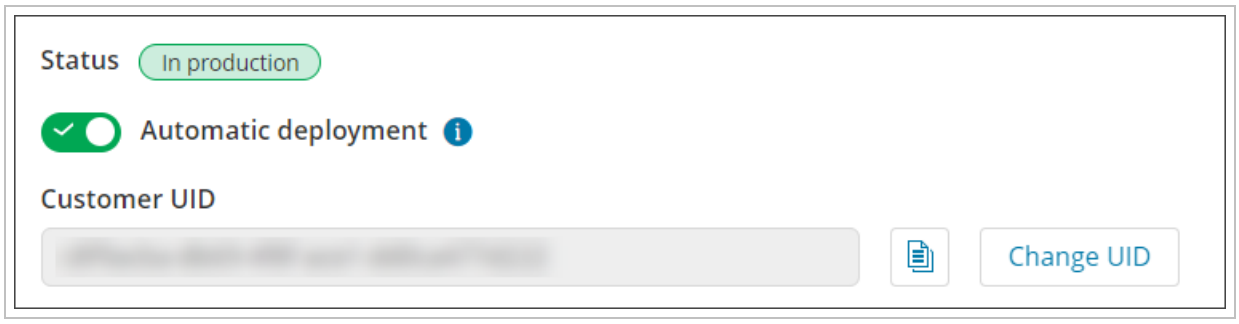


3. Find the partner in question

4. Scroll to the right of the Customer and click the three vertical dots to open the action menu and either:
   a. Click **Edit customer**

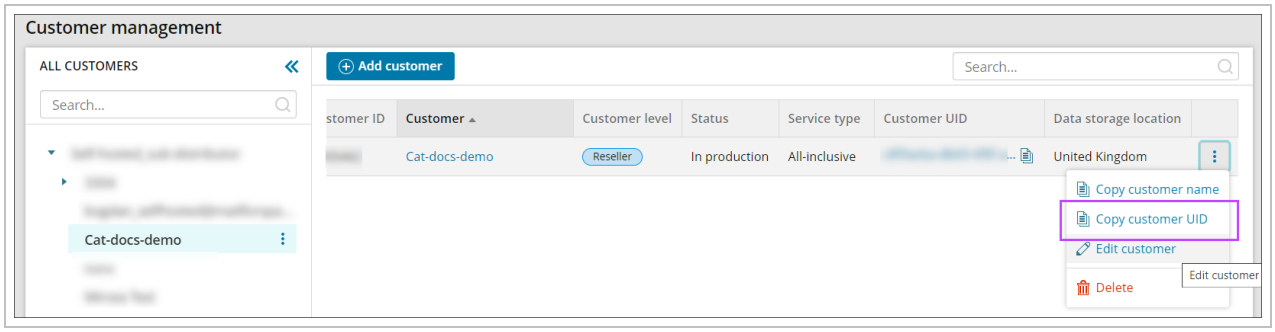


   b. Select the **General** tab, scroll until you see the Customer UID field:



or

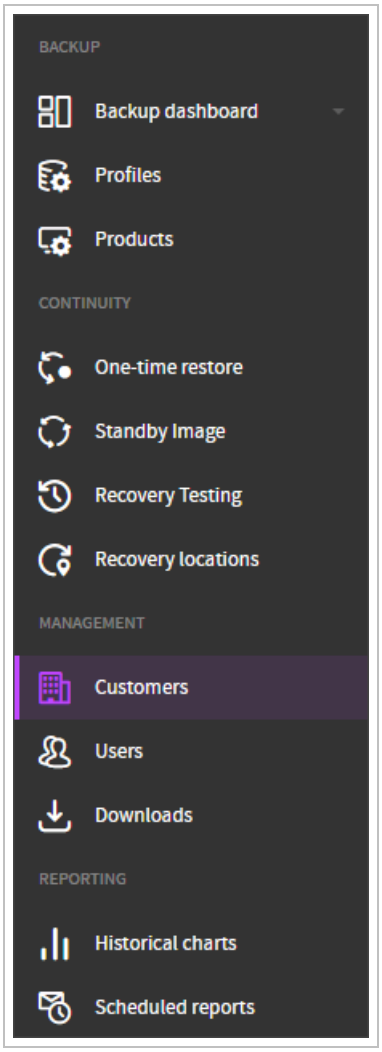
   a. Click **Copy Customer UID**



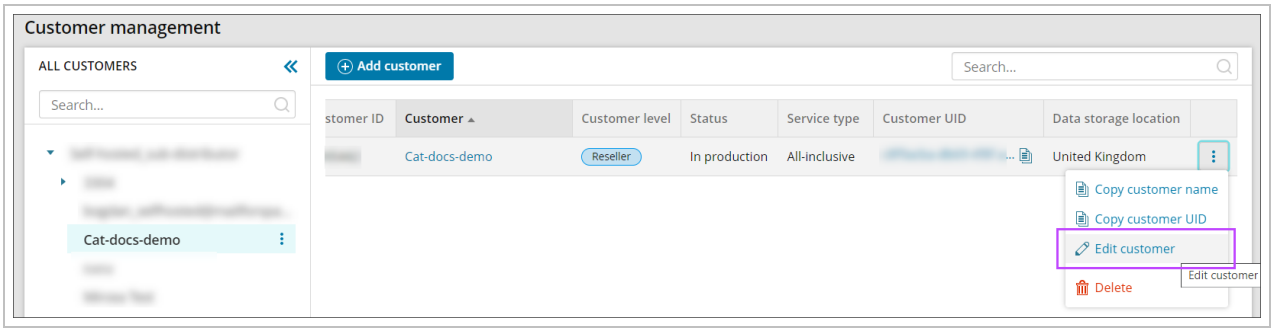
Change the Customer UID

Customer UID's can be changed as often as necessary. Doing so will not affect any of the previous installations.

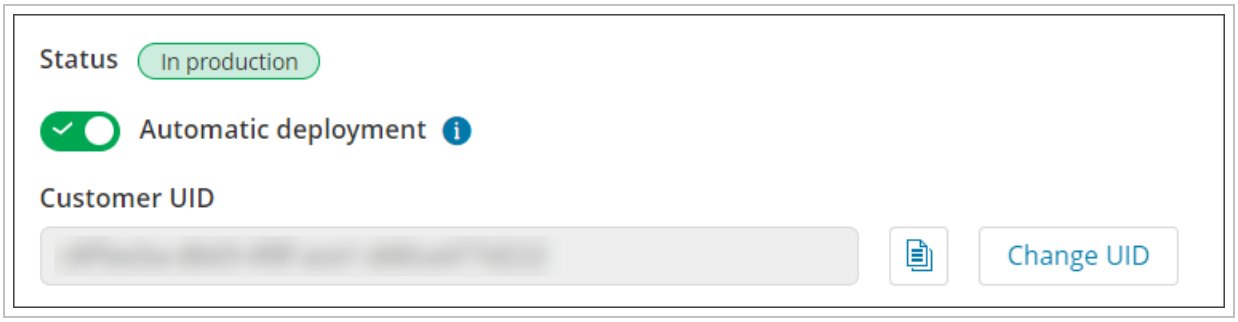
1. Log in to the Management Console
2. In the Management section of the vertical menu, click **Customers** to open the **Customer Management** window



3. Find the partner in question
4. Scroll to the right of the Customer and click the three vertical dots to open the action menu
5. Click **Edit customer**



6. Select the **General** tab, scroll until you see the Customer UID field:



7. Click **Change UID**
8. Confirm you want to change the Customer UID by clicking **Yes**

> The ID will now update to a new 36 character string

> Once the Customer UID has been changed, you will need to update the installation package name of any instances where this has been downloaded but not yet ran, to include the new UID and remove the old one.

User management in Management Console

Users (or user accounts) are required for access to the Console and other Cloud services.

- There are several **user roles** to choose from. They make it possible to **differentiate access** to data and features within a company.
- Customers can have an unlimited **number** of users.

User roles

The following user roles are available:

- SuperUser
- Administrator
- Manager
- Operator
- Supporter

Security Officer is an additional setting which can be applied to certain roles to provide additional access to generate a passphrase:

- SuperUser
- Administrator
- Manager
- Operator

Key

The following icons indicate availability:

Key	Status	Description
✅	Available	Is available for *all*
⚠	Limited Availability	Is available for with limitations (see **Note** for additional information)
⚠	Read Only	Is available in read only mode
⛔	Not Available	Is **not** available

Please see the table below for access permissions available to each of the roles.

Task	SuperUse	SuperUs	Administra	Administra	Manager	Manag	Operator	Operat	Supporter p
Automatic Deployment[1]	✅	✅	⛔	⛔	⛔	⛔	⛔	⛔	⛔
Export of monthly device statistics	✅	✅	✅	✅	✅	✅	✅	✅	✅
Generating passphrases[2]	✅	⛔	✅	⛔	✅	⛔	✅	⛔	⛔
Launching backup devices remotely	✅	✅	✅	✅	✅	✅	✅	✅	⛔
Recovering data in Backup Manager	✅	✅	✅	✅	✅	✅	✅	✅	⛔

[1]This feature is available to resellers and end-customers. It is used by the **Quick Installation** method.

[2]Passphrases are used instead of security codes during the re-installation of automatically deployed devices, for the cleanup of backup data sources and for the addition of devices to the Recovery Console.

Task	SuperUse	SuperUs	Administra	Administra	Manager	Manag	Operator	Operat	Supporter p
Recovering data in Recovery Console	✅	⚠ (Note)[1]	✅	⚠ (Note)[2]	✅	⚠ (Note)[3]	✅	⚠ (Note)[4]	⛔
Recovery Testing	✅	⚠ (Note)[5]	⚠	⚠	✅	⚠ (Note)[6]	⚠	⚠	⚠
StandBy Image	✅	⚠ (Note)[7]	⚠	⚠	✅	⚠ (Note)[8]	⚠	⚠	⚠
Recovery Locations	✅	✅	⚠	⚠	⚠	⚠	⚠	⚠	⚠
Managing backup	✅	✅	✅	✅	⚠	⚠	⚠	⚠	⛔

---

[1]If the device uses Passphrase-based encryption, this user level does not have access to generate these and so will not be able to add the device to the Recovery Console. If the device uses a Security code/Encryption key, this user level will be able to proceed with the recovery via Recovery Console.
[2]If the device uses Passphrase-based encryption, this user level does not have access to generate these and so will not be able to add the device to the Recovery Console. If the device uses a Security code/Encryption key, this user level will be able to proceed with the recovery via Recovery Console.
[3]If the device uses Passphrase-based encryption, this user level does not have access to generate these and so will not be able to add the device to the Recovery Console. If the device uses a Security code/Encryption key, this user level will be able to proceed with the recovery via Recovery Console.
[4]If the device uses Passphrase-based encryption, this user level does not have access to generate these and so will not be able to add the device to the Recovery Console. If the device uses a Security code/Encryption key, this user level will be able to proceed with the recovery via Recovery Console.
[5]If the device uses Passphrase-based encryption, this user level does not have access to generate these and so will not be able to add the device to the Recovery Console. If the device uses a Security code/Encryption key, this user level will be able to proceed with the recovery via Recovery Console.
[6]If the device uses Passphrase-based encryption, this user level does not have access to generate these and so will not be able to add the device to the Recovery Console. If the device uses a Security code/Encryption key, this user level will be able to proceed with the recovery via Recovery Console.
[7]If the device uses Passphrase-based encryption, this user level does not have access to generate these and so will not be able to add the device to the Recovery Console. If the device uses a Security code/Encryption key, this user level will be able to proceed with the recovery via Recovery Console.
[8]If the device uses Passphrase-based encryption, this user level does not have access to generate these and so will not be able to add the device to the Recovery Console. If the device uses a Security code/Encryption key, this user level will be able to proceed with the recovery via Recovery Console.

Task	SuperUse	SuperUs	Administra	Administra	Manager	Manag	Operator	Operat	Supporter p
profiles[9]									
Managing contact notes	✅	✅	✅	✅	✅	✅	⚠	⚠	⚠
Managing contacts[2]	✅	✅	✅	✅	⚠	⚠	⚠	⚠	⚠
Managing customers	✅	✅	⚠	⚠	⚠	⚠	⚠	⚠	⚠
Managing devices[3]	✅	✅	⚠	⚠	✅	✅	⚠	⚠	⚠
Managing Microsoft 365 domains	✅	⚠ (Note)[4]	⚠ (Note)[5]	⚠	⚠ (Note)[6]	⚠	⚠ (Note)[7]	⚠	⚠
Managing products	✅	✅	✅	✅	⚠	⚠	⚠	⚠	⛔
Managing security officers[8]	✅	⛔	⛔	⛔	⛔	⛔	⛔	⛔	⛔
Managin-	✅	✅	✅	✅	⚠	⚠	⚠	⚠	⚠

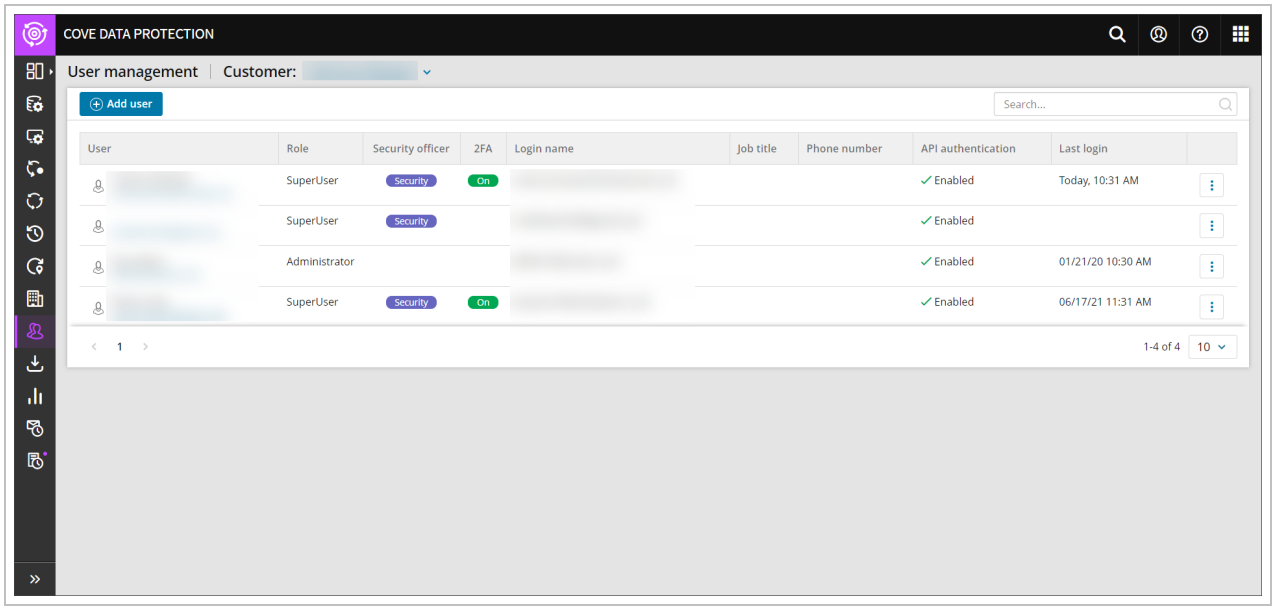
[9]Feature available to resellers and end-customers only
[2]Names of customer representatives and their contact details
[3]All features except for aQuick Installation and generating passphrases
[4]Cannot delete services or delete account/site backup history
[5]Cannot delete services or delete account/site backup history
[6]Cannot delete services or delete account/site backup history
[7]Cannot delete services or delete account/site backup history
[8]Flagging SuperUsers as Security Officers and removing the flag

Task	SuperUse	SuperUs	Administra	Administra	Manager	Manag	Operator	Operat	Supporter p
g users[9]									
Managin-g views	✅	✅	✅	✅	✅	✅	✅	✅	✅
Sending remote com-mands to devices	✅	✅	✅	✅	✅	✅	✅	✅	⛔

Adding users

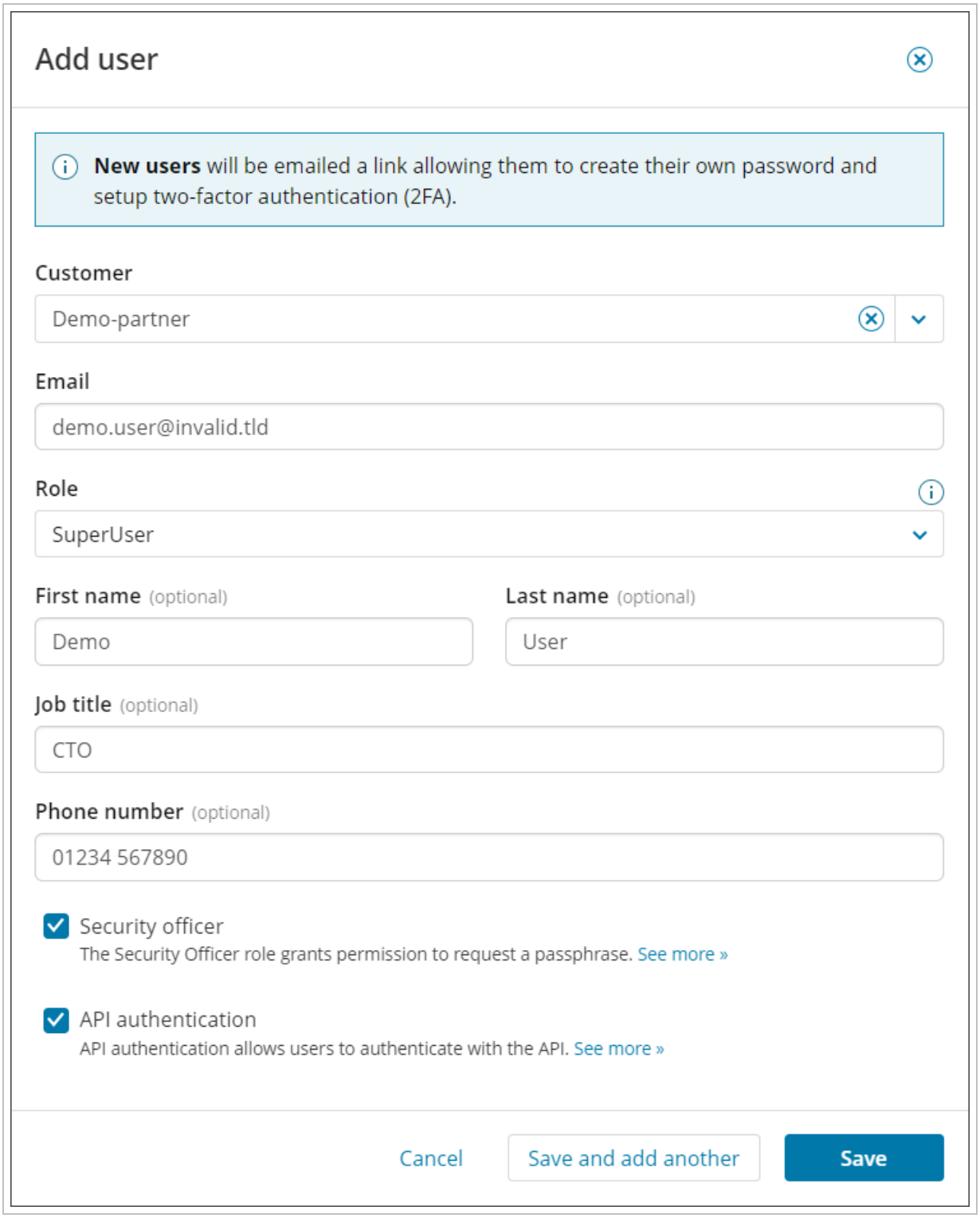
You can add new users for your own company and for your customers. Here are steps to follow:

1. In the vertical menu, click **User management**
2. Click **Add user**



[9] All features except for managing security officers

3. Fill out the fields as fully as you can



4. Ensure that you check **API Authentication** if the user needs to be able to log in to the platform via an API call

> If disabled, the user cannot log in to the platform via API. They will only be have access via the Web portal.

5. Ensure you check Security Officer if the user role if the user needs to be able to generate a passphrase
6. Click **Add** to apply the changes

The owner of the new user account will get an email notification with a password setup link.

Editing users

You can change any of the settings configured for a user except for the log-in name. Here is how to:

1. Click the pen icon next to the name of the user you want to edit
2. Edit the settings as required and click **Save** to apply

> For extra security, users control password management. To change their password the user goes to Login to the Backup Console, selects **Forgot password?** then enters the their email address to **Reset your password**.
>
> Where this email address corresponds to a user in the system, we send an email notification containing a link to reset their password.

> **API Authentication** can be enabled and disabled for users after they have been added through the edit user functionality.

Removing users

Here is how to remove a user from the system:

1. Click the trashcan icon next to the name of the user
2. Confirm your intention to proceed

> After a user is removed, it will not be possible to access the Console with the deleted user account. All people logged in under that account will be logged out within the next 15 minutes.

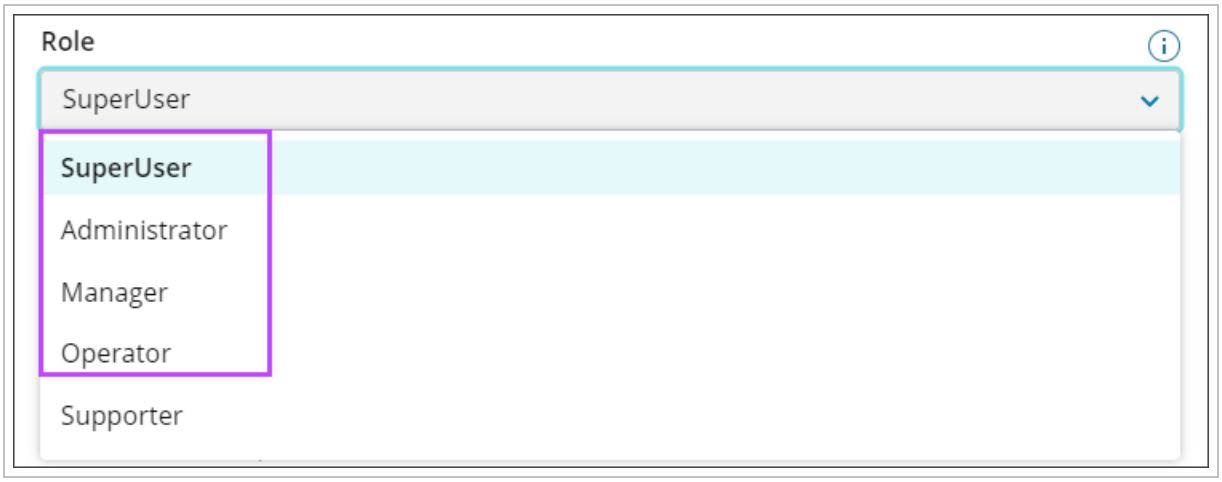
Managing security officers

The first **SuperUser** who logs in to the Console is immediately flagged as a **security officer**. Only security officers can manage other security officers including themselves.

To add a user with the security officer permissions, do the following:

1. Log in to the Management Console as a user with security officer permissions
2. Navigate to the User Management module
3. Click **Add user**

4. Set the user role to **SuperUser, Administrator, Manager** or **Operator**



5. Select the **Security officer** checkbox
6. Click **Add**

You can also grant or remove security officer permissions to existing SuperUsers if necessary (see Edit user dialogue).

> Each customer of the reseller or end-customer level must have **at least 1 security officer**. You cannot delete the last security officer.

Single Sign-On

Users log into the Management Console through a Single Sign-On service.

> Our N-Able Single Sign-On (SSO) service is a convenient way for you to access our SSO products (including Take Control, MSP Manager and N-sight) with a single set of login credentials.
>
> Please be aware that any changes to your SSO credentials, including username and password updates, will apply to **all** of our SSO supporting products *and* the N-AbleMe.

Please visit N-Able Single Sign-On (SSO) in Management Console for further information.

N-Able Single Sign-On (SSO) in Management Console

The Single Sign-On service allows users to access our supported products through a single login.

> Our N-Able Single Sign-On (SSO) service is a convenient way for you to access our SSO products (including Take Control, MSP Manager and N-sight) with a single set of login credentials.
>
> Please be aware that any changes to your SSO credentials, including username and password updates, will apply to **all** of our SSO supporting products *and* the N-AbleMe.

Single Sign-On

After registering the user's credentials with the Single Sign-On service, these are then used to access all our supported products.

Single Sign-On has the following benefits:

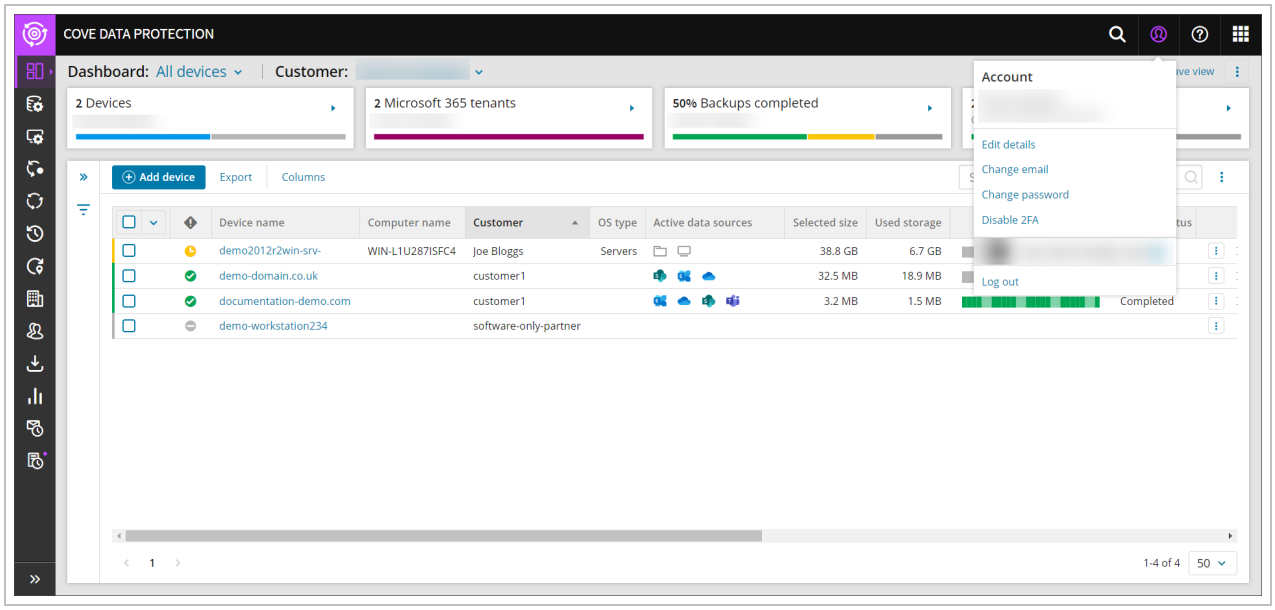
- Provides the user with full control over their login
- Makes logging into multiple products easier
- Improves security - login credentials are only entered once in the service, which leads to reduced exposure of login details
- Makes it easier to apply the company's login policy as there is only one login to manage
- Simplifies switching between products through the Navigator bar
- Increases productivity as users spend less time attempting to login
- Helps reduce administrative burden of dealing with lost credential requests
- Encourages the use of more complex passwords as there is only one login to remember

Single Sign-on utilizes the leading industry standard for cross-platform authentication. All login requests pass through HTTPS using this protocol.

SAML authentication is not currently supported with our Single Sign-On.

Console Update

After migration the Backup Console includes further user options when clicking on the username in the upper right corner. From here the user can change their details, reset their password and enable Two-Factor Authentication.

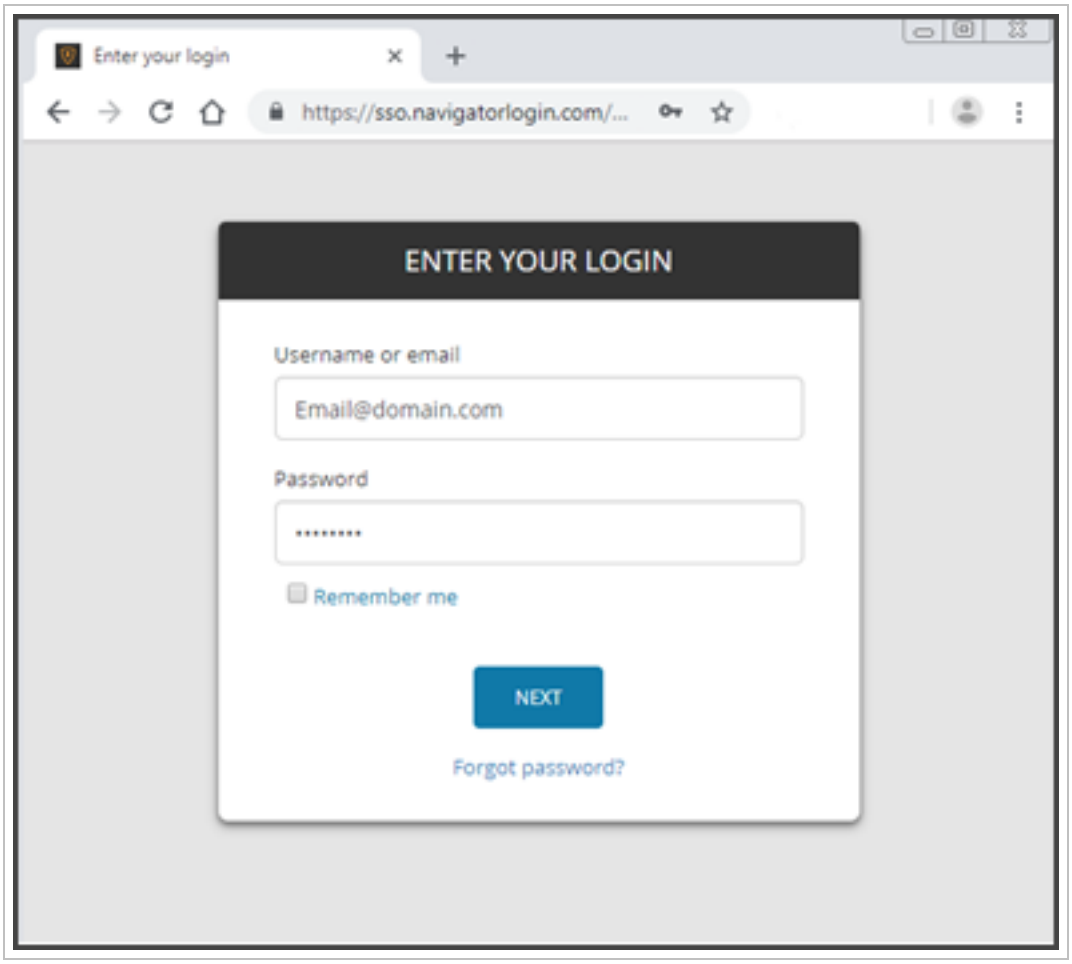


Email Address Credentials

Before the release of Single Sign-On, supported logins used usernames or email addresses.

Once migrated, users need active email address credentials to access the Backup Console.

Where users do not use an email-based login, a prompt will prompt them to correct their credentials and change their username to an email address



Single Sign-On URL Access https://sso.navigatorlogin.com

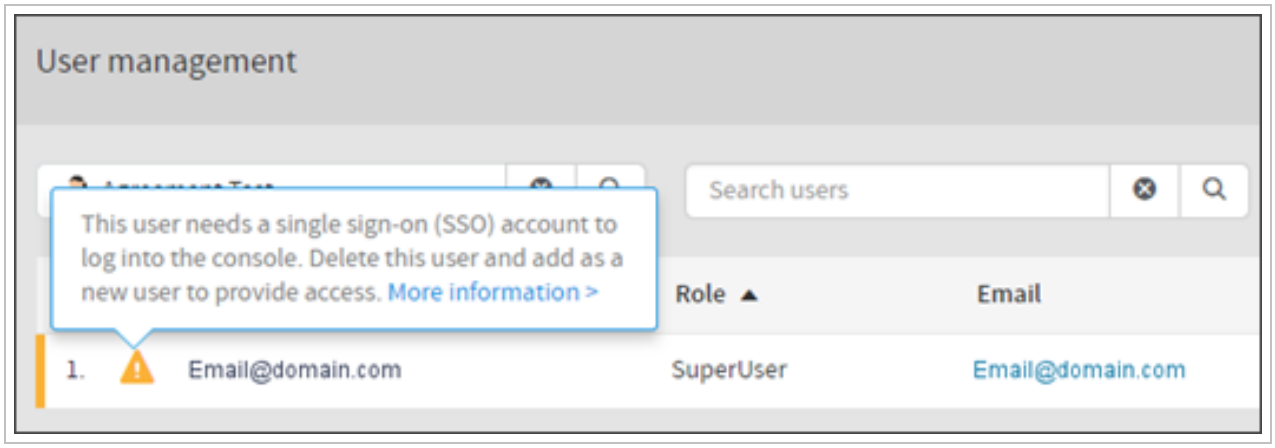
After migration, users are re-directed to the Single Sign-On service login page at https://sso.navigatorlogin.com. This will authenticate their credentials when logging into the Backup Console.

If experiencing problems reaching this page, it may be necessary to add navigatorlogin.com to the white-list on any Firewall or content filtering to ensure you can maintain Backup Console access.

> You cannot use https://sso.navigatorlogin.com to directly access the Backup Console

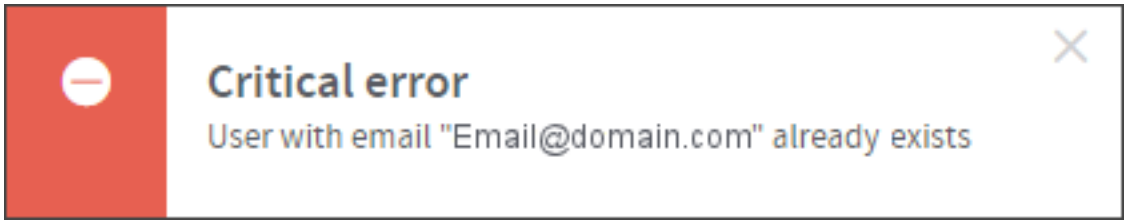
Duplicate Email Addresses

Username email addresses must be unique and only associated with one backup partner



If linked to more than one customer account, the user will receive a notification in the console to remove the non-unique email address from the other accounts.

When identifying duplicate accounts, the migration will take the active email account with the highest security level to the Single Sign-On service. The duplicate logins are converted to Integration Users and cannot log into the Backup Console. Integration Users can only access the legacy Cloud Management Console (CMC), API services or Storage Nodes.



Existing Single Sign-On users

The user may receive a message that their email address already exists in the Single Sign-On server. This can occur where the email address is also in use as a login for one of our other SSO utilizing MSP solutions (including N-able Remote Monitoring & Management and N-able MSP Manager).

To access the Backup Console post-migration the user simply enters their existing Single Sign-On username and password at the Single Sign-On login page.

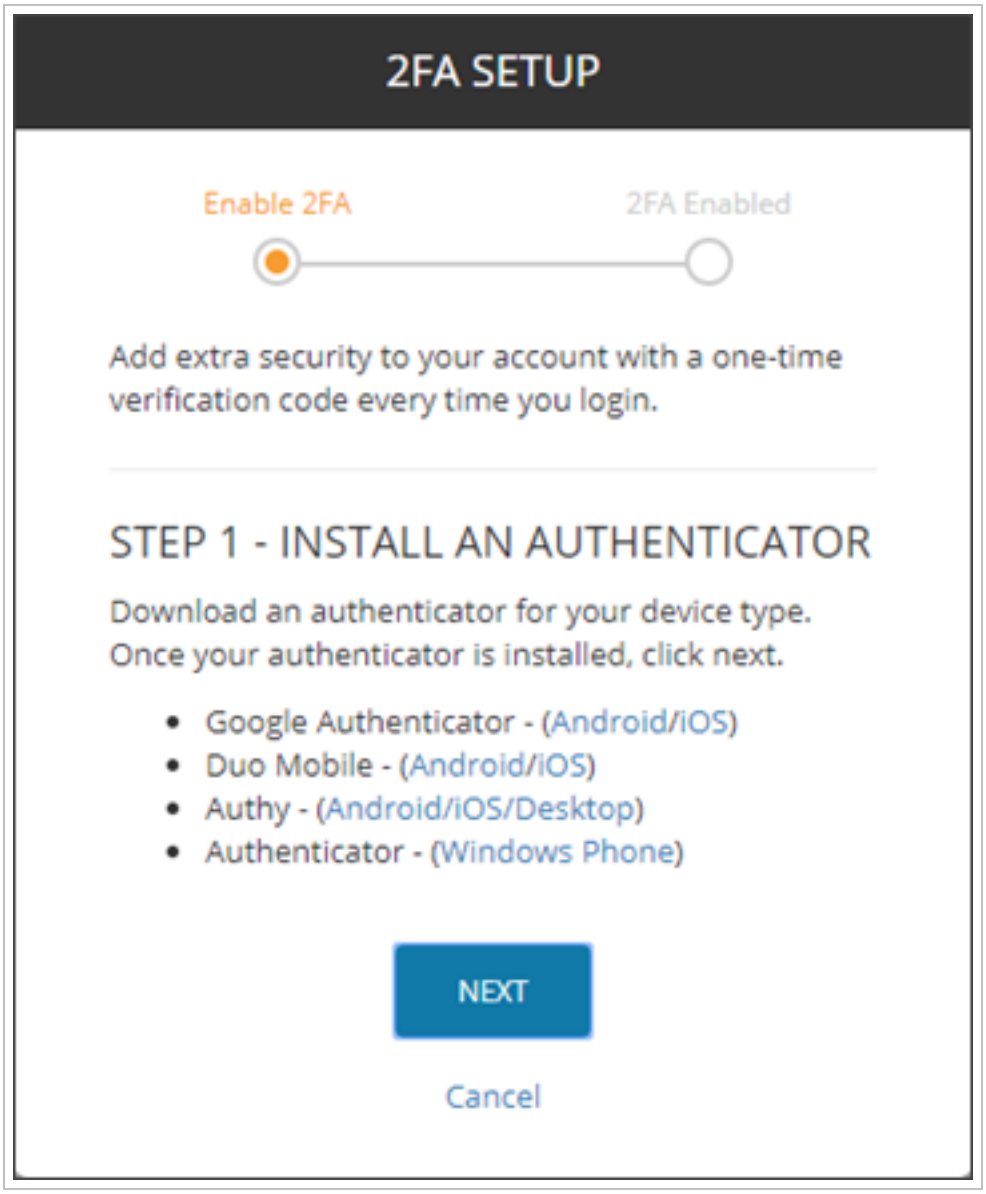
If the user experiences problems with their Single Sign-On password, they can use the “Forgot Password” link on the login page to receive a reset email.

Two-Factor / Multi-Factor Authentication

The Single Sign-On Service utilizes a Two-Factor / Multi-Factor Authentication (2FA or MFA) mechanism. This is a mandatory security measure and cannot be disabled.

Single Sign-on does not support the DoubleChecked app for 2FA. To continue using 2FA after migration, you must setup 2FA on the Single Sign-On server for the email-based login.

> 2FA for new SSO logins will prevent these credentials from working with the legacy Cloud Management Console (CMC), API services or Storage Nodes.



During the 2FA setup phase, you will be provided with a **Recovery Key** - keep this in a secure location. Should you need to reset 2FA due to no longer having access to your used Authenticator tool, you will require this **Recovery Key**.

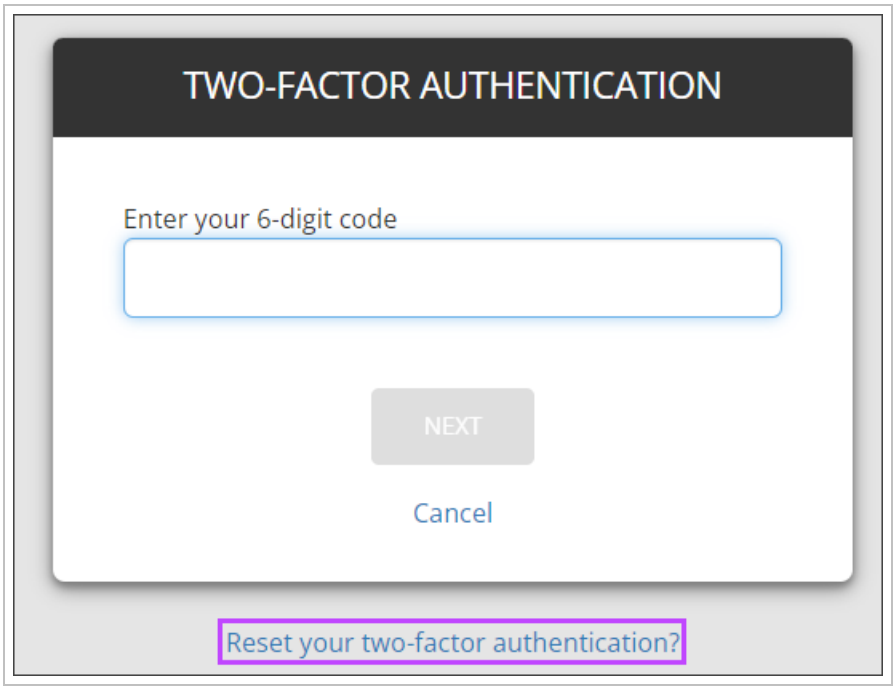
Resetting 2FA

If you no longer have access to the Authenticator to gain the 2FA code due to a replaced phone for example, you will need to reset your 2FA.

To do so, you require the **Recovery Key** given at the point 2FA was configured.

To reset your 2FA:

1. Attempt to log into Backup Manager as normal
2. When presented with the prompt for your MFA code, click the **Reset your two-factor authentication?** link



3. Enter your **Recovery Key** and click **Disable 2FA**
4. You are now prompted to select either **Continue to product** or **Two-Factor Setup** - in either case you will be prompted to configure 2FA before being able to access Management Console

Software Only Partners

Those hosting their own storage nodes must run the Storage Node Installer before and after migration. They must use email-based credentials and update these with a valid password.

> We recommend creating a unique SuperUser for exclusive use in Storage Node authentication.

> Storage Nodes do not support login email credentials linked to 2FA

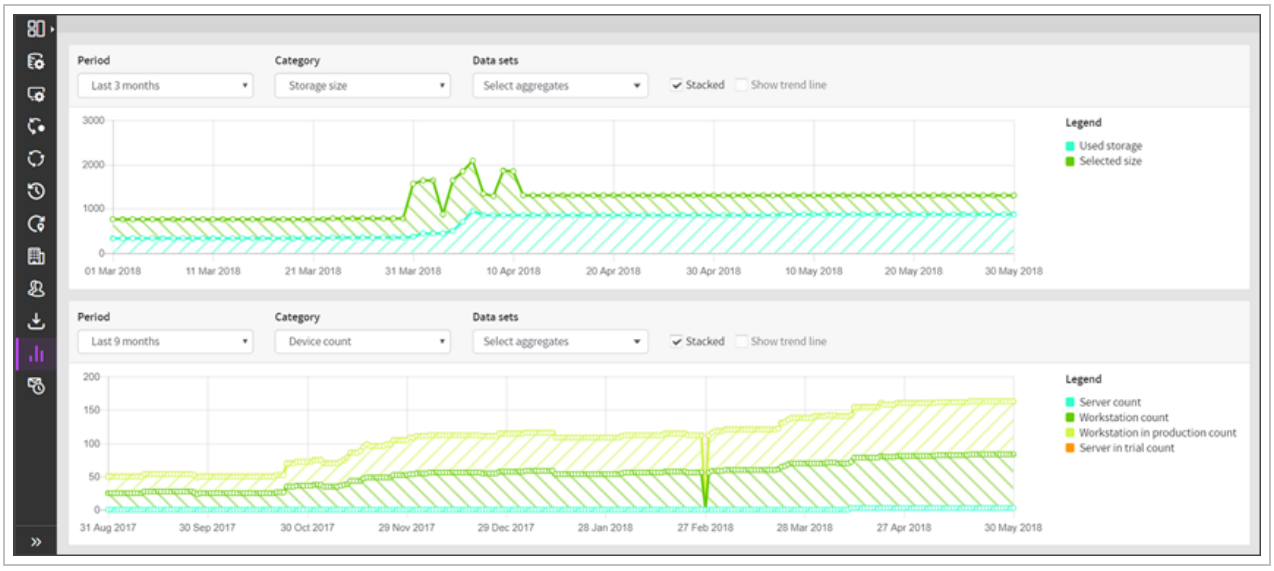
> Failure to confirm or update the storage node credentials can result in missed backups

If experiencing any issues identifying or correcting accounts or have any other issues after migration, please open a support case.

Historical charts in Management Console

You can view customizable charts for a selected period. To access the feature, select **Historical charts** from the **Reporting** section of the vertical menu.

> The data in the charts is for the backup devices belonging to your company and your customers.



Here is the statistics the **Historical charts** module provides.

Category	Definition	Sub-categories
Storage size	The total amount of storage space taken by backup data from the devices belonging to your company and your customers.	Used storage/selected size, trial/production
Device count	The total number of devices belonging to your company and your customers.	Servers/workstations, trial/production, unused devices
Customer count	The total number of customers your company has.	Levels of customers (resellers, end-customers), trial/production
Data source count	The total number of data sources included into backups on all devices belonging to your company and your customers.	Data sources, trial/production
Data source size	The total size of backup selections on all devices belonging to your company and your customers.	Data sources, trial/production

Scheduled Reports in Management Console

You can schedule the delivery of email reports on recent backup and recovery activities. Both the body of the message and the subject field are customizable.

Requirements

A user account of the **distributor**, **sub-distributor**, **reseller** or **end-customer** level is required.

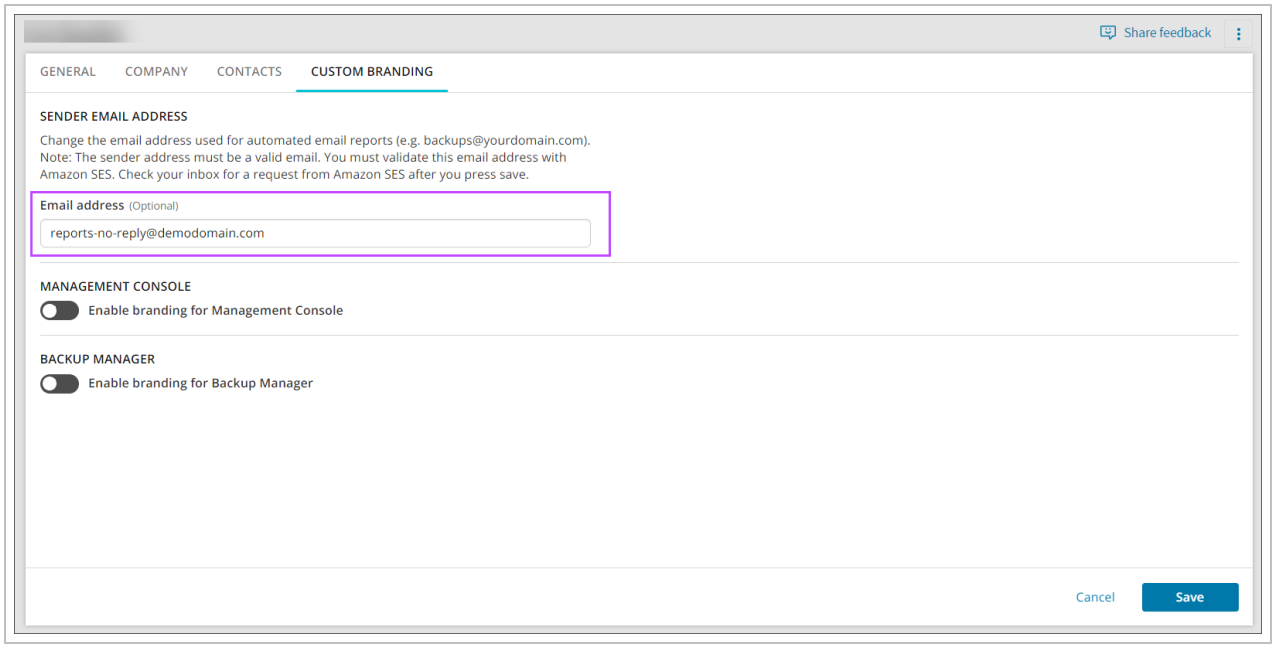
The following needs to be added to the SPF Record for the domain:

- `include:amazonses.com`

Be aware if you use a custom sender address you will will need to verify the address by clicking on a verification link that arrives in the configured email address's inbox. If this does not happen then you will not receive any backup related emails (Let's get started, Backup daily Dashboards, reports, email views etc.).

How it works

- The report **size** is limited to 10 columns and 200 rows: all extra entries are automatically truncated
- The delivery **timing** is approximate, so if you set the delivery to 11am, the report will be send between 10:30am and 11:30am
- The delivery is performed through a specialized **mail service** (Amazon SES), so no outgoing mail settings are needed
- The **From** field of all scheduled reports contains the address from your **Custom Branding** settings (the Edit customer dialogue). If no address is specified there, the address of your parent customer is used.



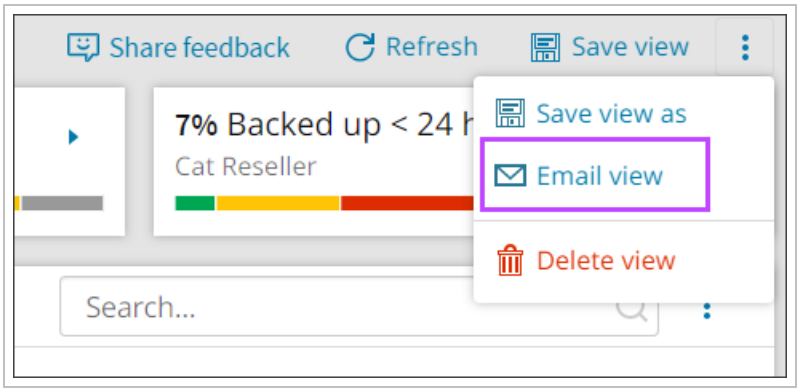
Log in to the Console under a SuperUser account to access the **custom branding** settings.

Add a schedule

1. Login to the Management Console
2. In **Backup > Dashboard**, configure a view for the report (you can select **columns** to display and apply **filters**)

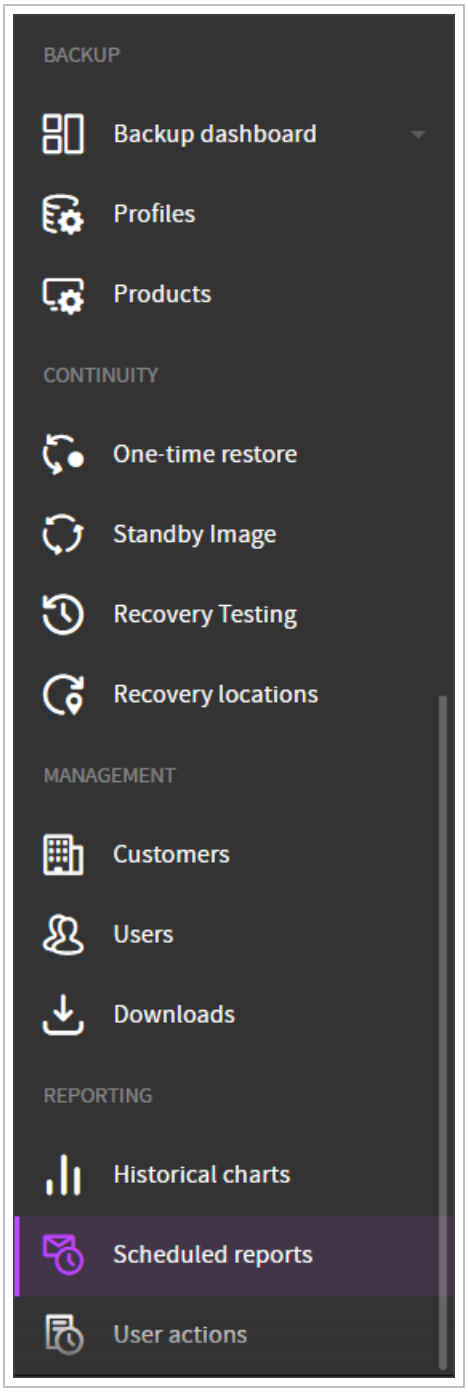
   Custom Columns will not be included in Scheduled Reports.

3. Open the **View Management** menu by clicking the three vertical dots to the right of **Save view** and select **Email view**

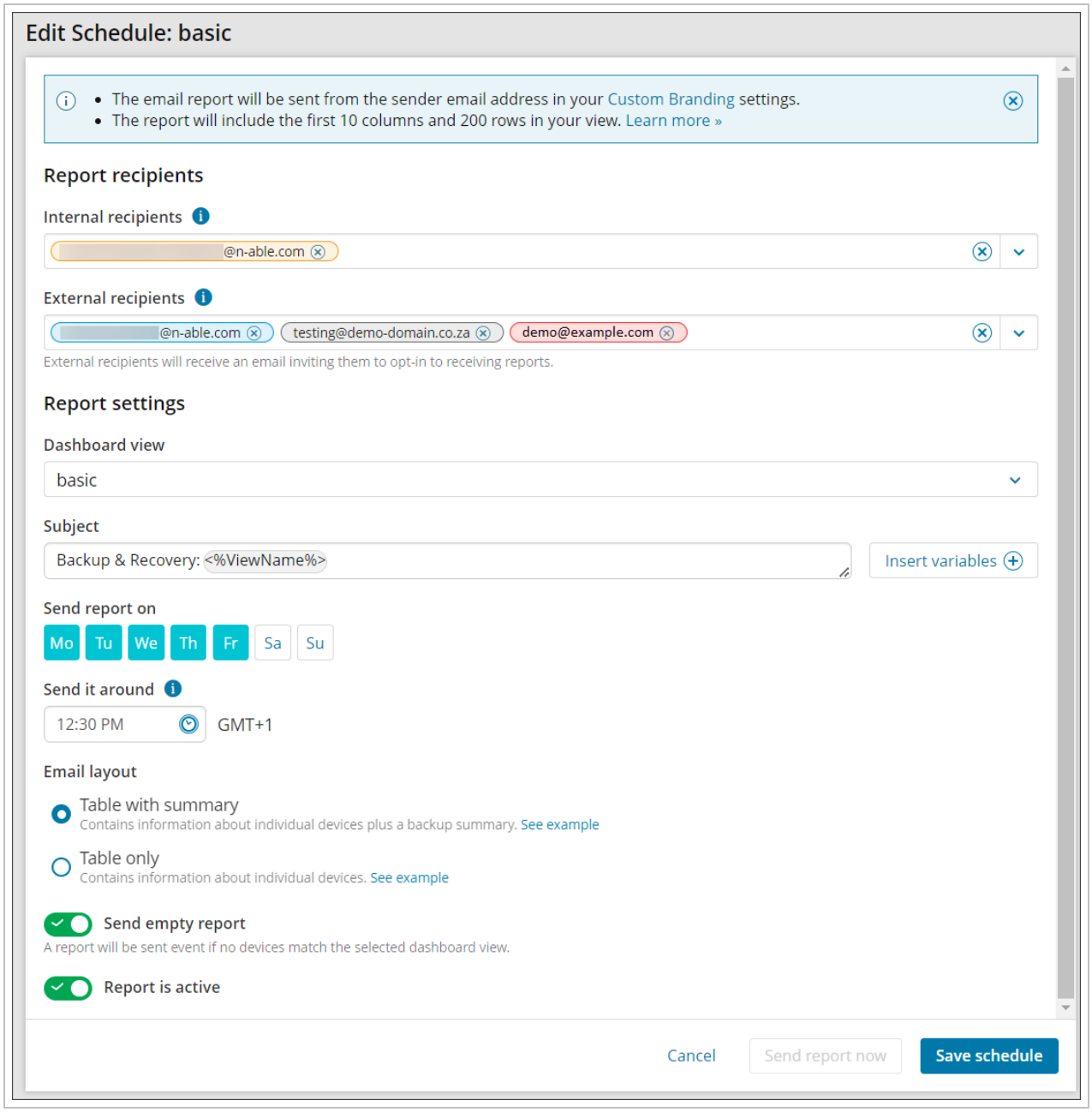


Or

4. Using the left-hand menu, navigate to **Reporting** > **Scheduled Reports**


BACKUP
Backup dashboard
Profiles
Products
CONTINUITY
One-time restore
Standby Image
Recovery Testing
Recovery locations
MANAGEMENT
Customers
Users
Downloads
REPORTING
Historical charts
Scheduled reports
User actions

5. Both options will take you to the **Scheduled Reports** page, click **Add schedule**



6. Fill out the **Recipient(s)** for the report:
   - **Internal recipient(s)** - Type or select single or multiple Management Console users who should receive the report
   - **External recipient(s)** - Type single or multiple external email addresses to receive a copy of the report

     > Hit **Enter** after each address to add them. Each address should be contained within it's own bubble

     ### Recipient Status

     The colour of the bubble surrounding each recipient corresponds to the **Status** of the recipient:

Bubble Colour	Recipient Status	Status Meaning
White	Report Unsaved	The report has not yet been saved, so the recipient's status has not yet been determined
Blue	Subscribed	The recipient has been automatically subscribed (Internal recipients) or clicked **Confirm Opt-In** on the **Report Notification email** (External recipients)
Orange	Unsubscribed	The recipient has clicked **Unsubscribe** on a received report indicating they no longer wish to receive them, see Unsubscribe
Grey	Awaiting Confirmation	The recipient has not clicked **Confirm Opt-In** on the **Report Notification email**. This status is only applicable for 48 hours after scheduling the report
Red	Expired Invitation	The recipient has not clicked **Confirm Opt-In** on the **Report Notification email**, but 48 hours has passed and the invitation has now expired

7. Fill out the **Report Settings**:
   - **Dashboard View** - Select the custom or predefined dashboard view to include in the report from the dropdown
   - **Subject** - Provide an email subject by either typing into the text box or selecting **Insert Variables** to be included. See Variables for the "Subject" field to be for more information
   - **Send report on** - Select the days of the week the report should be sent
   - **Send it around** - Using the time dropdown, select a time for the email to be sent around

     > The current timezone of your computer will be displayed next to this

   - **Email Layout** - make a selection for the way the email is displayed, you may choose between:
     - **Table with summary** - Contains information about the individual devices plus a backup summary
     - **Table only** - Contains information about the individual devices only
   - **Send Empty Report** - Though included within the Email Layout section, this setting is independent of the display structure: when enabled, the report will be sent even if no devices match the selected dashboard
   - **Report is active** - Activate or deactivate the report. The report will automatically be enabled upon creation

8. Click **Save schedule** to save the schedule

> When you use **Email View**, you can only send the view to a user at the same level where the view was created. For example, if you create a view at the Reseller level, you cannot send it to a user at the End-Customer level.

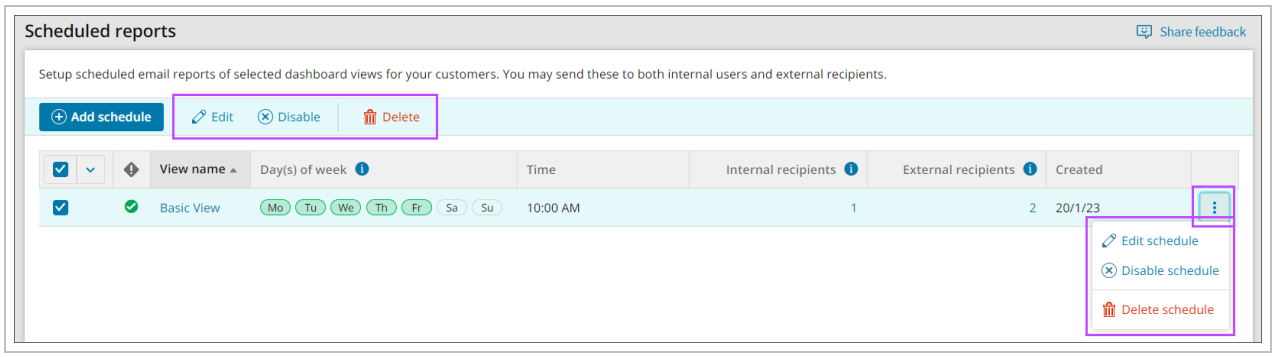
Variables for the "Subject" field

You can customize the **Subject** field of your email reports with the help of variables.

- **View name** (`ViewName`) - the name of the view the report is based on
- **Total number of devices** (`DeviceCount`) - the total number of devices belonging to the customer
- **No backups** (`NoBackupsCount`) - the number of devices on which no backups have been performed yet
- **Completed** (`CompletedCount`) - the number of devices on which the last backup session was successfully completed
- **Completed with errors** (`CompletedWithErrorsCount`) - the number of devices on which the last backup session was completed with errors
- **In process** (`InProcessCount`) - the number of devices on which a backup is currently running
- **Unsuccessful** (`UnsuccessfulCount`) - the number of devices on which the last backup session was unsuccessful (has the "Failed" or "Not started" status)
- **Less than 24 hours ago** (`LastBackupLess24Count`) - the number of devices on which the last backup was performed less than 24 hours ago
- **Less than 48 hours ago** (`LastBackupMore24Less48Count`) - the number of devices on which a backup was performed between 24 and 48 hours ago
- **More than 48 hours ago** (`LastBackupMore48Count`) - the number of devices on which a backup was performed more than 48 hours ago

Manage Existing Schedules

Once a scheduled report has been created, it can be easily edited or deactivated from the **Scheduled Reports** page.



Edit

To edit the schedule:

1. Place a check in the box to the left-hand side of the schedule and click **Edit** from the top bar

   Or,

2. Open the action menu to the right-hand side of the schedule and click **Edit schedule**

> This will allow you to change all aspects of the email schedule as if creating a new one.

Disable/Enable

To disable/enable the schedule either:

1. Place a check in the box to the left-hand side of the schedule and click **Disable** or **Enable** from the top bar

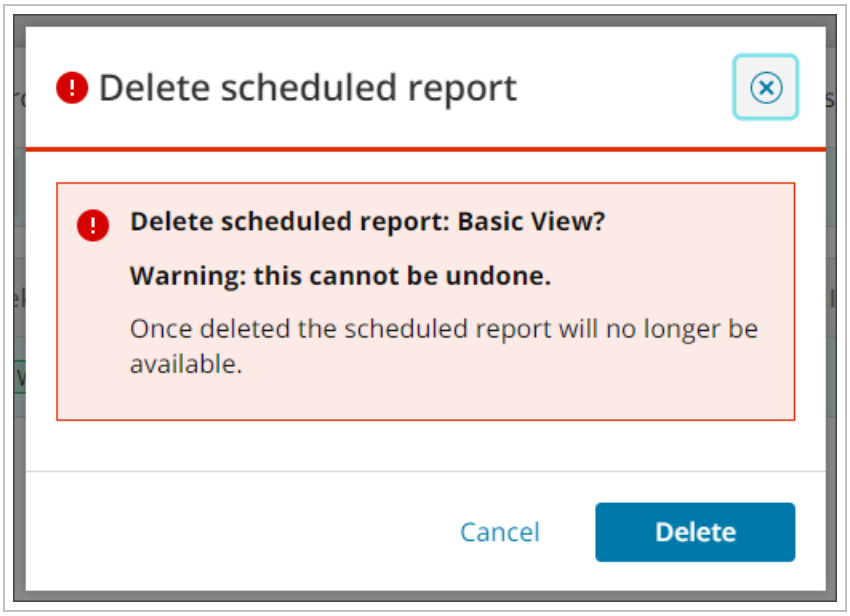
   Or,
2. Open the action menu to the right-hand side of the schedule and click **Disable schedule** or **Enable schedule**

Delete

To delete the schedule:

1. Place a check in the box to the left-hand side of the schedule and click **Delete** from the top bar

   Or,
2. Open the action menu to the right-hand side of the schedule and click **Delete schedule**
3. Confirm deletion of the scheduled report

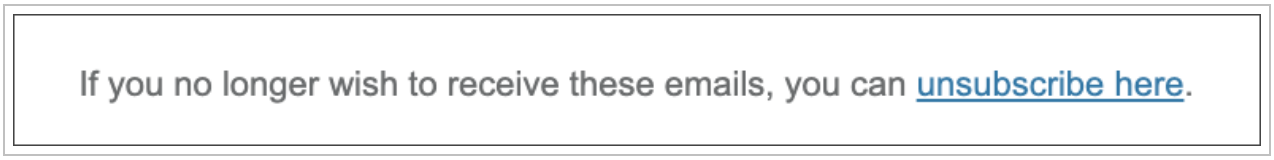


Unsubscribe

If you no longer wish to receive the report, you can Unsubscribe from it without deleting or editing the report in the Management Console.

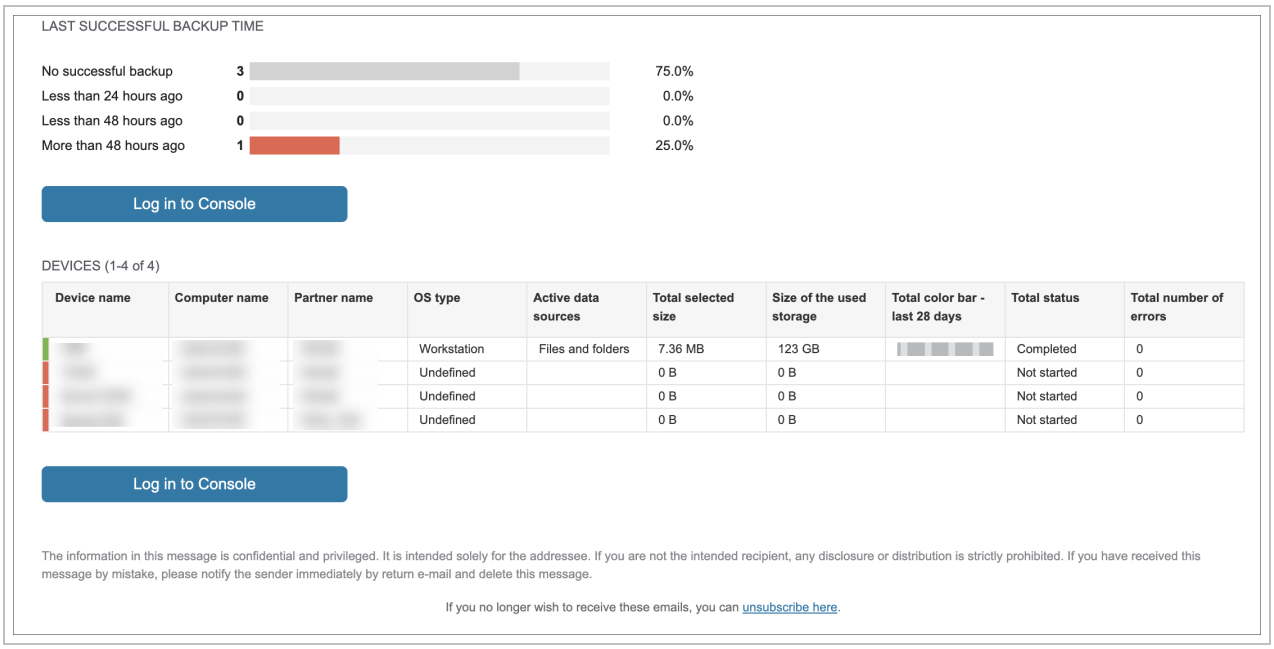
1. Open the report email in your inbox
2. Scroll to the bottom of the email

3. Click **Unsubscribe**



Example Report

How Scheduled Reports looks will depend on the selection you have made in the report settings, however, the report will be displayed similarly as follows:



LAST SUCCESSFUL BACKUP TIME

No successful backup	3	75.0%
Less than 24 hours ago	0	0.0%
Less than 48 hours ago	0	0.0%
More than 48 hours ago	1	25.0%

Log in to Console

DEVICES (1-4 of 4)

Device name	Computer name	Partner name	OS type	Active data sources	Total selected size	Size of the used storage	Total color bar - last 28 days	Total status	Total number of errors
			Workstation	Files and folders	7.36 MB	123 GB		Completed	0
			Undefined		0 B	0 B		Not started	0
			Undefined		0 B	0 B		Not started	0
			Undefined		0 B	0 B		Not started	0

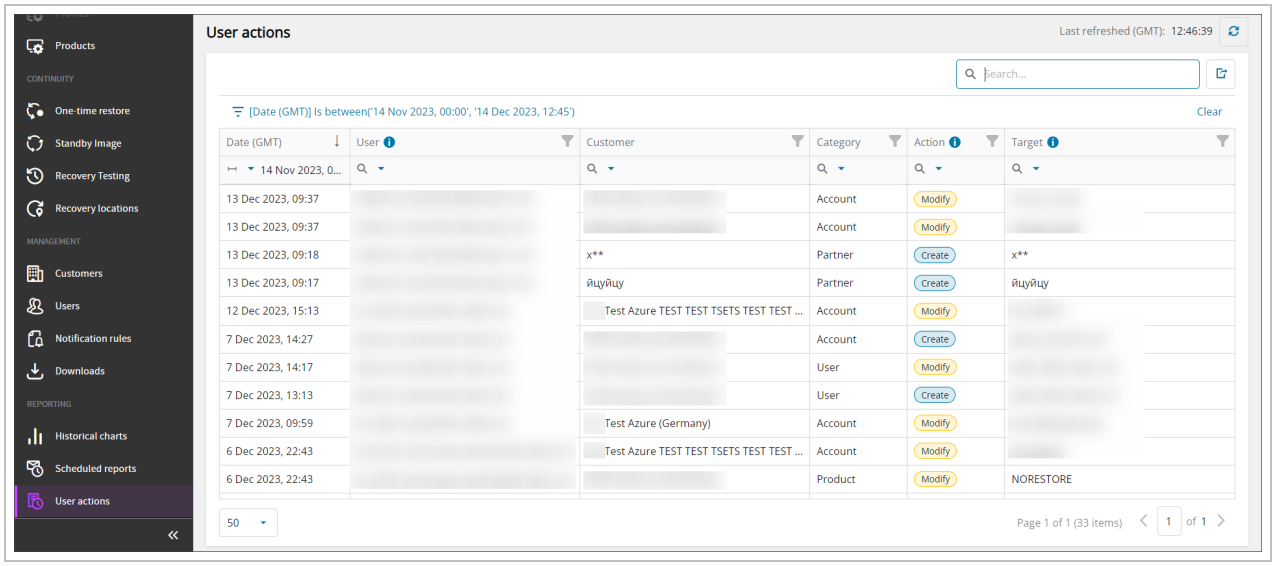
Log in to Console

The information in this message is confidential and privileged. It is intended solely for the addressee. If you are not the intended recipient, any disclosure or distribution is strictly prohibited. If you have received this message by mistake, please notify the sender immediately by return e-mail and delete this message.

If you no longer wish to receive these emails, you can unsubscribe here.

User Actions Log

Cove Data Protection (Cove)'s User Actions log displays one month worth of data detailing actions taken by users on the Management Console. The feature can be found by navigating to **Management** > **User Actions**.



The User Actions page does **not** show system actions

Export

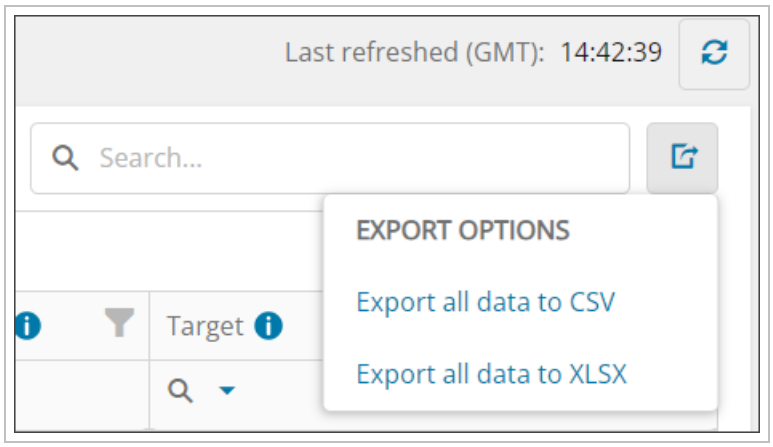
It is possible to export the content of the User Actions Log page.

Searches and filters will be taken into account when the data is exported.

This can be done by:

1. Click the export button at the top right-hand corner of the actions list

2. Select the format to export as:
   a. Export all data to CSV
   b. Export all data to XLSX



3. A pop-up will indicate the export is in progress complete

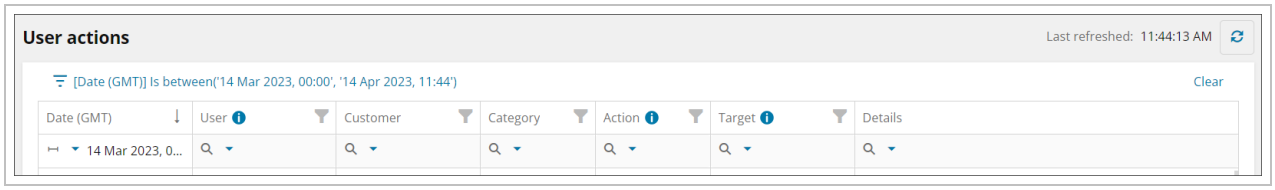
Searching and Filtering

Search

From the **User Action** page, you can search by the **Date**, **User**, **Customer**, **Category**, **Action**, **Target** or **Details** columns specifically to find actions from the full list that meet your required criteria.

> The filter is set to the previous 30 days by default, and so this time frame is already filled in to this cell.

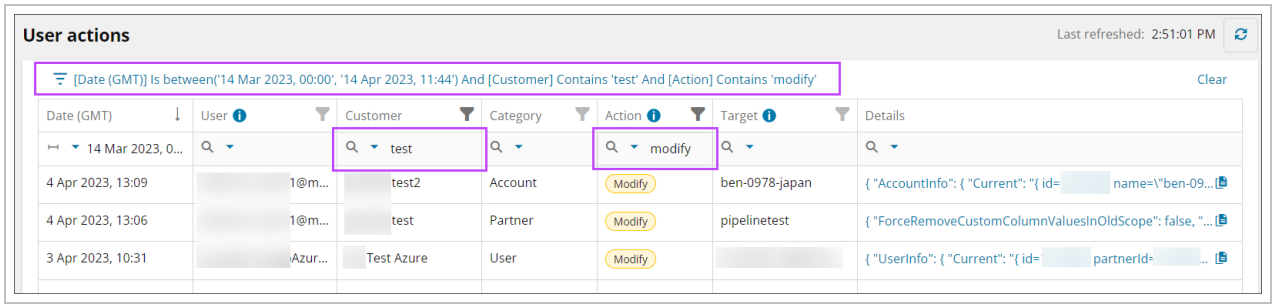
1. The top row of the Actions list is the search bar, click into the cell with the magnifying glass icon to search the data in that column



2. Enter the search term: the list of actions will update automatically to display results

> Searches can be layered, e.g. **User** contains 'admin@domain.invalid' and **action** is 'Modify'

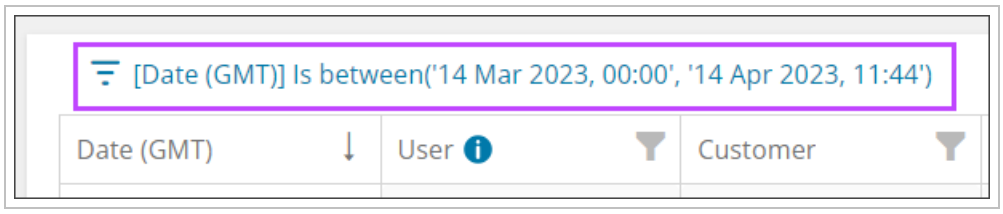
Any search you place will be displayed above the Actions list as a filter:



Filter

From the **User Actions** page, it is possible to create **custom filters** using the **Filter Builder** to find specific actions from the list.

1. The filter is set to the previous 30 days by default, to create a custom filter, click the date filter above the Actions list to open the **Filter Builder**



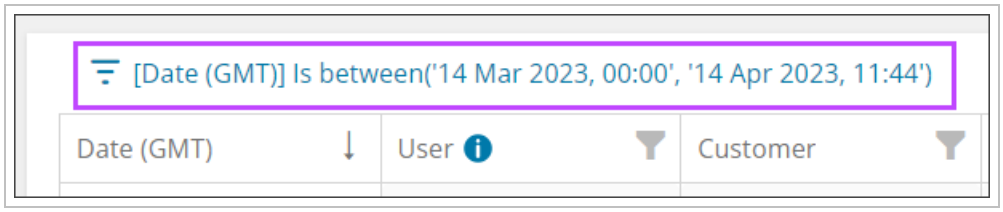
2. In the Filter Builder window, create the filter using the following selections:
    - **And**
        - **Date (GMT)** to which the following may be applied:
            - **Is Between** - use the date and time selectors to select the start and end date and time
        - **User** to which the following may be applied:
            - **Contains** - Text box to enter the filter text
            - **Equals** - Text box to enter the filter text
            - **Is any of** - Select from the list of values
            - **Does not equal** - Text box to enter the filter text
        - **Customer** to which the following may be applied:
            - **Contains** - Text box to enter the filter text
            - **Equals** - Text box to enter the filter text
            - **Is any of** - Select from the list of values
            - **Does not equal** - Text box to enter the filter text
        - **Category** to which the following may be applied:
            - **Contains** - Text box to enter the filter text
            - **Equals** - Text box to enter the filter text
            - **Is any of** - Select from the list of values
            - **Does not equal** - Text box to enter the filter text
        - **Action** to which the following may be applied:
            - **Contains** - Text box to enter the filter text
            - **Equals** - Text box to enter the filter text
            - **Is any of** - Select from the list of values
            - **Does not equal** - Text box to enter the filter text
        - **Target** to which the following may be applied:
            - **Contains** - Text box to enter the filter text
            - **Equals** - Text box to enter the filter text
            - **Is any of** - Select from the list of values
            - **Does not equal** - Text box to enter the filter text
        - **Details** to which the following may be applied:
            - **Contains** - Text box to enter the filter text

> Searches can be layered, e.g. **User** contains 'admin@domain.invalid' and **action** is 'Modify' and **Target** contains 'All Devices'. Once the filter is created, this will appear above the updated list similar to:
> `[Date (GMT)] Is between('14 Mar 2023, 00:00', '14 Apr 2023, 11:44') And [User] Contains 'admin@domain.invalid' And [Action] Equals 'Modify' And [Target] Contains 'All Devices'`

3. Use the **+** icon to add more layers to the filter
4. Click **OK**

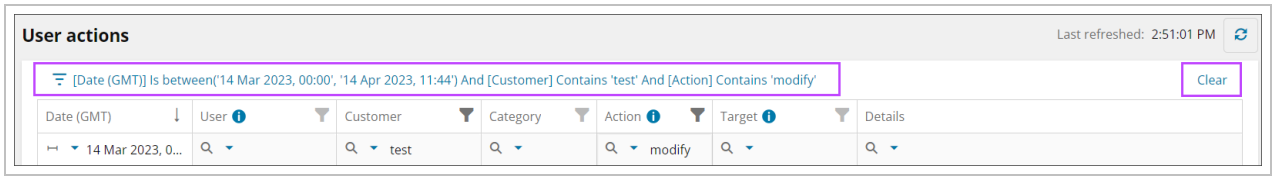
Edit Filters

Filters can be edited by clicking the filter string at the top of the User Actions page:



Clear Filters

Filters can be cleared by clicking the **Clear** button at the top of the User Actions page, next to the filter string:



Data export in Management Console

You can export **monthly device statistics** from the Management Console to a spreadsheet in the .xlsx file format.

> Export files created by the Console contain **all the data** that is currently displayed in the **Devices** table. If the data spans across multiple pages, all the pages are exported.

How to Export

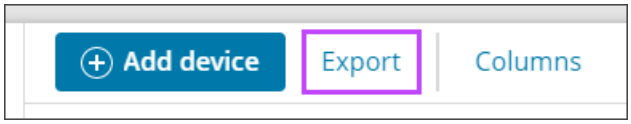
1. From the **Customer** list, select the customer to export statistics for
2. If needed, apply any additional filters to change the list of devices displayed

   > For example using the **Account Type** filter to show only Microsoft 365 devices

   > You **cannot** use checkboxes to select devices for export

3. From the **Columns** list, select all the columns you want to be displayed in the export

4. Click **Export** from the Toolbar



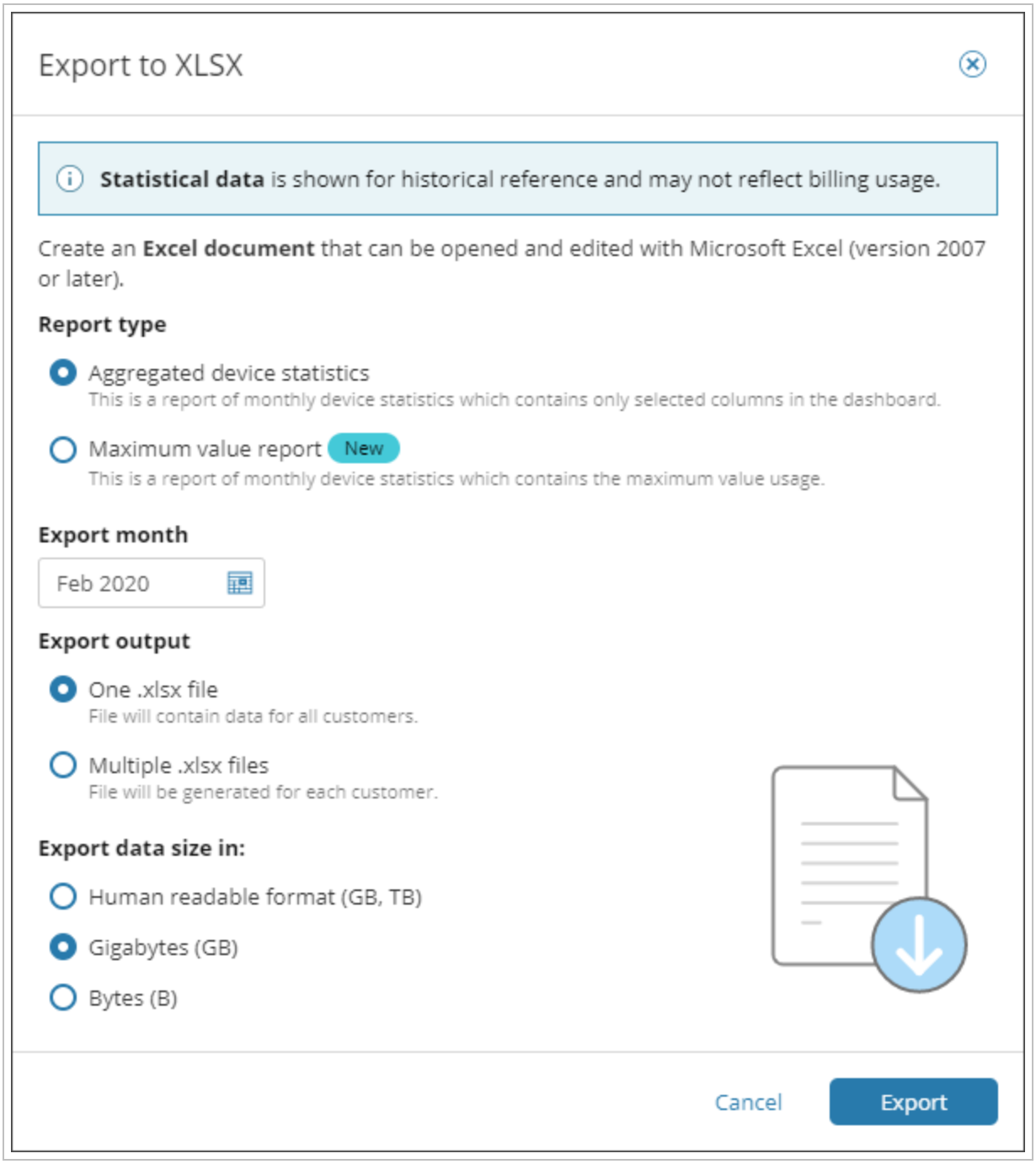
There are two report types to choose from in here:

1. **Aggregated device statistics** - This is a report of monthly device statistics which contains only selected columns in the dashboard
2. **Maximum Value report** (NEW) - This is a report of monthly device statistics which contains the maximum value usage

Configure Aggregated Device Statistics report

1. Select **Aggregated device statistics** under **Report type**
2. Select the **Export month** of data to view
3. Choose an **Export Output** type. This can be either:
   - One .xlsx file containing data for all customers
   - Multiple .xlsx files each one containing data for one customer
4. Select an appropriate data size output. This can be:
   - Human readable format (Gigabytes and Terabytes)
   - Gigabytes only
   - Bytes only

5. Click **Export**

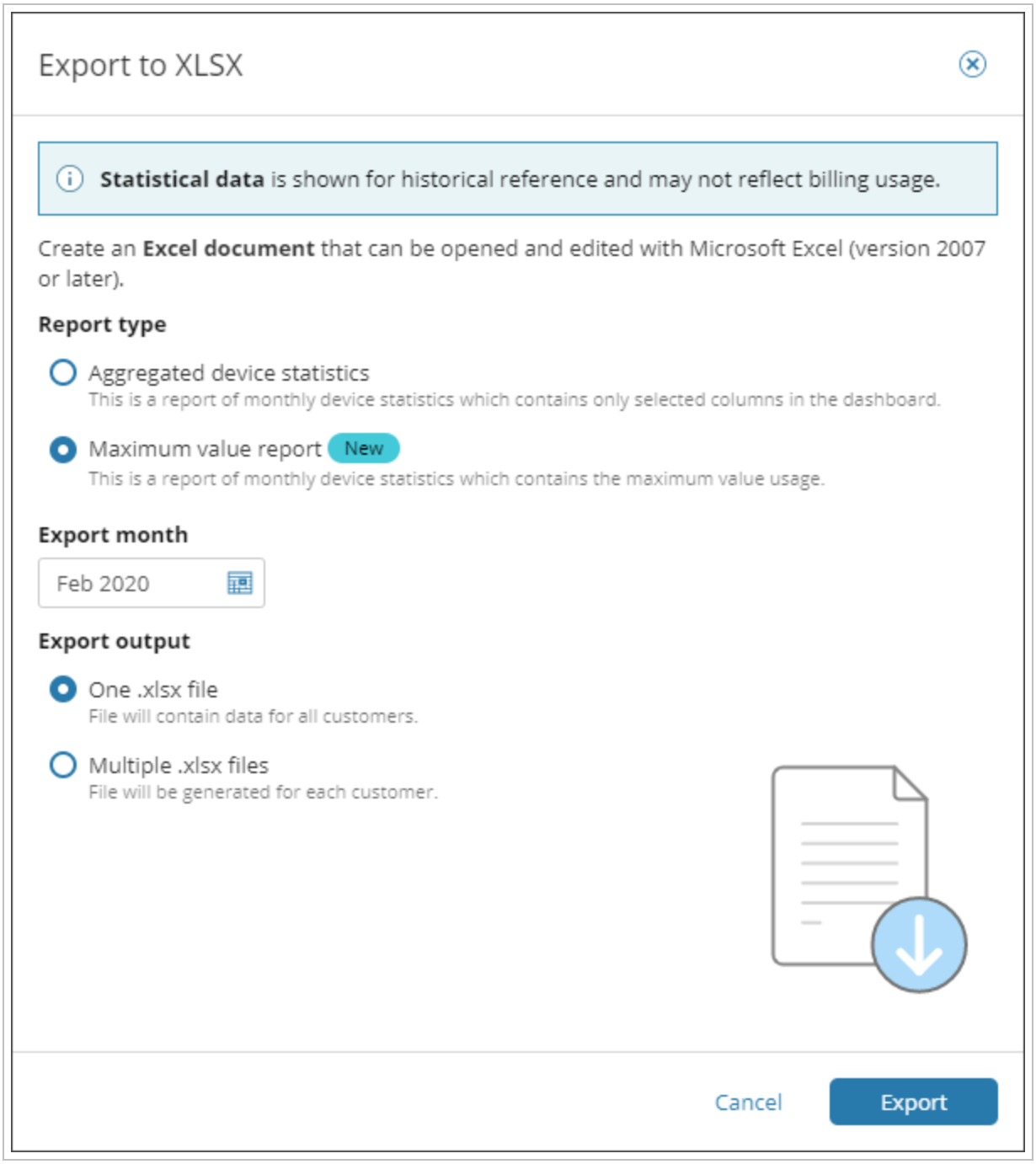


When clicking **Export**, a file explorer box will appear to select the download location. If nothing appears, ensure your browser is set to allow pop-ups from Backup Manager.

Configuring Maximum Value reports

1. Select **Maximum Value Report** under **Report type**
2. Select the **Export month** of data to view
3. Choose an **Export Output** type. This can be either:
    - One .xlsx file containing data for all customers
    - Multiple .xlsx files each one containing data for one customer

4. Click **Export**



When clicking **Export**, a file explorer box will appear to select the download location. If nothing appears, ensure your browser is set to allow pop-ups from Backup Manager.

Glossary of Cove Data Protection (Cove) terms

Microsoft 365 protection

Cove Data Protection (Cove) offers a backup and recovery service for Exchange, OneDrive, Sharepoint and Teams. The service handles full Microsoft 365 Exchange, OneDrive, SharePoint and Teams backups so you can recover data long after it is cleaned or lost from Microsoft databases.

Cove relies on **tenant access** to Microsoft 365, where each tenant may include multiple domains. You have functionality to select only the mailboxes or accounts required for backup.

All backed up data is encrypted during the backup process and the encryption key is securely stored in the cloud.

> Software-Only partners can create Microsoft 365 devices but devices will use N-able storage nodes

> For additional information on what is and is not included in the Teams data Source, see Microsoft 365 Teams: What Is/Is Not Included

Requirements

The following account types are required:

- A **SuperUser** account for the Management Console (for adding domains and initiating backups and restores)
- A Security Officer role (for initiating a restore)
- A **Global administrator** account for Microsoft 365

Benefits

For full details on the benefits of backing up each service with Cove, see Microsoft 365 Benefits.

Limitations

For full details on the limitations of Cove per service, see Microsoft 365 Limitations.

Microsoft 365 Benefits

Cove Data Protection (Cove) is a useful addition to the Microsoft 365 data centre redundancy services.

Teams

- Retention 7 years
- Backup runs up to 6 sessions a day
- Backups up the Channels messages of Teams
- Allows restore from a specific data and session

- Allows restore to a new location
- **All data processing and storage is kept regional**[1]

Exchange

- Retention 7 years
- Backup runs up to 6 sessions a day
- Backups up the full content of the mailbox
- You can restore accepted event **invitation** emails through the calendar restore
- Allows restore from a specific data and session
- Allows restore to 3 target locations:
  - Auto-generated location
  - Original location
  - New location
- **All data processing and storage is kept regional**[2]

OneDrive

- Retention 7 years
- Backup runs up to 4 sessions a day
- Allows restore from a specific date and session

---

[1]Storage locations used:
United States
Brazil
Canada
Australia
United Kingdom
Germany
The Netherlands
Switzerland
Belgium
[2]Storage locations used:
United States
Brazil
Canada
Australia
United Kingdom
Germany
The Netherlands
Switzerland
Belgium

- Allows restore to 3 target locations:
  - Auto-generated location
  - Original location
  - New location
- **All data processing and storage is kept regional**[1]

SharePoint

- Retention 7 years
- Backup runs up to 4 sessions a day
- Allows restore from a specific date and session
- From version 19.12, SharePoint online permissions are now protected. See the Microsoft 365 SharePoint Permissions page for more details.

  > This allows you to restore SharePoint files and folders to their original state from the backup session

- Allows restore to 2 target locations:
  - Original location
  - New location
- **All data processing and storage is kept regional**[2]
- Role definitions can be restored only in root site (or site collection)
- Meta-data of SharePoint files can be backed up and restored

Microsoft 365 Limitations

Microsoft 365 protection has the following limitations depending on the service:

---

[1]Storage locations used:
United States
Brazil
Canada
Australia
United Kingdom
Germany
The Netherlands
Switzerland
Belgium
[2]Storage locations used:
United States
Brazil
Canada
Australia
United Kingdom
Germany
The Netherlands
Switzerland
Belgium

Teams

- Only user accounts with Security Officer permissions can restore from deleted or unlicensed accounts
- Only user accounts with Security Officer permissions can delete backup history for accounts

  > See the User roles for full details on how this might affect you.

- All **private channels** will be restored as public
- **Deleted channels** will not be backed up
- **Guest users** in the channels will not be restored in the channels

  > Guest users must be added after the channel is restored.

- It is not possible to configure settings for the General channel and as such will restore Microsoft's default settings
- **Group settings** cannot be restored, Microsoft's default group settings will be applied on restored channels
- If a Team is **Archived** prior to the recovery, it will restore in full and must be archived again manually
- **Tags** and **Apps** in the Team will not be backed up

Exchange

- We do not currently support backup or restore of Groups
- We do not currently support backup or restore of Outlook Notes
- You cannot restore calendar events that have not been accepted by the recipient
- Only user accounts with Security Officer permissions can restore from deleted or unlicensed mailboxes
- Only user accounts with Security Officer permissions can delete backup history for accounts

  > See the User roles for full details on how this might affect you.

- We do not support hybrid Microsoft 365 installations for backup. On-premises mailboxes may be detected as connected to Microsoft 365 but we are unable to protect them as access is not given to the on-premises installation
- We do not currently support backup or restore of Public folders. This is due to the configuration of Microsoft data layers
- We do not currently support backup or restore of Tasks
- Colour categories will not be included in the backup and restore of Contacts
- Protection for Archived mailboxes or a native Archive folder is not provided through backup
- You cannot backup from **unlicensed** mailboxes. Please confirm that the mailbox does not fall under one of these scenarios:
  1. The mailbox is present, but the license was removed. In this case, it will not be possible to add the mailbox to the backup
  2. The mailbox and license were removed while the backup is in progress. In this case, the backup will not be able to complete and you will see the error "**Unable to backup user without license**" for such mailboxes
  3. The mailbox is removed before the backup is started. In this case, the backup will run but skip this mailbox

     > To resolve this issue you will need to undelete the mailbox via the Microsoft 365 Admin portal and provide a license to the mailbox. After the backup is completed for the mailbox, you can then delete the mailbox and remove the license. We cannot backup deleted mailboxes, even if they have a license assigned.

- We do not currently support delegated Microsoft 365 tenants. It’s required to grant permissions being logged in as administrator of original tenant

OneDrive

- Only user accounts with Security Officer permissions can restore from deleted or unlicensed accounts
- Only user accounts with Security Officer permissions can delete backup history for accounts

  > See the User roles for full details on how this might affect you.

- Cove does not currently support backup or restore of OneNote folders. This means we cannot backup *any* OneNote data, as (by default) all OneNote pages are located in Folder notebooks.
- Though OneDrive supports versioning, we only backup the latest version of files
- You cannot backup from accounts that are **not licensed** or **deleted**
- You cannot restore OneDrive items from the Trash folder (if the item was backed up before being moved to Trash, restore from the original location will be possible)
- We do not currently support backup and restore items protected by Information Rights Management (IRM)
- We do not currently support delegated Microsoft 365 tenants. It's required to grant permissions being logged in as administrator of original tenant.

SharePoint

- We do not backup previous versions of files, only the current version
- We do not backup SharePoint lists
- We do not support Loop pages
- We do not support backup of the SharePoint pages, styles and images used to create the SharePoint site
- We do not support backup of planners via SharePoint as these are a separate data source which is not detected during the Backup process
- We do not support backup of Wikis via SharePoint as these are a separate data source which is not detected during the Backup process
- We do not support backup and restore items protected by Information Rights Management (IRM)
- We do not support delegated Microsoft 365 tenants. It's required to grant permissions being logged in as administrator of original tenant
- Cove does not currently support backup or restore of OneNote folders. This means we cannot backup *any* OneNote data, as (by default) all OneNote pages are located in Folder notebooks.
- We cannot re-create a deleted site collection. If a site collection is deleted, it can be restored to a new location, which must be created manually

  > A site collection includes the site within SharePoint, as well as a site's necessary structures (for instance, the site's Document Library).

- Due to a SharePoint Online limitation, role definitions can only be restored in a root site (or site collection)

Custom Document Library

If you are using a custom document library (DL) within SharePoint and the below applies, files may be inaccessible and **will not** be backup:

1. **Enforce unique values** is set to 'yes'
2. Files are not checked in on SharePoint

To ensure all files are backed up when using a custom document library you must ensure:

1. **Enforce unique values** is set to 'no'
2. Files have been checked in on SharePoint to recognize changes

Enable Microsoft 365 Backups

To enable a new Exchange, OneDrive, SharePoint or Teams device or to add a new service to an existing domain for Microsoft 365 backups, add the domain to the Management Console using the appropriate steps below. Before you begin, ensure you have met the necessary requirements:

Requirements

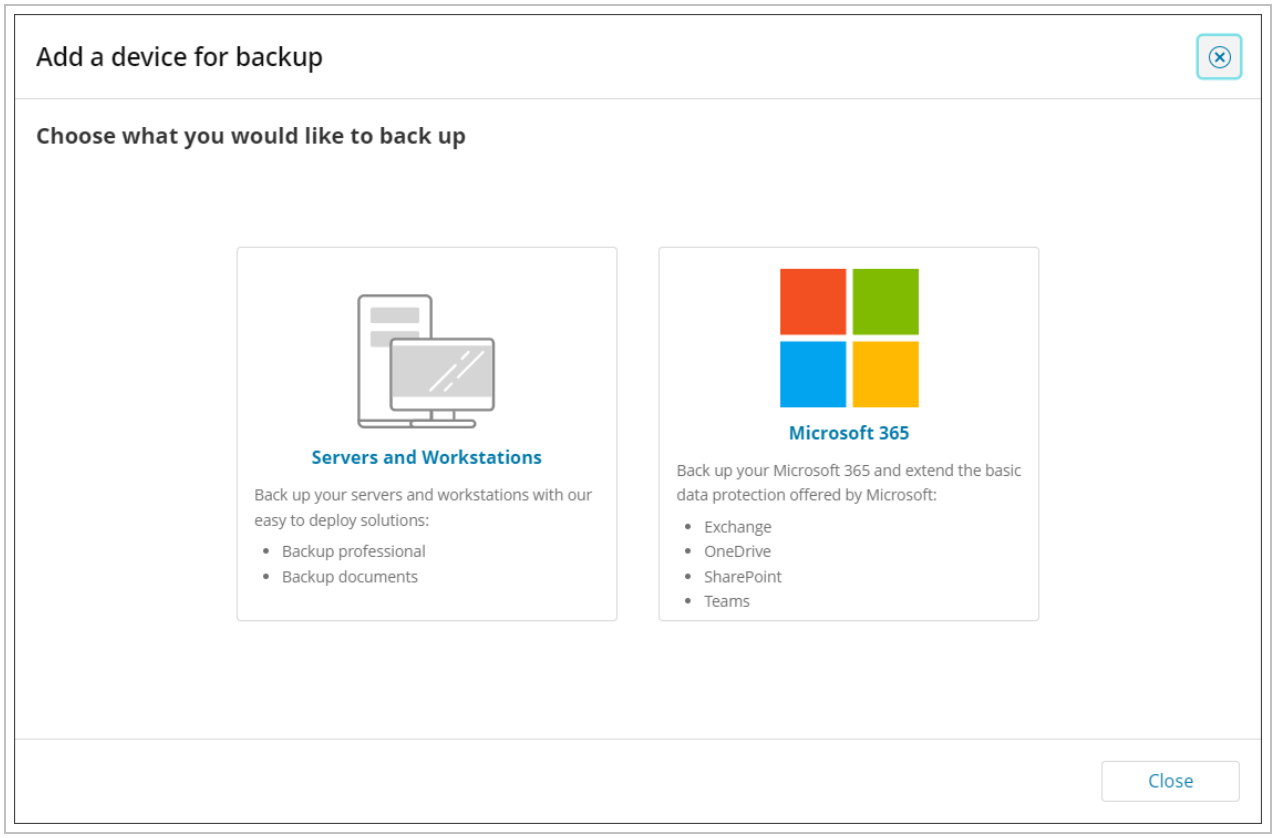
The following account types are required:

- A **SuperUser** account for the Management Console (for adding domains and initiating backups and restores)
- A Security Officer role (for initiating a restore)
- A **Global administrator** account for Microsoft 365

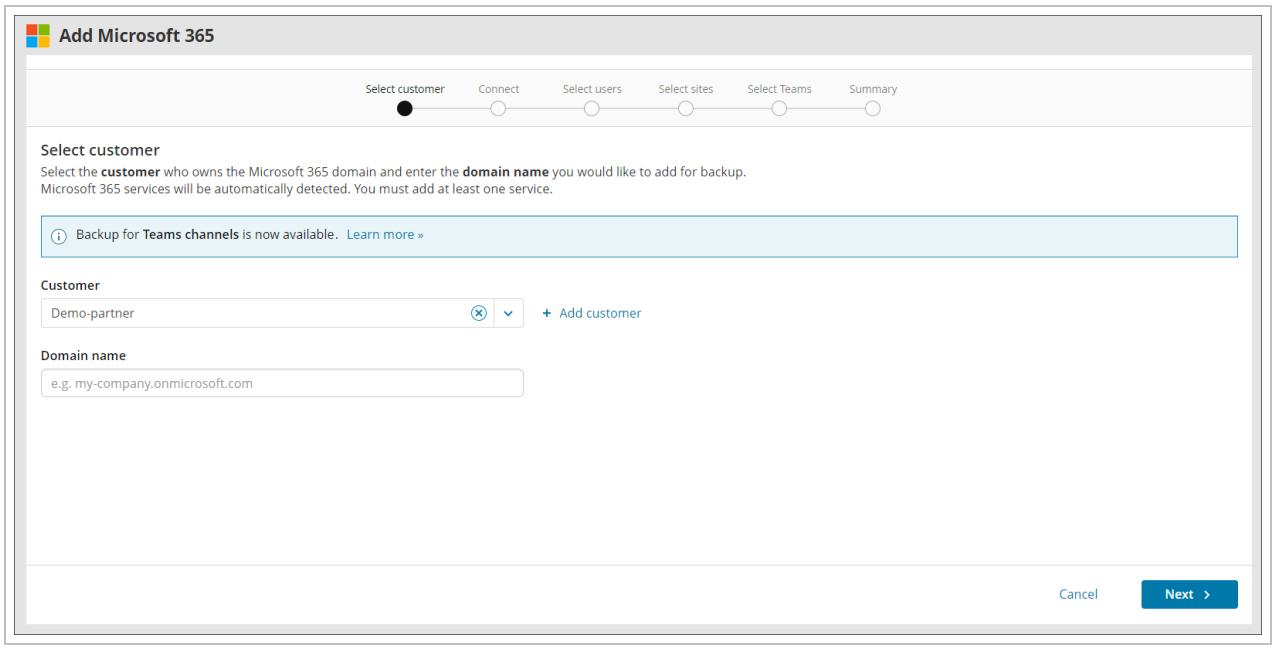
> For additional information on what is and is not included in the Teams data Source, see Microsoft 365 Teams: What Is/Is Not Included

Teams, Exchange, OneDrive and SharePoint

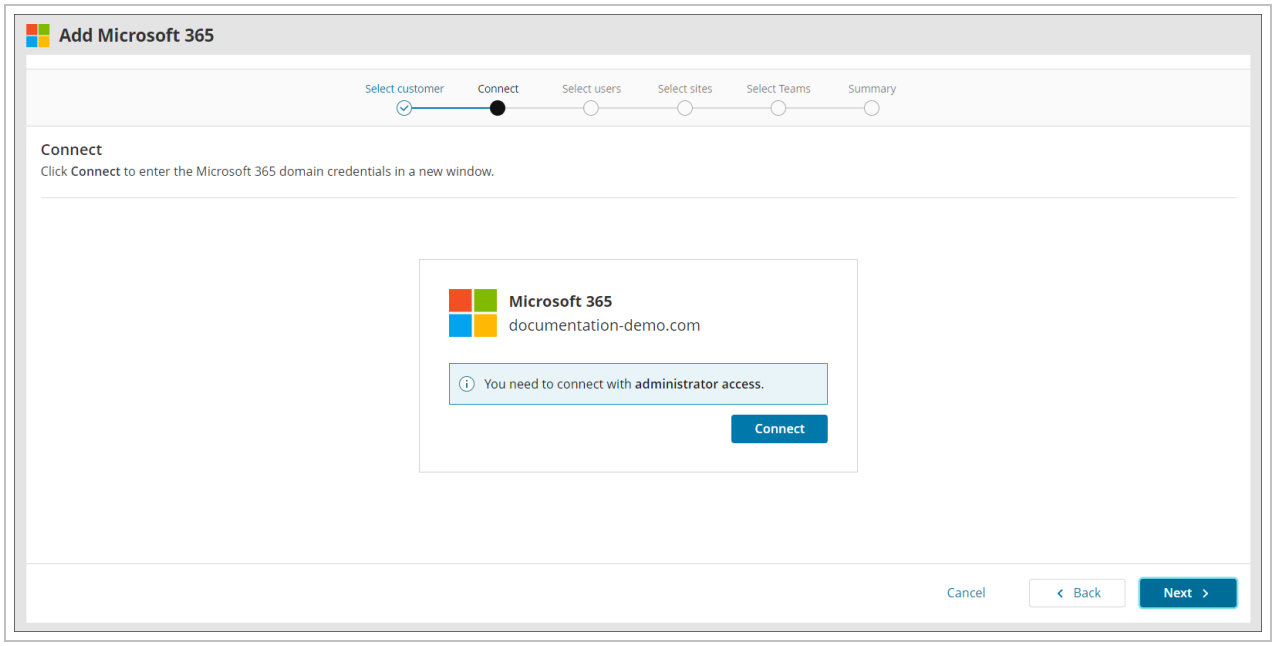
1. Log in to the Management Console under a **SuperUser** account
2. Click **Add** > **Microsoft 365**



3. Select the **Customer** from the customer dropdown or +Add new customer
4. Enter the **Domain name** and accept that you acknowledge that Microsoft 365 data will be backed up and restored in accordance with our regional data principals, then click **Next**

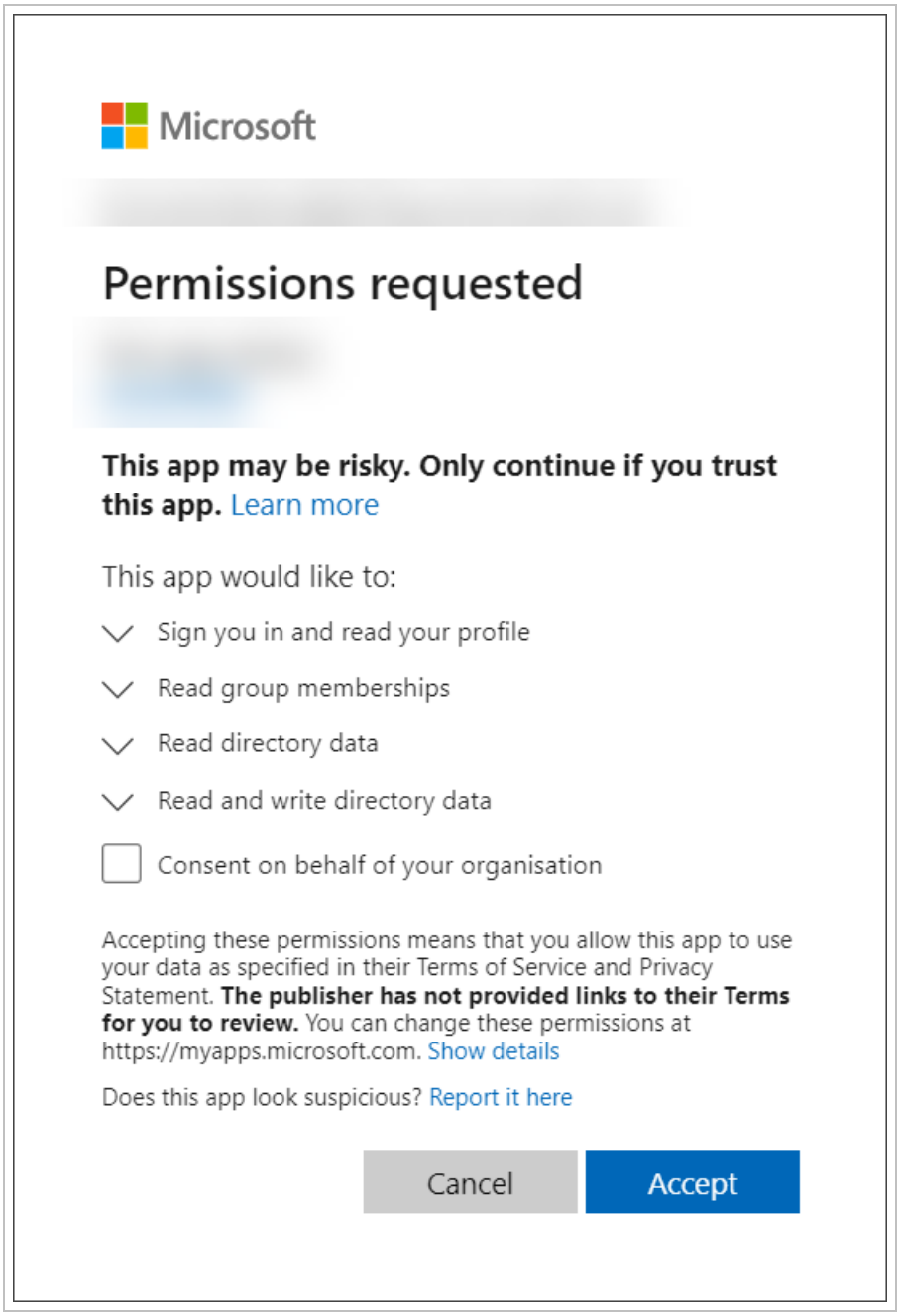


5. **Connect** to the domain using administrative access



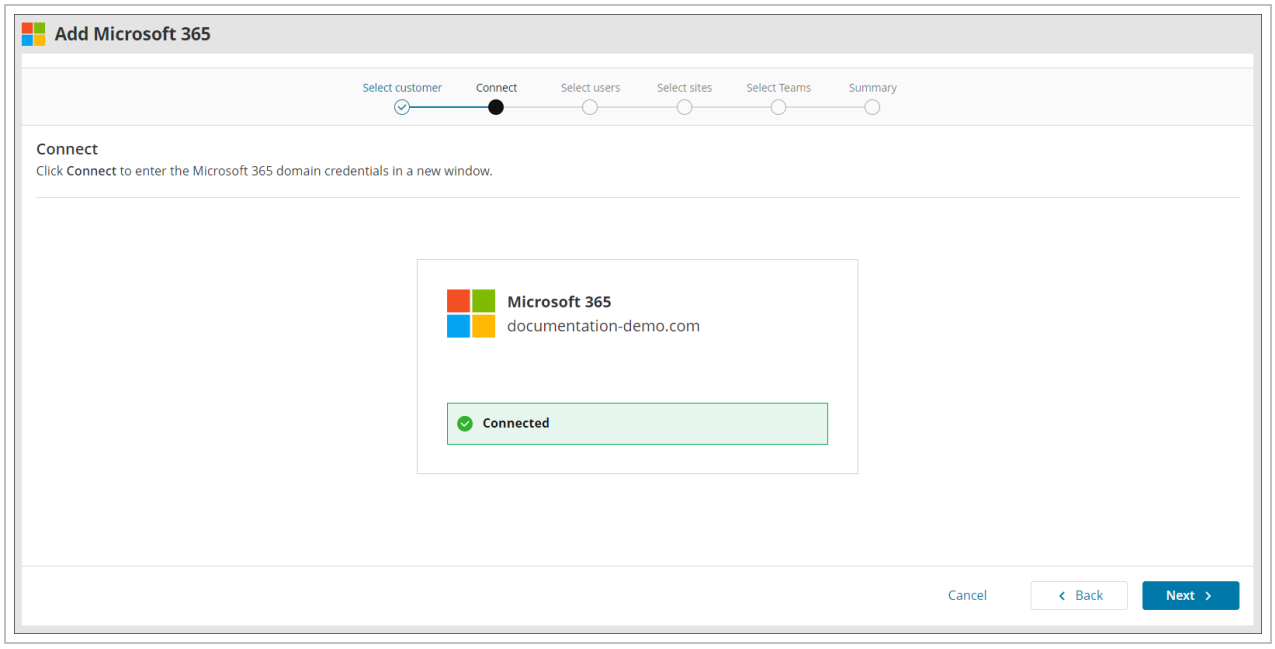
If you do not see the authentication page, make sure your browser is not blocking **pop-up windows**.

6. Accept the required permissions

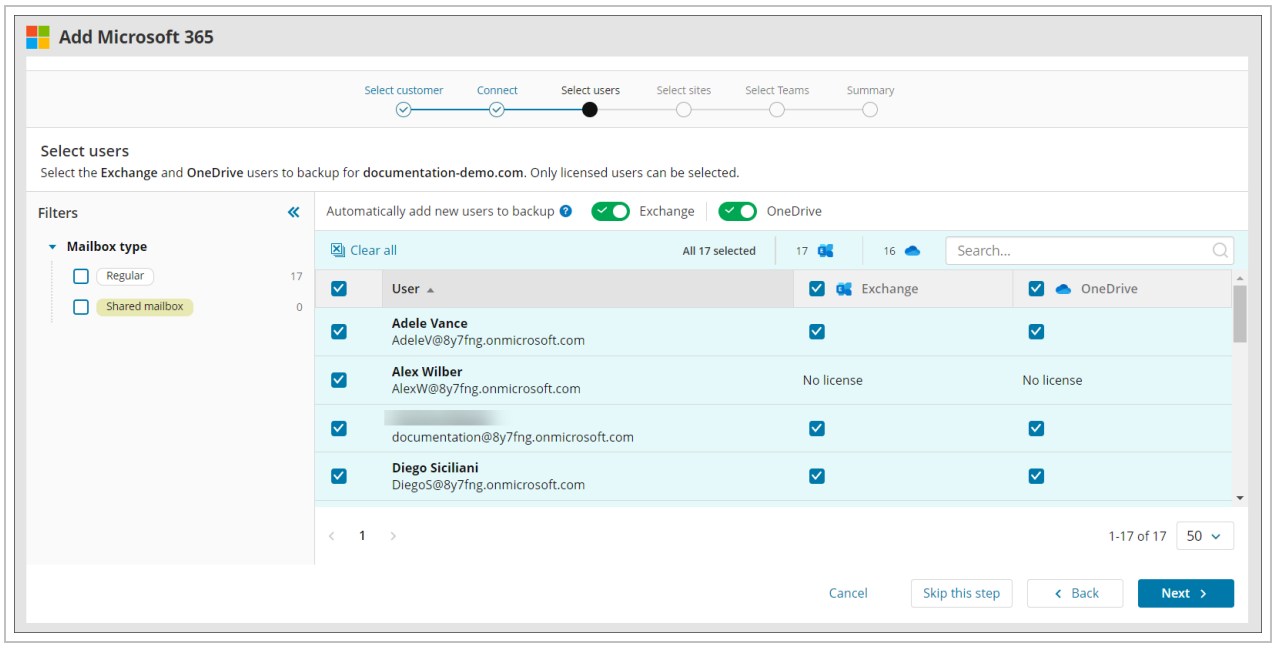


> Tick **Consent on behalf of your organisation** if you wish to allow this app access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

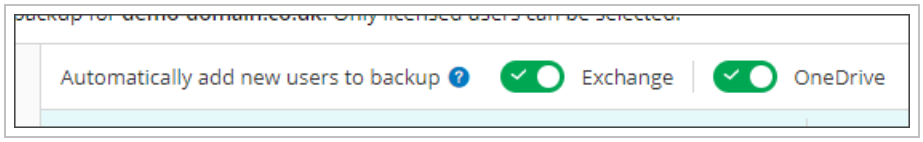
7. When the connection is established, and you see the **Connected** dialog below, click **Next** to continue



8. View the **Exchange** and **OneDrive** accounts found in the domain and select the required data to backup

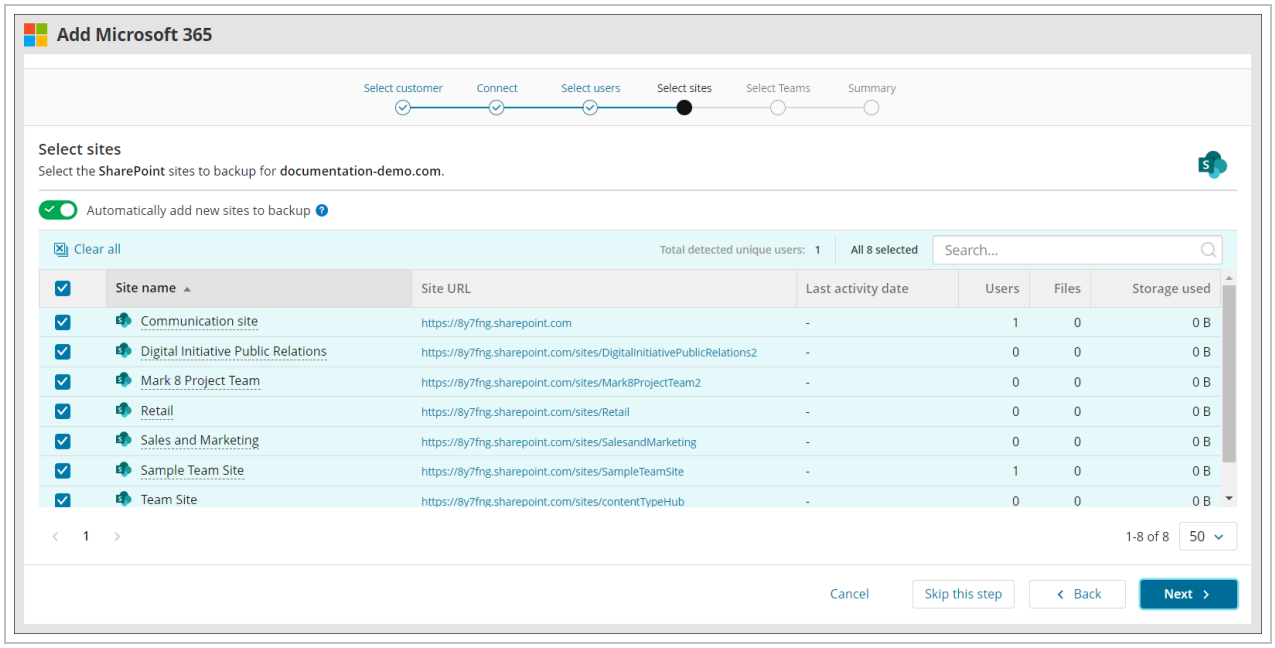


a. Enable the **Automatically add new users to backup** if you wish to allow users discovered during a backup to be added to the backup selection

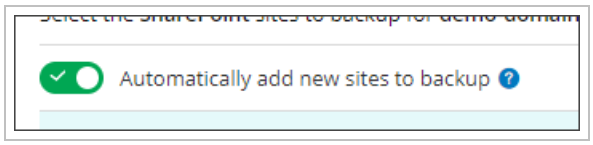


9. Click **Next** to continue

10. View the **SharePoint** sites found in the domain and select the required data to backup



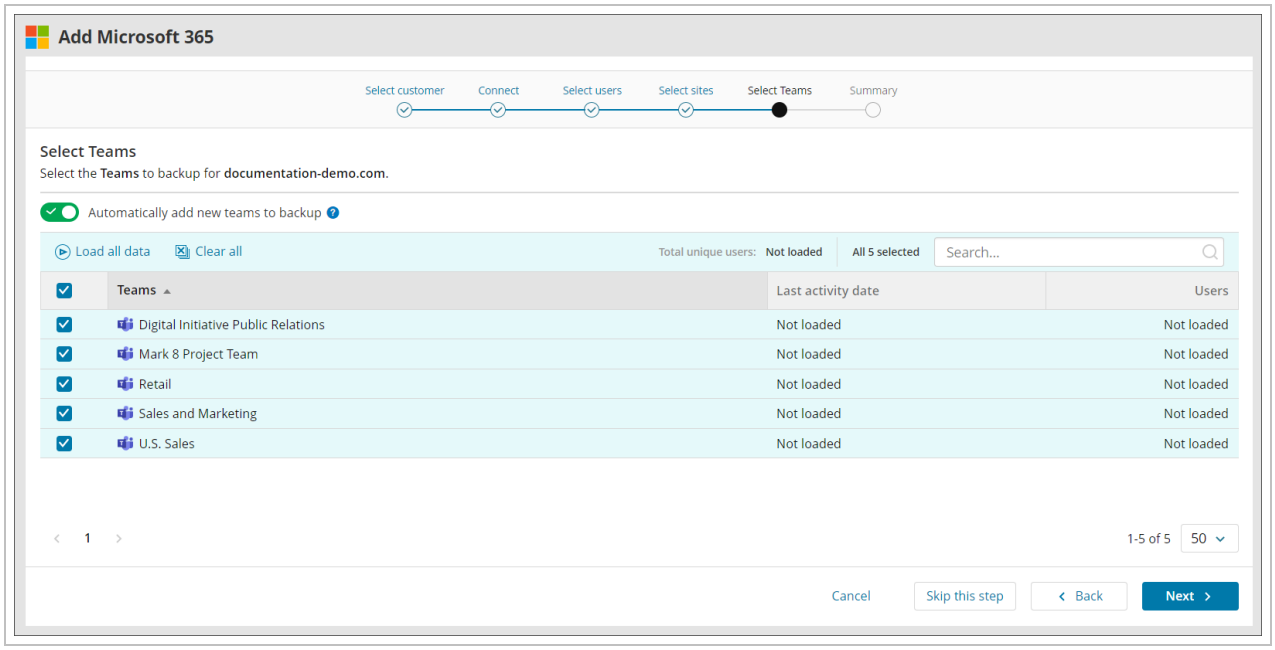
a. Enable the **Automatically add new sites to backup** if you wish to allow sites discovered during a backup to be added to the backup selection



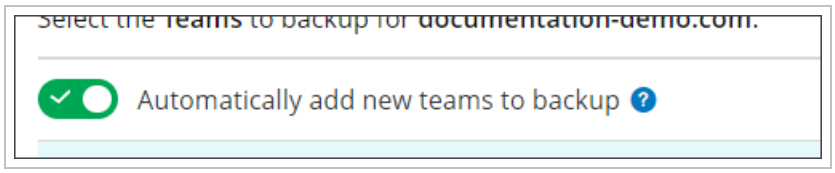
11. Click **Next** to continue

> If you are not adding **SharePoint** sites to the backup selection, click **Skip this step**

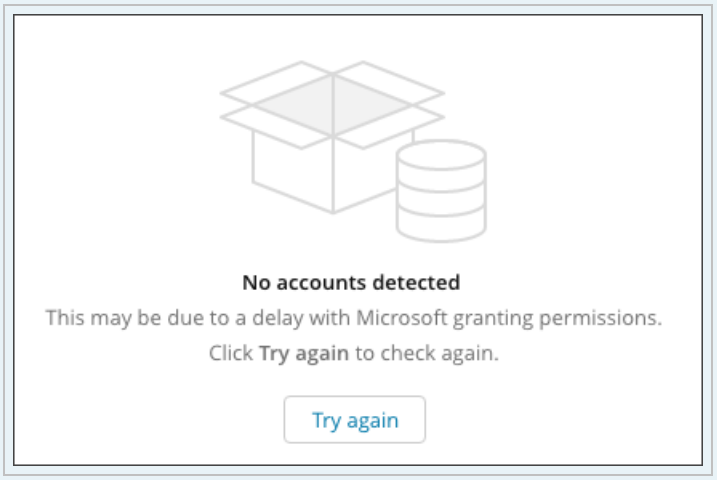
12. View the **Teams** sites found in the domain and select the required data to backup



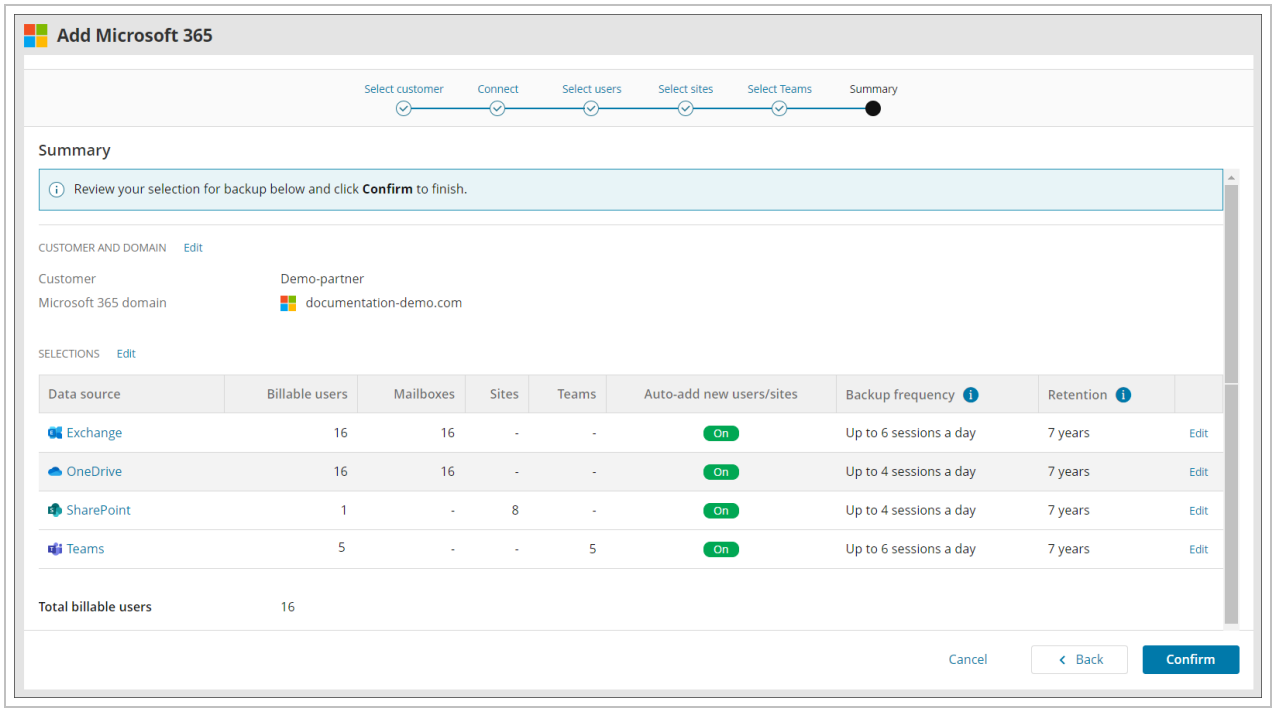
a. Enable the **Automatically add new teams to backup** if you wish to allow teams discovered during a backup to be added to the backup selection



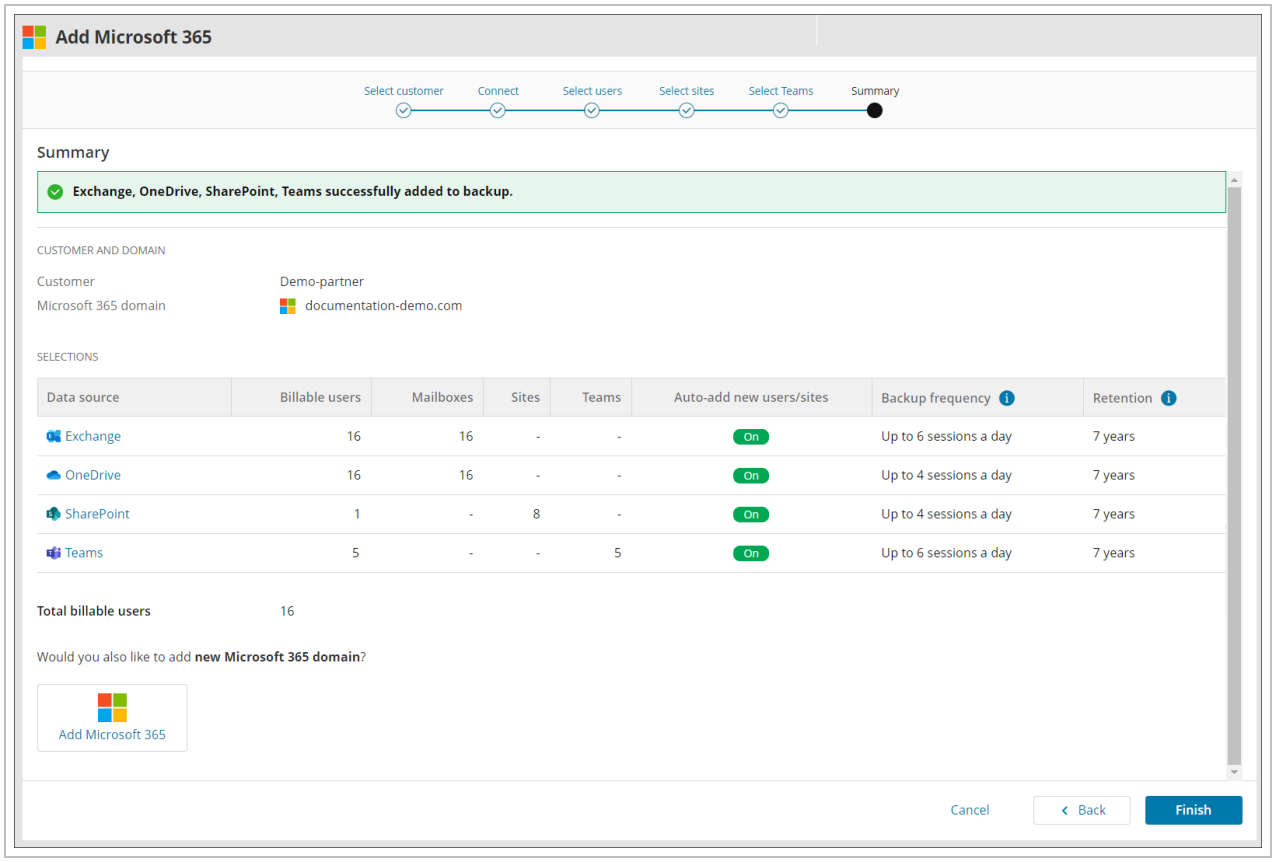
In cases where no users, sites or teams channels show when adding a device, click **Try again** to check again.



13. Review and **Confirm** the backup selection that has been made - use the **Edit** links to make changes if required



14. Once confirmed, the domain or service with your selection has been successfully added - If you do not wish to add other services now, click **Finish** and you will see the device added to your list of devices



> You can add further services by clicking the **Add Microsoft 365 device** button to the right of the **Summary** dialog or by editing the current domain's backup selection.

Microsoft 365 Teams: What Is/Is Not Included

Due to the constraints of Microsoft 365, it is important to note what can and cannot be backed up and restored for the Teams service.

What's included

- Teams
- Team member settings
- Channels in the Teams
- Messages in the Channels
- Attachments in the Channels (Private, Public and Shared)
- Embedded pictures in the Channels (Gifs and Pictures)

What's not included

- General channel settings
- Deleted channels
- Guest users in channels

- Tags and Apps in Teams
- Personal and Group chats
- Files in personal chats
- Reactions
- Wiki
- Meeting notes
- Meeting recordings

> In order to restore Files from groups or chats, this must be done via the Microsoft 365 SharePoint service. These **cannot** be restored individually via the Teams service.

Manage Microsoft 365 domains

Searching and Filtering

Users of all roles can view Microsoft 365 domains present in the Management Console. They appear next to regular Backup Manager devices in **Backup > Dashboard**.

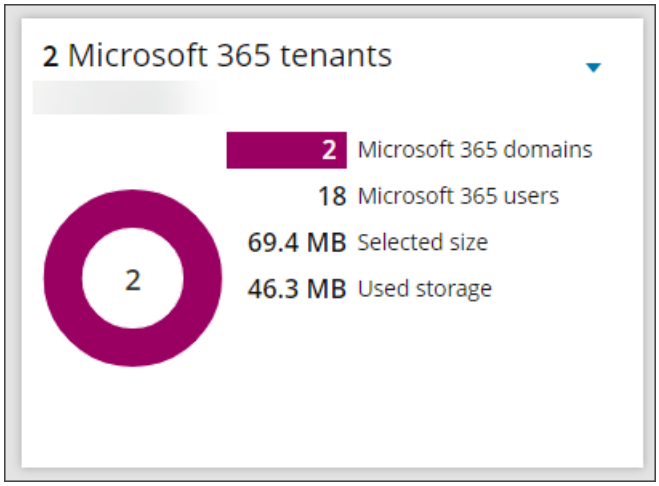
There are several ways to display only Microsoft 365 domains:

1. Widgets
2. Searching
3. Filtering

Widgets

To display only Microsoft 365 devices using the widgets:

1. Expand the widgets at the top of the Dashboard
2. Click **Microsoft 365 domains** on the Microsoft 365 widget



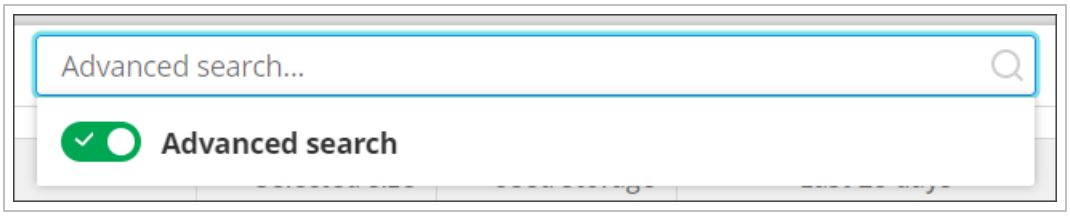
3. Click on a domain name to view the Domain's property tabs

The list of devices will automatically update to display only Microsoft 365 domains belonging to the customer selected.

Searching

To search for Microsoft 365 domains:

1. Use the **Search** bar to the top right of the devices list
2. Enable Advanced searching by clicking the toggle



3. Use the Type shortcode of `AT` and the value of `2` to search for devices with the **Account Type of Microsoft 365**

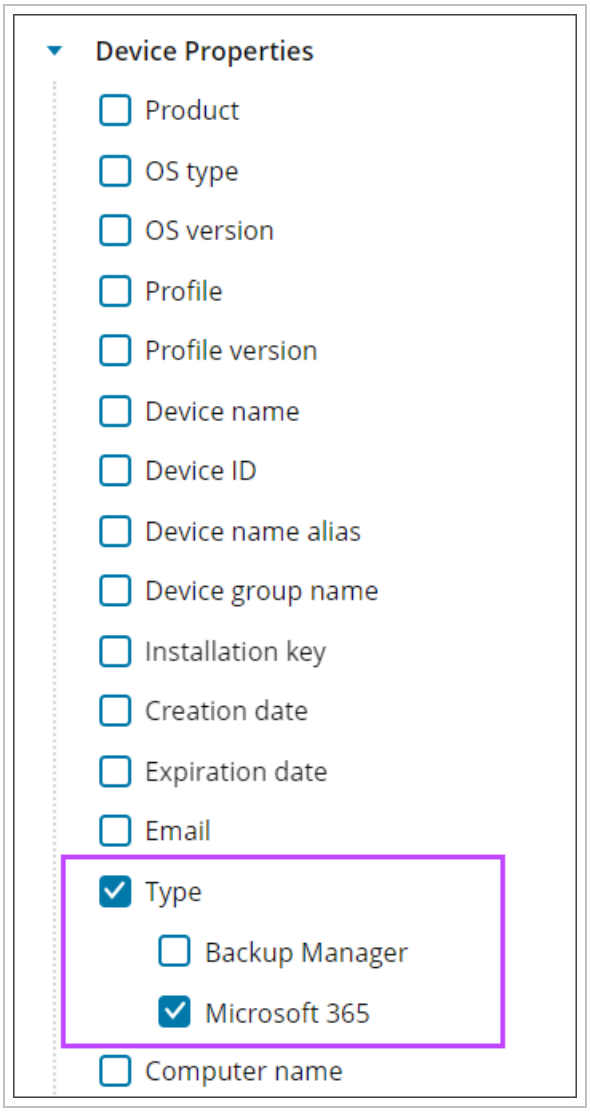
> Full details on Advanced searching and the syntax and column codes to use can be found on Searching in Management Console

4. Hit **Enter**
5. Click on a domain name to view the Domain's property tabs

Filtering

To filter for Microsoft 365 domains:

1. Use the **Filter** panel to the left of the devices list, this can be expanded or collapsed by clicking the two arrows (>>/<<)
2. Under the Device Properties section, select the **type** filter
3. Tick **Microsoft 365**



4. The devices list will automatically update to display the list of devices meeting this criteria
5. Click on a domain name to view the Domain's property tabs

> For full details on filtering, see the Filtering Devices in Management Console page for full details.

Export Protected Users

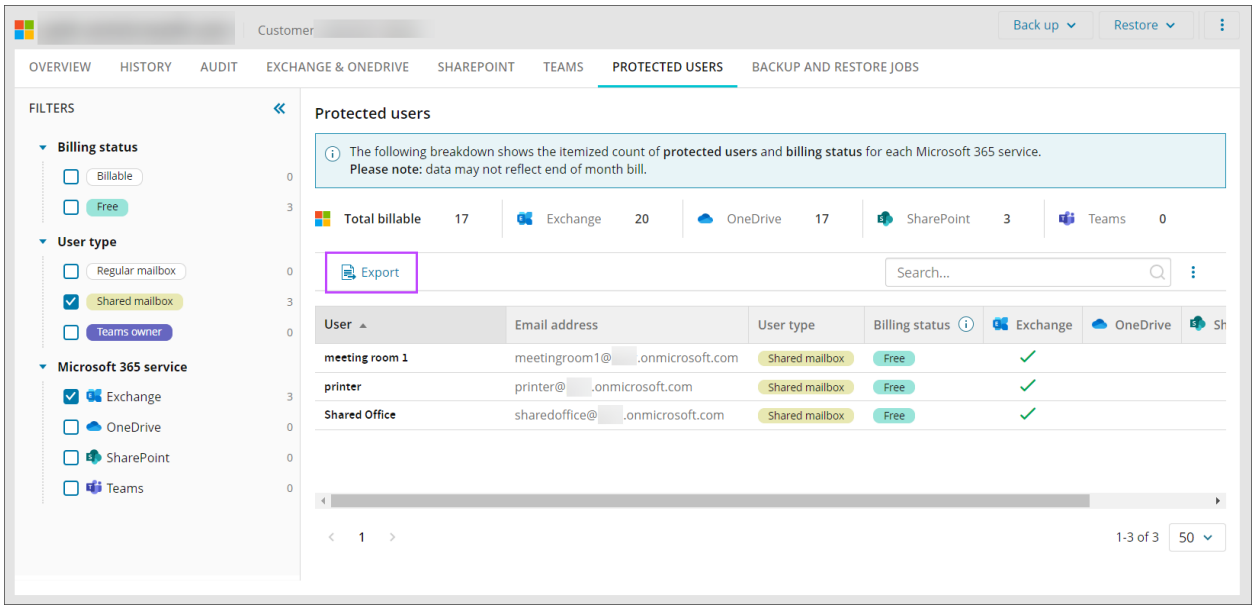
You can export a list of **protected users** from the Management Console to a spreadsheet in either .xlsx or .csv file formats.

> Export files created by the Console contain **all the data** that is currently displayed in the **protected users** table. If the data spans across multiple pages, all the pages are exported.

1. From the protected users tab apply any filters or searches to limit the list of users displayed

   > For example using the **User Type** filter to show only Shared mailboxes

2. Click **Export** from the Toolbar



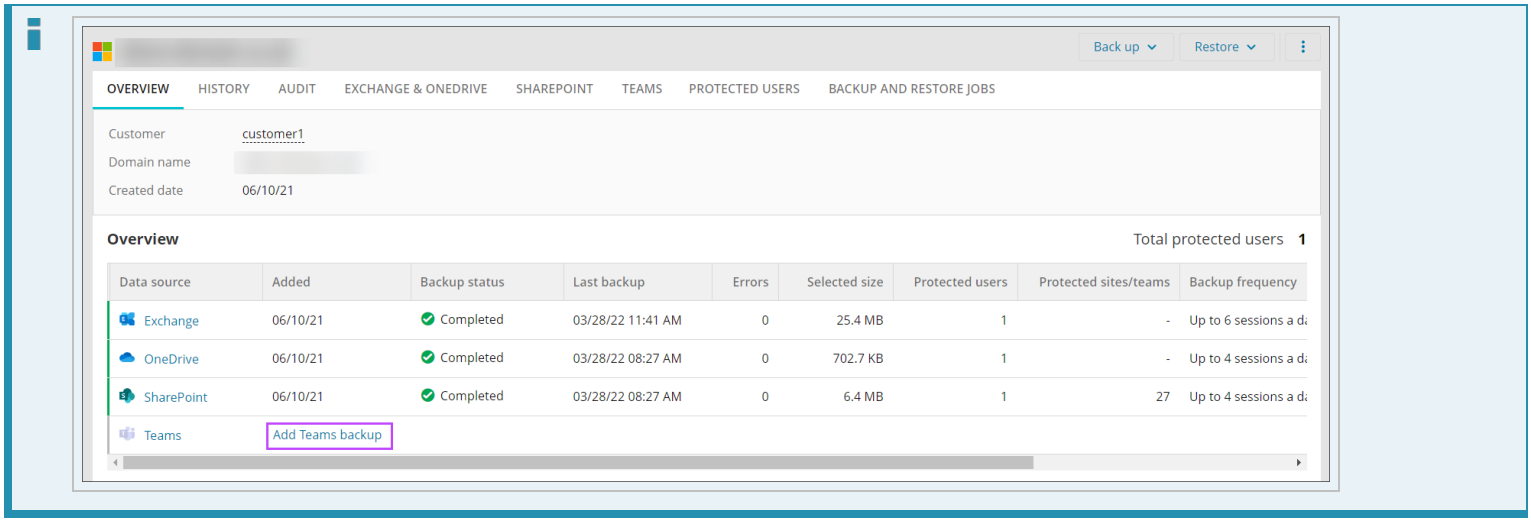
3. Select the file format from:
   - XLSX
   - CSV
4. Click **Export**

   The report will then be generated and downloaded

Manage backup selection

When looking at the domains properties, select either the **Exchange & OneDrive**, **SharePoint** or **Teams** tab to view all mailboxes, accounts or sites present in the domain.

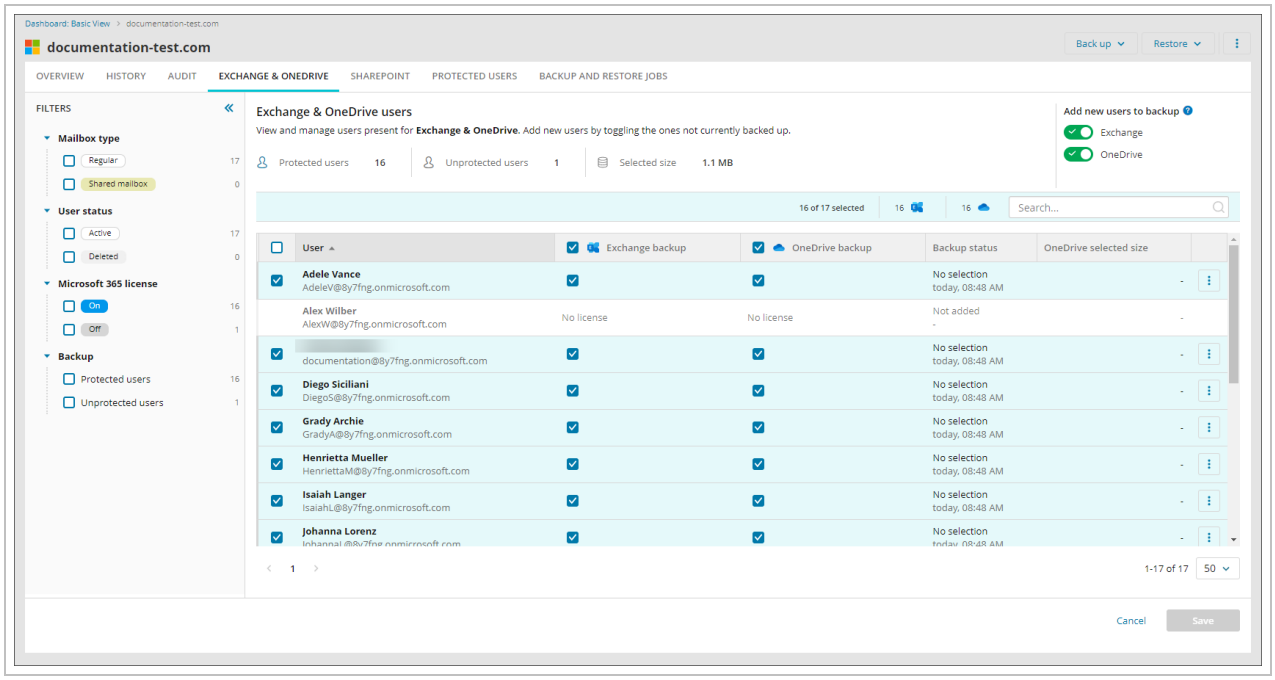
> Selecting a tab where no data source has been configured for backup will resent you with the option of adding a new data source



Exchange & OneDrive

You can also **Add new users, sites or teams to backup** automatically using the toggle switches at the top right corner of the tab;

Toggle State	Result
On	newly added users/sites/teams will be added to the backup selection automatically
Off	newly added users/sites/teams will appear in the list but will not added to the backup selection



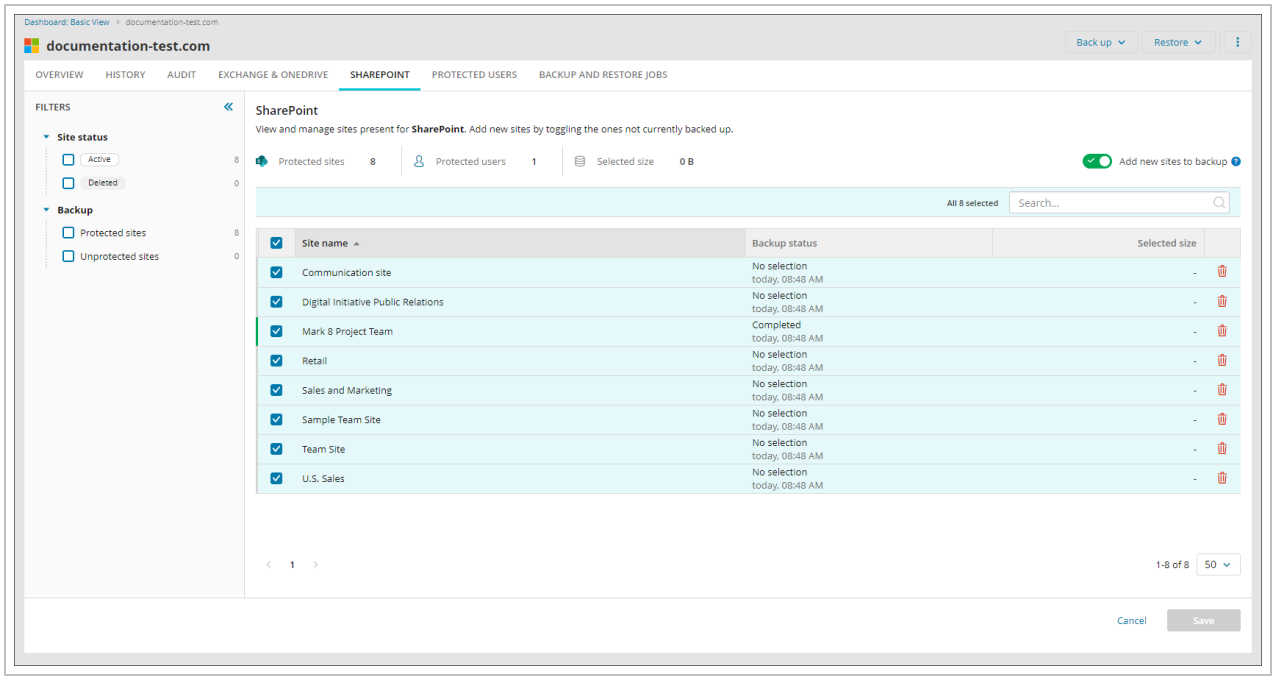
You can filter the displayed list by using the **Filters** on the left of the display, filtering on the Mailbox Type of **Regular** or **Shared**, User Status of **Active** or **Deleted**, Microsoft 365 license **On** or **Off** and Backup **Protected** or **Unprotected** users.

> Unlicensed users will show in the list as greyed out. This is to show which mailboxes or accounts cannot be selected for backup due to not being correctly licensed.

SharePoint

You can also **Add new users, sites or teams to backup** automatically using the toggle switches at the top right corner of the tab;

Toggle State	Result
On	newly added users/sites/teams will be added to the backup selection automatically
Off	newly added users/sites/teams will appear in the list but will not added to the backup selection

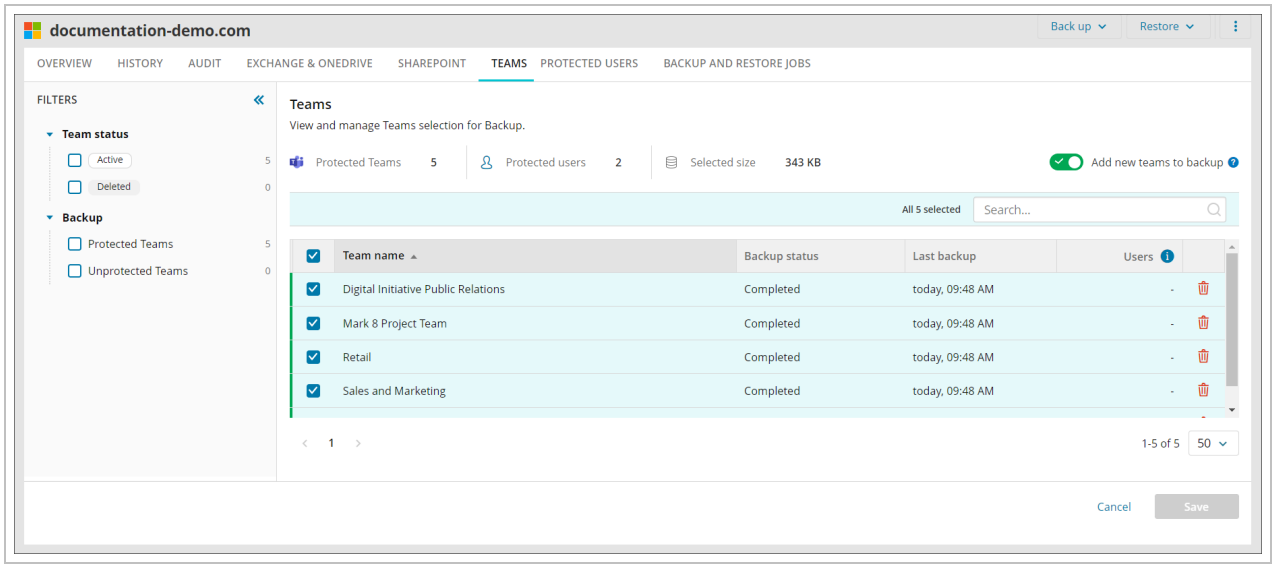


You can filter the displayed list by using the **Filters** on the left of the display, filtering on the Site Status of **Active** or **Deleted** and Backup **Protected** or **Unprotected** sites.

Teams

You can also **Add new users, sites or teams to backup** automatically using the toggle switches at the top right corner of the tab;

Toggle State	Result
On	newly added users/sites/teams will be added to the backup selection automatically
Off	newly added users/sites/teams will appear in the list but will not added to the backup selection



You can filter the displayed list by using the **Filters** on the left of the display, filtering on the Teams status or backup data.

Add data to Backup

In here, you can add new accounts or sites for backup by ticking the ones not currently backed up. You may look for the specific account using the search bar and filter the output using the left hand tool bar.

You may also enable or disable '**Automatically add new accounts to backup/Automatically add new sites to backup**' by toggling the on/off slider.

> After making any changes, you must click **Save** at the bottom of this dialog box or changes will be lost.

Delete Backups

You can delete backups made by searching for the account or site you wish to remove then clicking the trash can icon towards the right hand side of the screen. Doing this will remove the account from the backup schedule and will remove all backup history on the device for this account.

You will be prompted to confirm that you wish to proceed.

Deleting data can take up to 30 days.

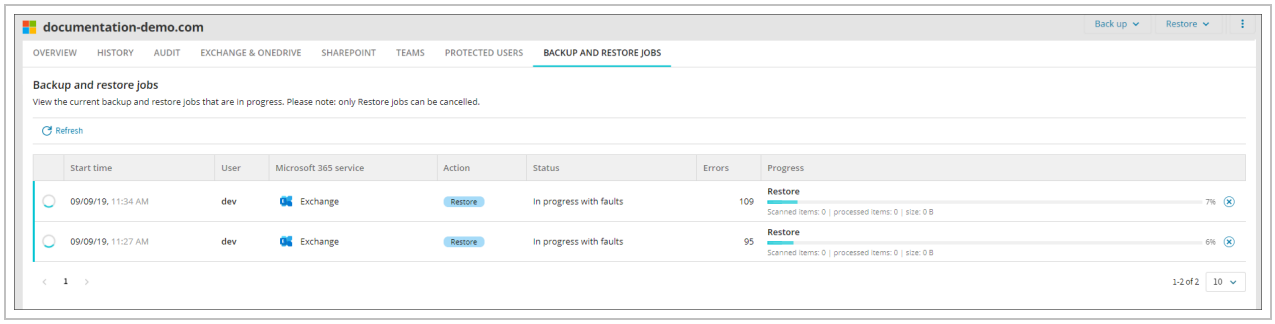
> After making any changes, you must click **Save** at the bottom of this dialog box or changes will be lost.

> It will not be possible to recover previously backed up data from any mailbox, account or site which has since been removed from the N-able Cloud

This is only available to Management Console users with Security Officer permissions, all other users will not see this option.

View backup and restore job queue

To view the current backup and restore sessions that are in progress, these can be found in the **Backup and Restore Jobs** tab. The tab itself will also indicate how many jobs are active by showing a badge in the tab header. Beneath the progress bar you can also see the number of scanned items, processed items and size of the backup.

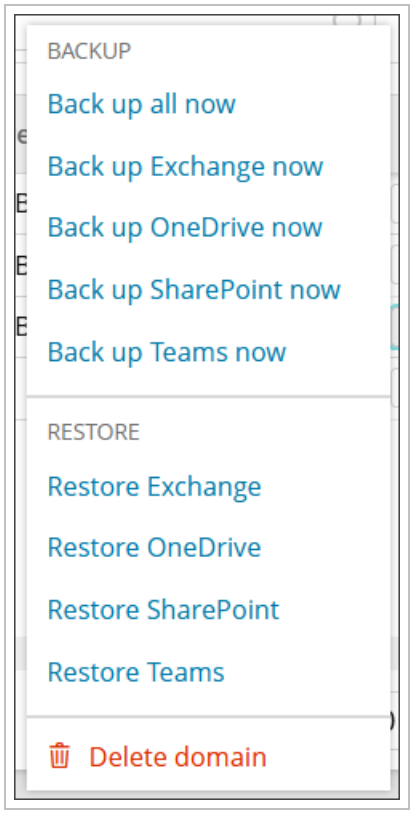


Backup jobs cannot be canceled but restore jobs can by clicking the **cancel** button in the **Actions** column.

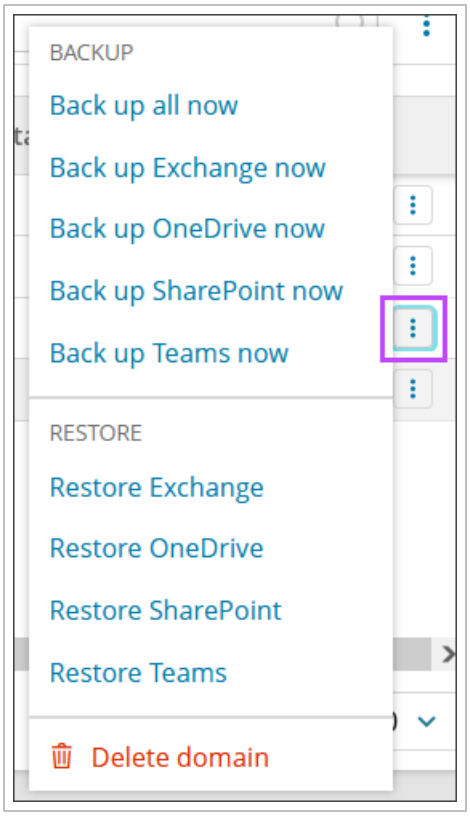
Actions for domains

The action menu for Microsoft 365 domains can be accessed in a number of different ways:

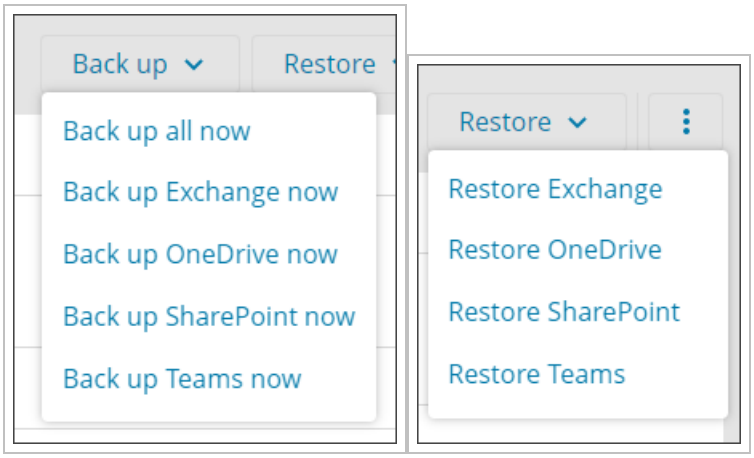
1. On the BackupDashboard, right click the domain to view the action menu



2. On the BackupDashboard, scroll to the far right-hand side of the devices list and click the three vertical dots to view the action menu



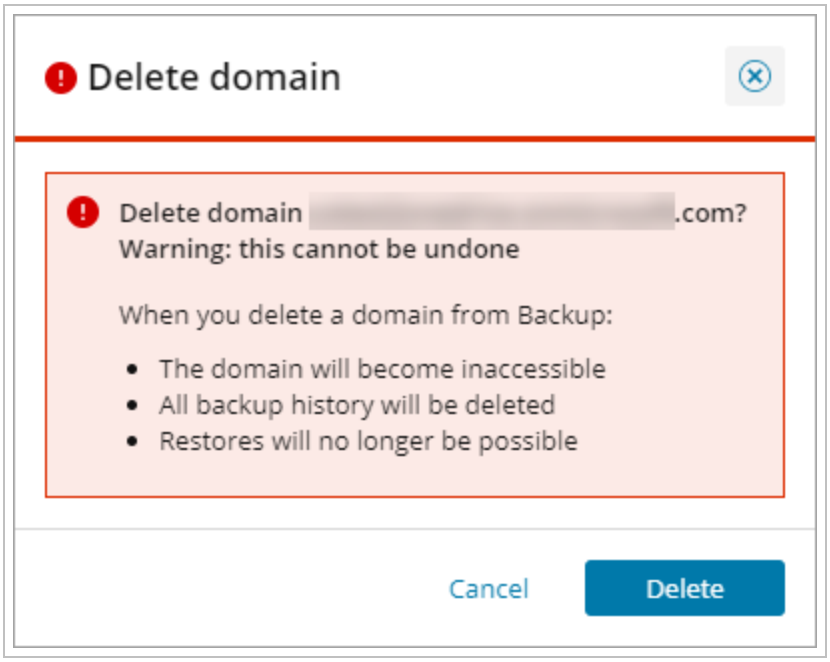
3. Click the Domain name to open the domain overview and use the **Back up** and **Restore** menus in the top right corner



The **action menus** for Microsoft 365 domains have up to 8 items depending on services configured for the domain:

- **Back up all now** (initiates an unscheduled backup for all services)
- **Back up Exchange now** (initiates an unscheduled backup for Exchange)
- **Back up OneDrive now** (initiates an unscheduled backup for OneDrive)
- **Back up SharePoint now** (initiates an unscheduled backup for SharePoint)

- **Back up Teams now** (initiates an unscheduled backup of Teams)
- **Restore Exchange** (lets you restore selected Exchange items)
- **Restore OneDrive** (lets you restore selected OneDrive items)
- **Restore SharePoint** (lets you restore selected SharePoint items)
- **Restore Teams** (lets you restore selected Teams items)
- **Delete domain** (the domain is deleted from the Console and all its backup data is cleared from the N-able cloud with **no possibility** of recovery)



Microsoft 365 Domain Properties

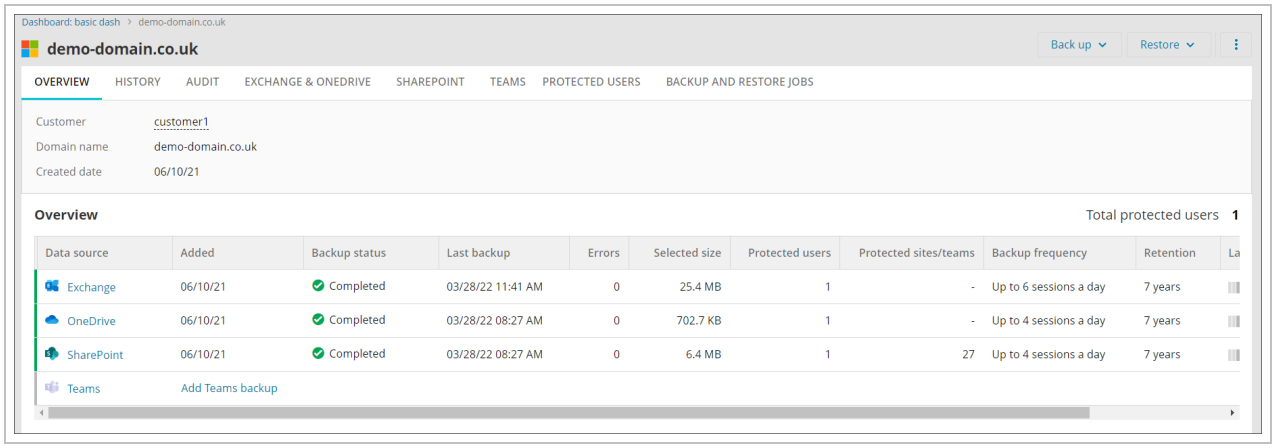
Once the **Domain Properties** windows is open, the different tabs will provide you with the relevant information.

View Overview

On the **Overview** tab, you can check the account statistics for the services added to the domain.

In here, you will have the opportunity to change the customer that the domain belongs to.

To add new services, follow the Add Microsoft 365 domain steps for the relevant service in the **Enable Backups** page.

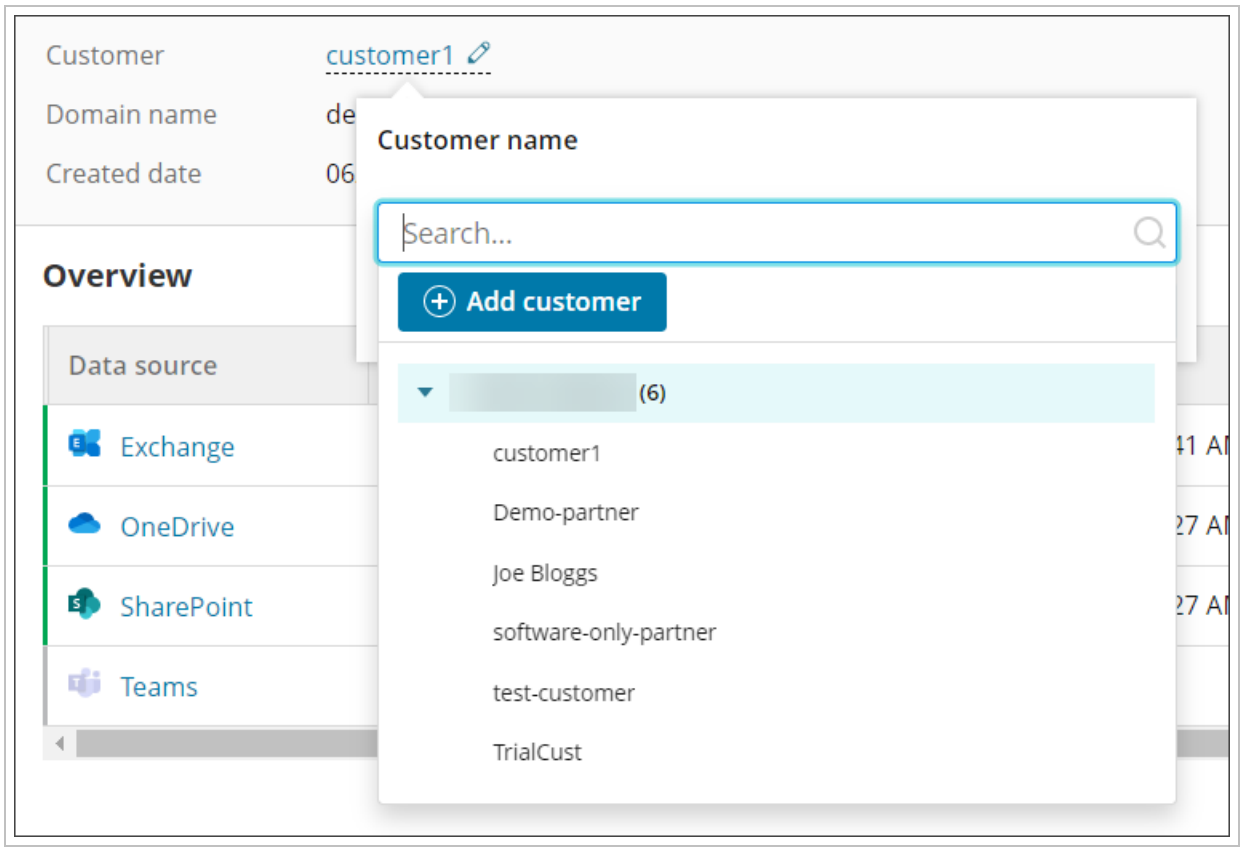


- You can also add a service from the **Overview** tab if one has not yet been added
- You can also use the 3 dots menu to the right of each entry to delete the data source from Backup (2 or more data sources must be configured for this option to be available)

Change Customer

The customer a domain belongs to can be changed by:

1. Click the customer name

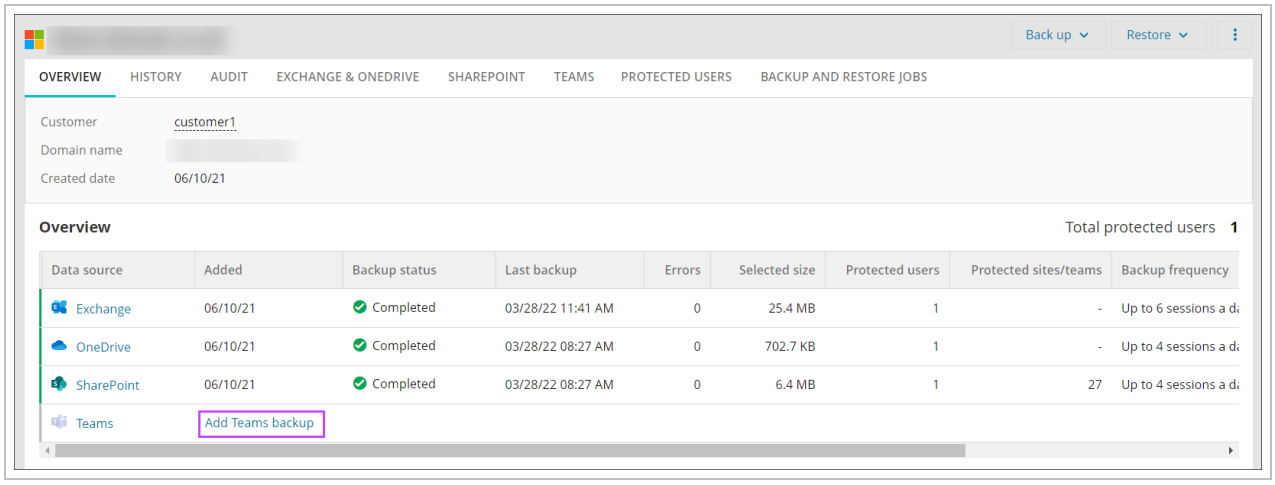


2. Select the new customer from the dropdown or add a new customer by clicking **Add**
3. Click **Save**

Add Services

To add new services either:

1. Add it using **Add *Service Name*** from the Device **Overview** tab



Or

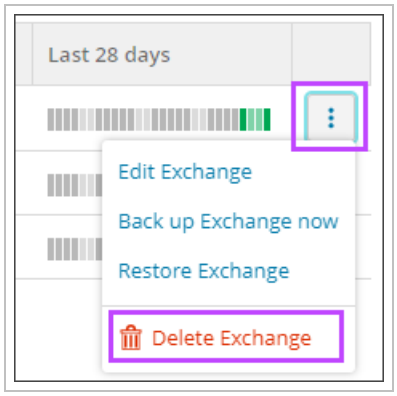
2. Follow the Add Microsoft 365 domain steps for the relevant service in the **Enable Backups** page

Remove Services/Delete Backups

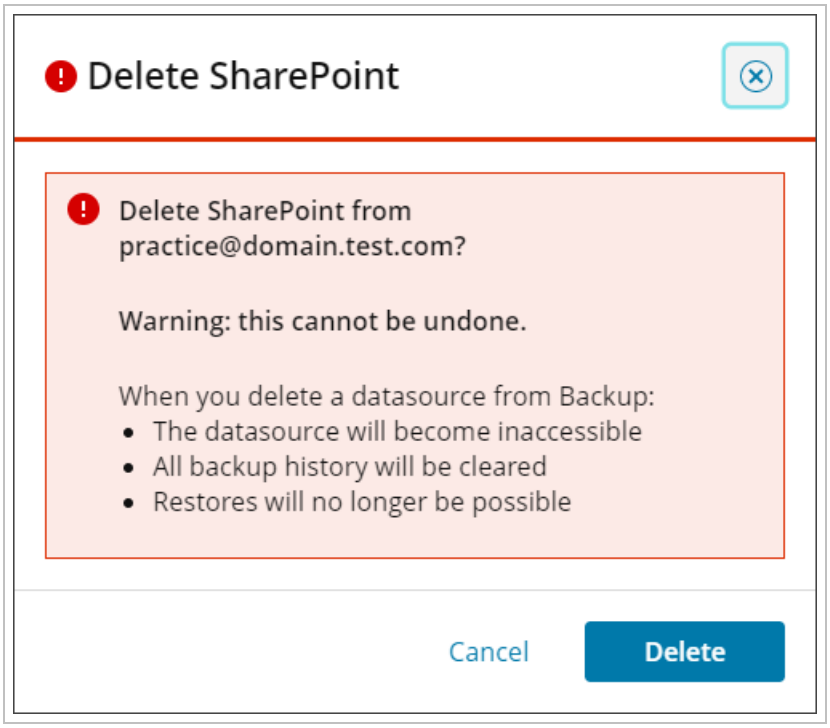
> This is only available to Management Console users with **Security Officer** permissions, all other users will not see this option.

To remove a service and delete the backups for this service,

1. Click the three dots to the right of the service to open the **Action Menu**



2. Select **Delete** ***Service Name***

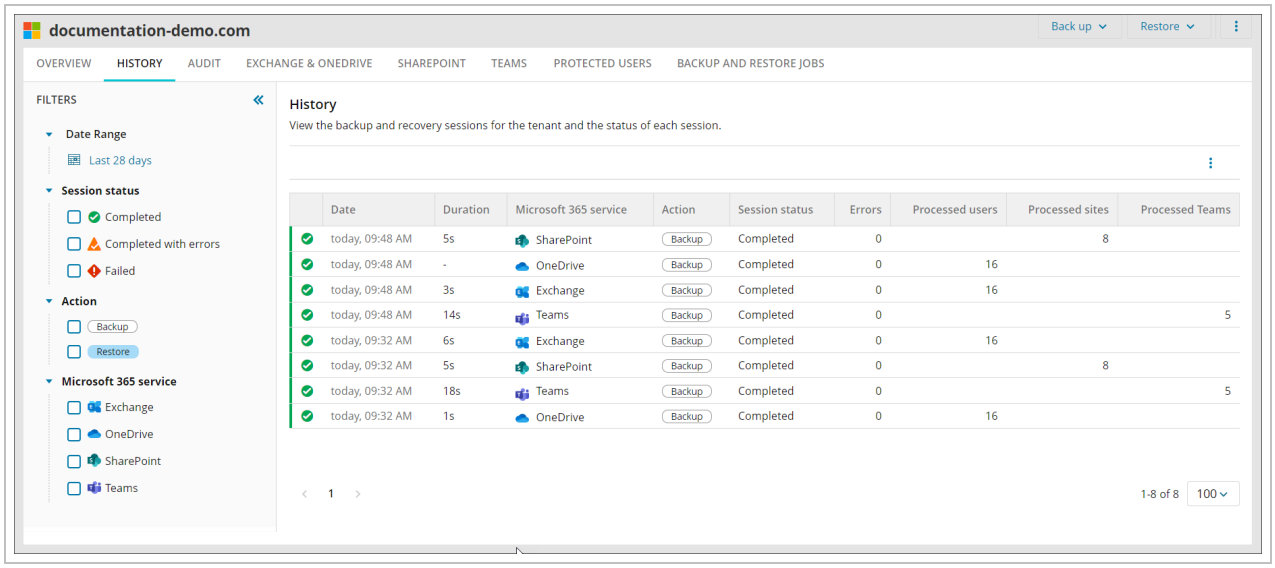


Deleting data can take up to 30 days.

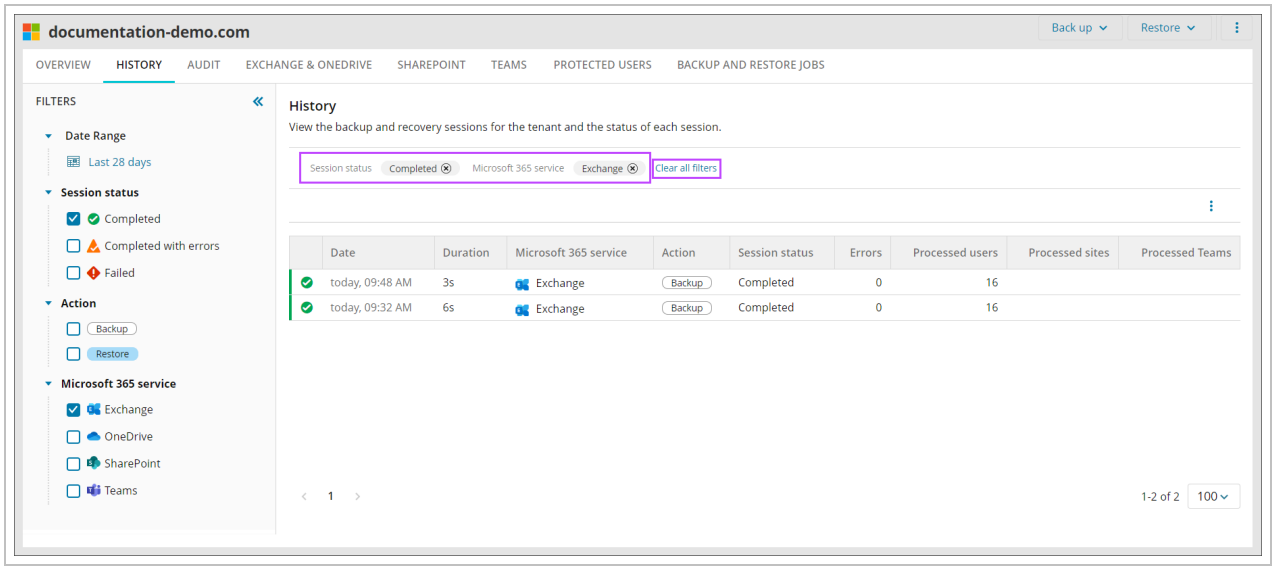
It will not be possible to recover previously backed up data from any mailbox, account or site which has since been removed from the N-able Cloud

History

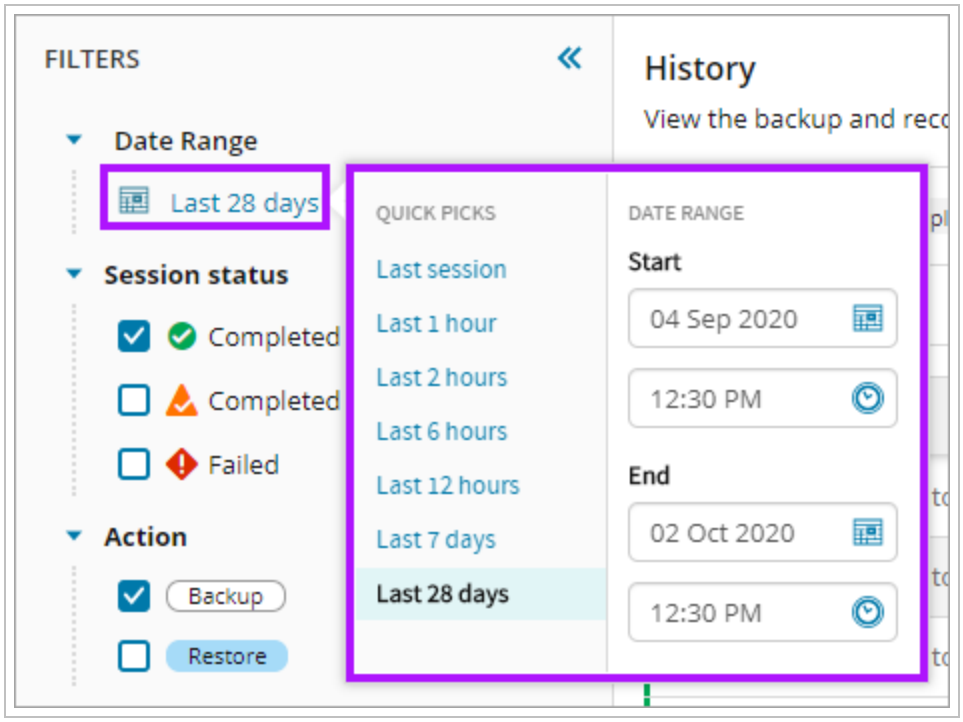
The **History** tab will provide you with a list of the backup and recovery sessions for this device, what data source they are for and the status of this backup session.



The list of historical events can be filtered using the filter options on the left hand side - as each filter is configured, you will see filter chips across the top of the results. Click 'x' in the chip to remove that filter item, or to remove all filters, click **Clear all filters**.

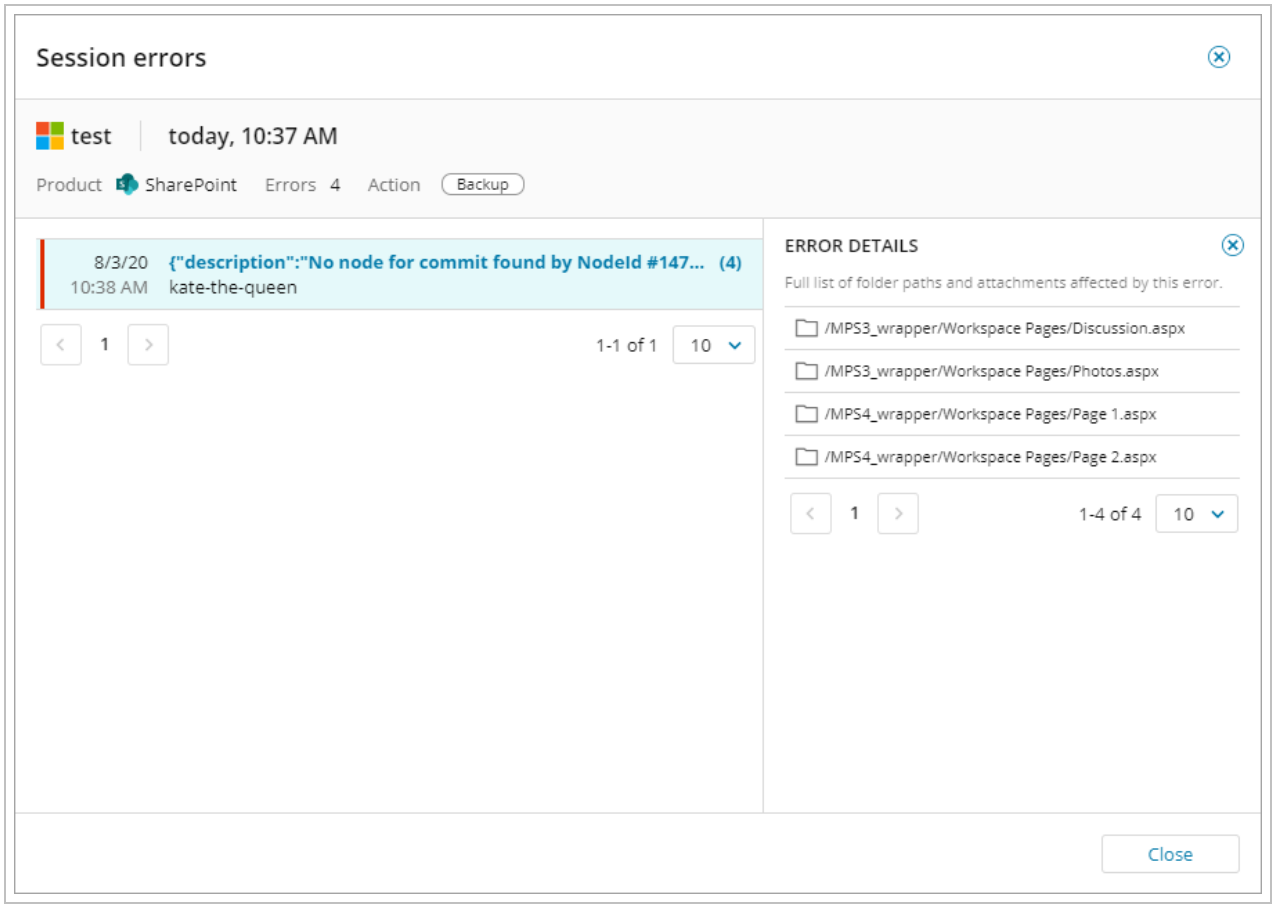


The date range filter item allows selection of default or custom ranges.



Errors Column

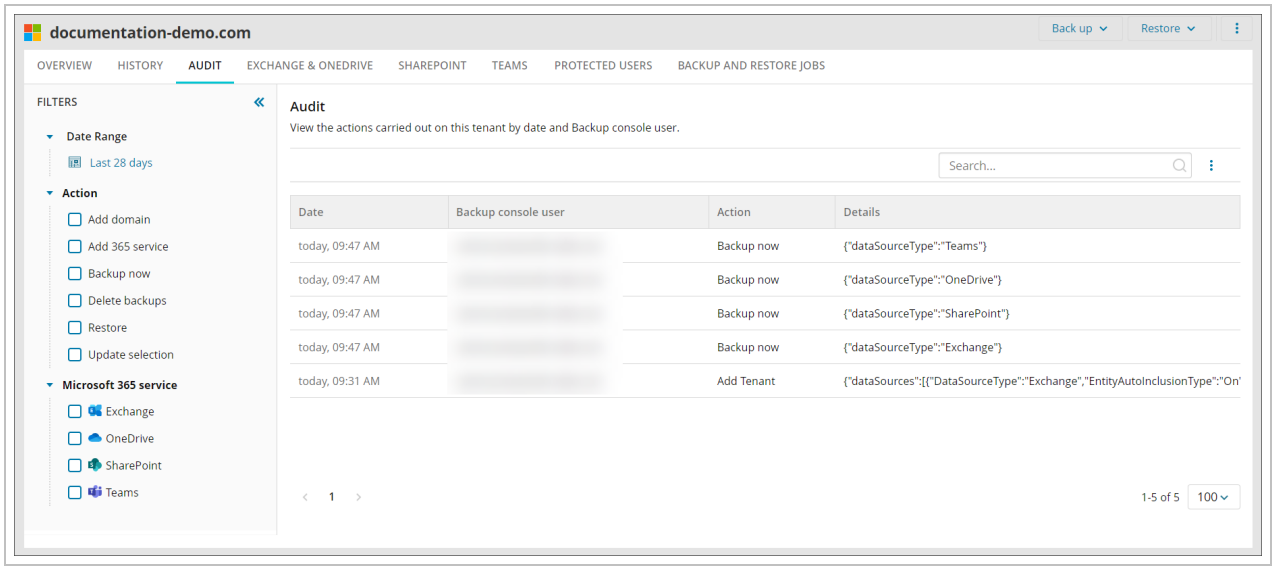
In the **Errors** column of the **History** tab, you can click the errors count (if it is over 0) to open the **Session errors** dialog, which details the errors encountered during the backup itself - these may aid with any troubleshooting of the issue.



Error information given here will be required by support in cases where you contact them for assistance.

Audit

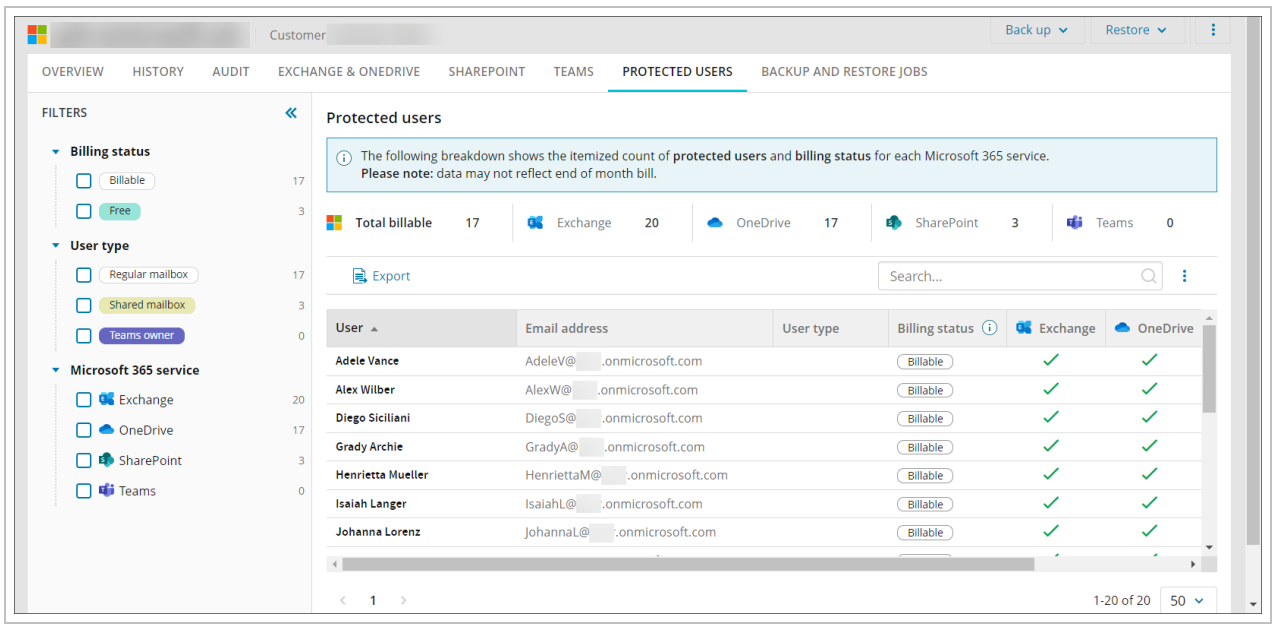
You can check the **Audit** tab to see which user account has been used to carry out actions on the domain.



In here you will be able to see which user account created the domain, added or removed services, amended backup selections, started restores and deleted backup history.

Protected Users

On the **Protected users** tab, you can view a full list of all protected users, how many of these users are billable and the services protected for these users.



This tab is read-only, but filtering is available on the left hand banner to select which services and types of users you wish to view.

- Where there is a backup for an **Exchange** user it will be counted as a **Billable User**
- Where there is a backup for a **OneDrive** user it will be counted as a **Billable User**
- **SharePoint** users detection: the public Microsoft API is utilized to gain information about users on the selected **SharePoint site collections**. If a user has never logged into the site collection, or had never been referenced in the site collection in some other fashion, then that user will not appear in the console list
- Where every **unique owner** of a team will be counted as a **Billable User**

Export Protected Users

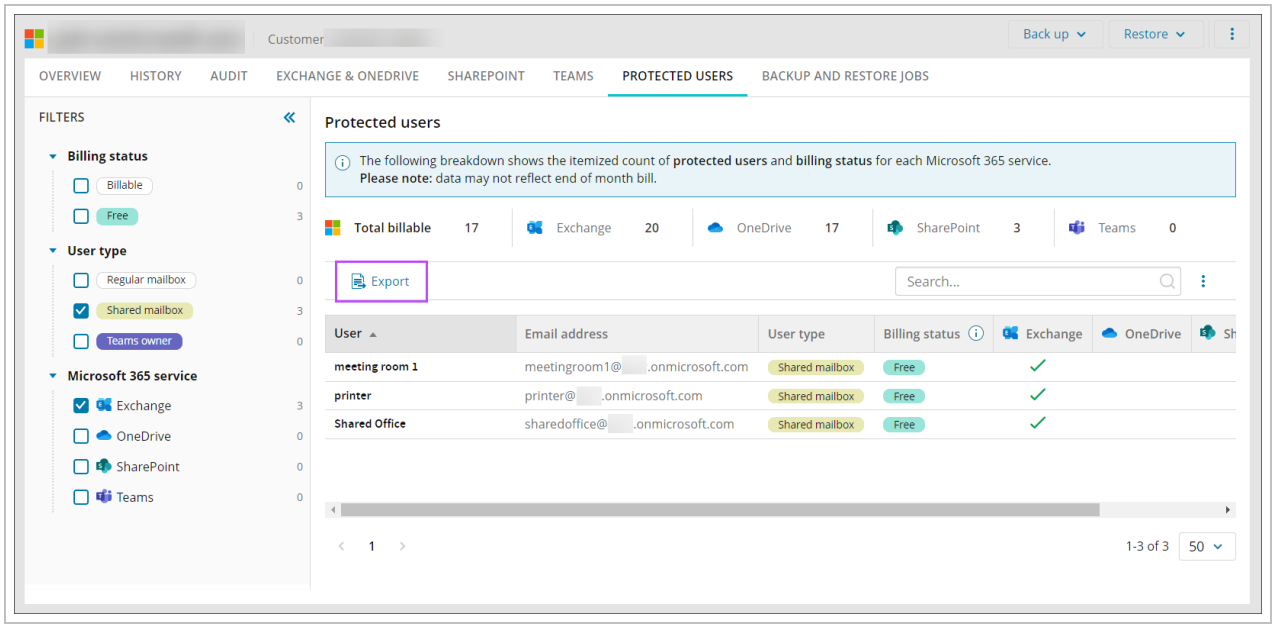
You can export a list of **protected users** from the Management Console to a spreadsheet in either .xlsx or .csv file formats.

> Export files created by the Console contain **all the data** that is currently displayed in the **protected users** table. If the data spans across multiple pages, all the pages are exported.

1. From the protected users tab apply any filters or searches to limit the list of users displayed

   > For example using the **User Type** filter to show only Shared mailboxes

2. Click **Export** from the Toolbar



3. Select the file format from:
   - XLSX
   - CSV
4. Click **Export**

   The report will then be generated and downloaded

Restore Microsoft 365 Data

For detailed steps on restoring date for each of the Microsoft 365 services, select the appropriate service below. Before you begin, ensure you have met the necessary requirements:

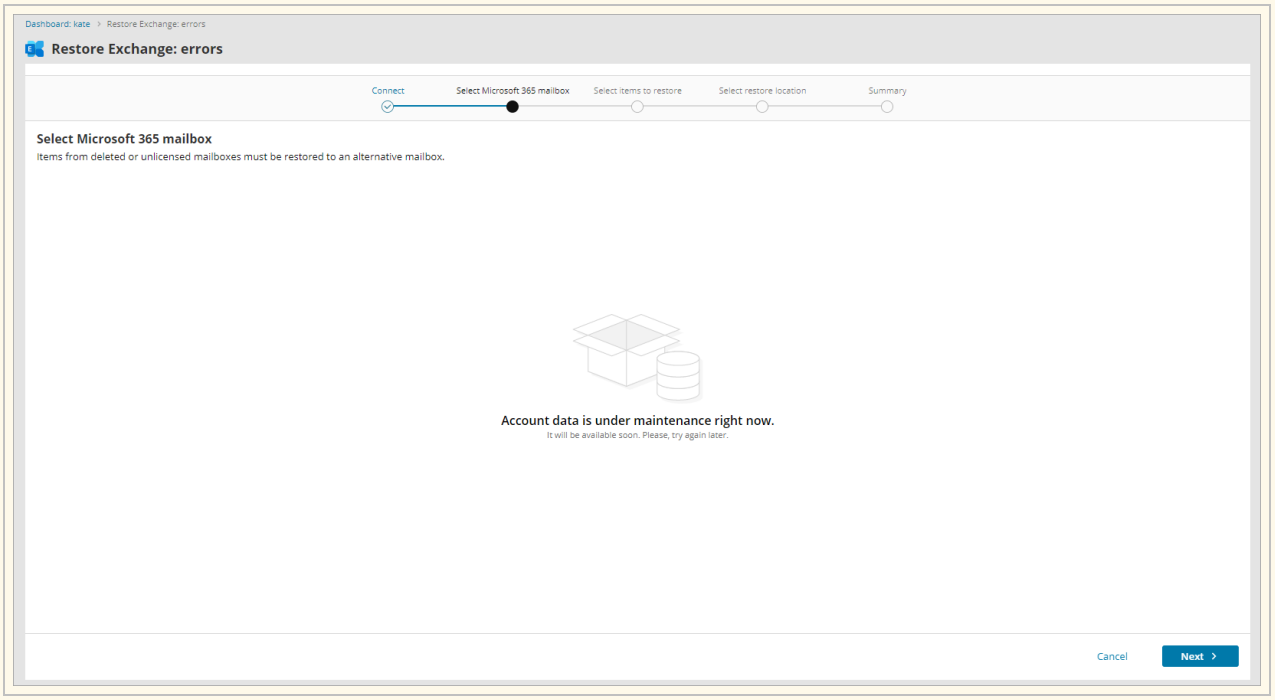
Requirements

The following account types are required:

- A **SuperUser** account for the Management Console (for adding domains and initiating backups and restores)
- A Security Officer role (for initiating a restore)
- A **Global administrator** account for Microsoft 365

> To restore data to a newly created Exchange mailbox or OneDrive account you have to login at least once to the created mailbox/account

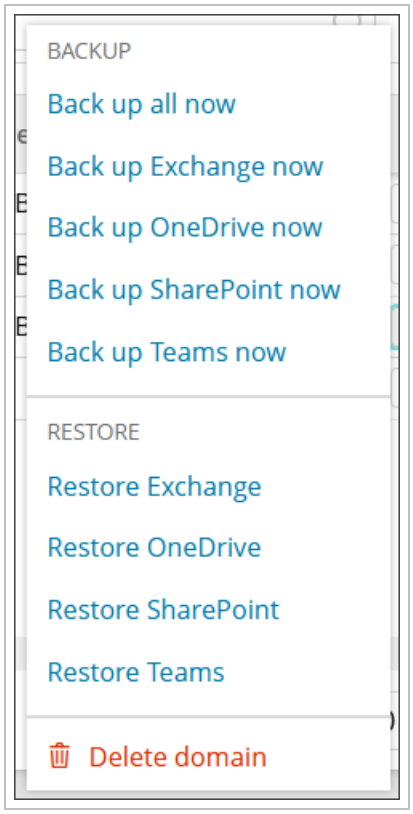
> N-able may perform maintenance on the account data to improve performance. The duration of such maintenance is expected to be short and the restore will available shortly.



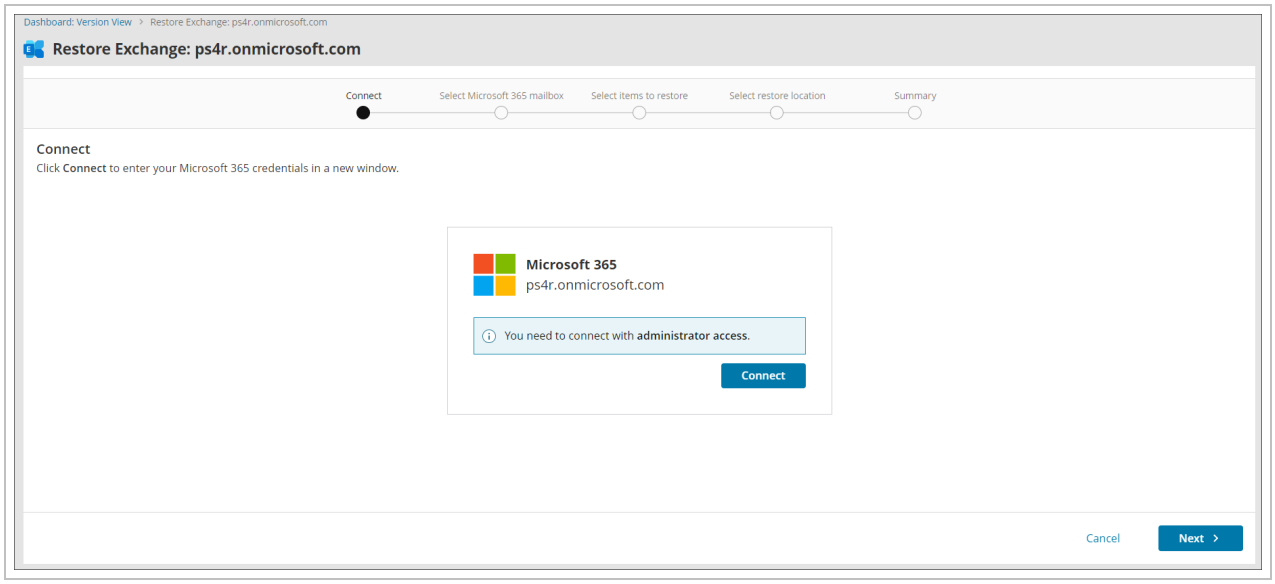
Instructions

Exchange

1. Log in to the Management Console under a SuperUser account
2. Open the action menu for the domain and click **Restore Exchange**

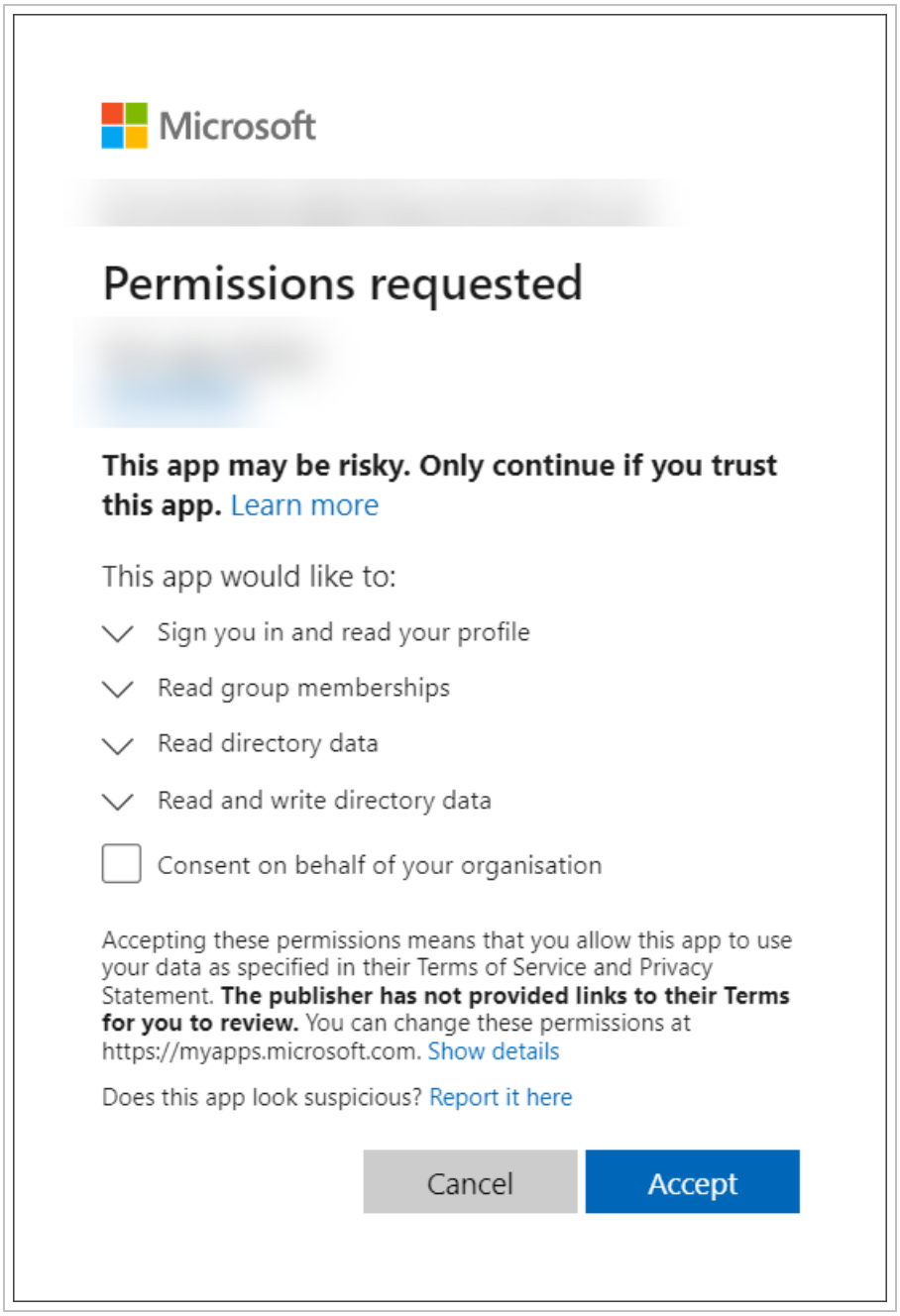


3. Connect to the Microsoft 365 Exchange domain with administrative account credentials

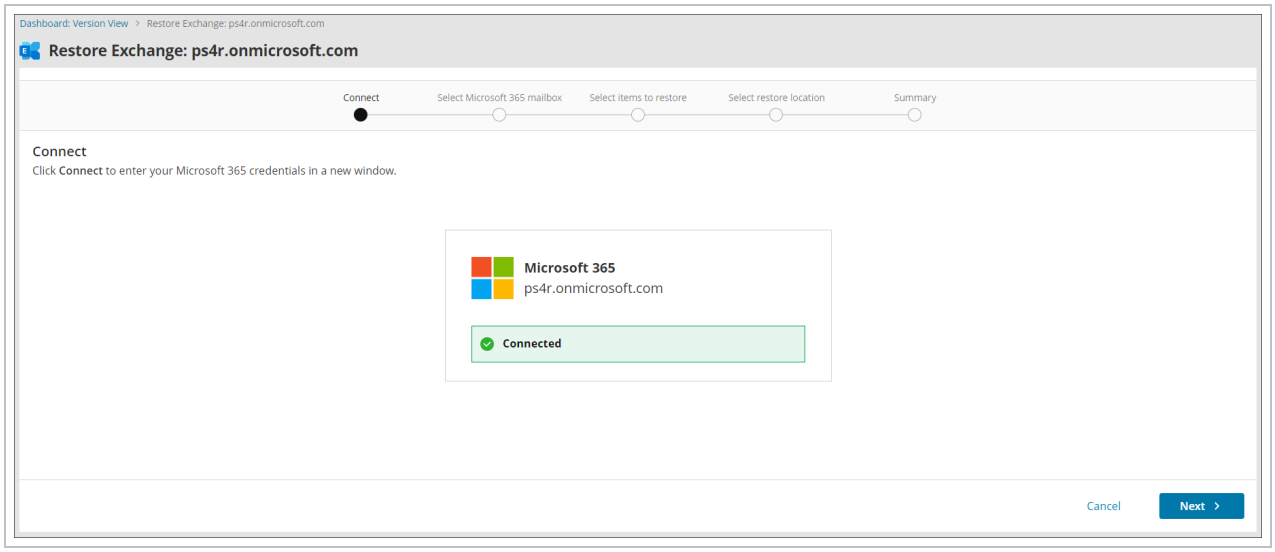


If you do not see the authentication page, make sure your browser is not blocking **pop-up windows**.

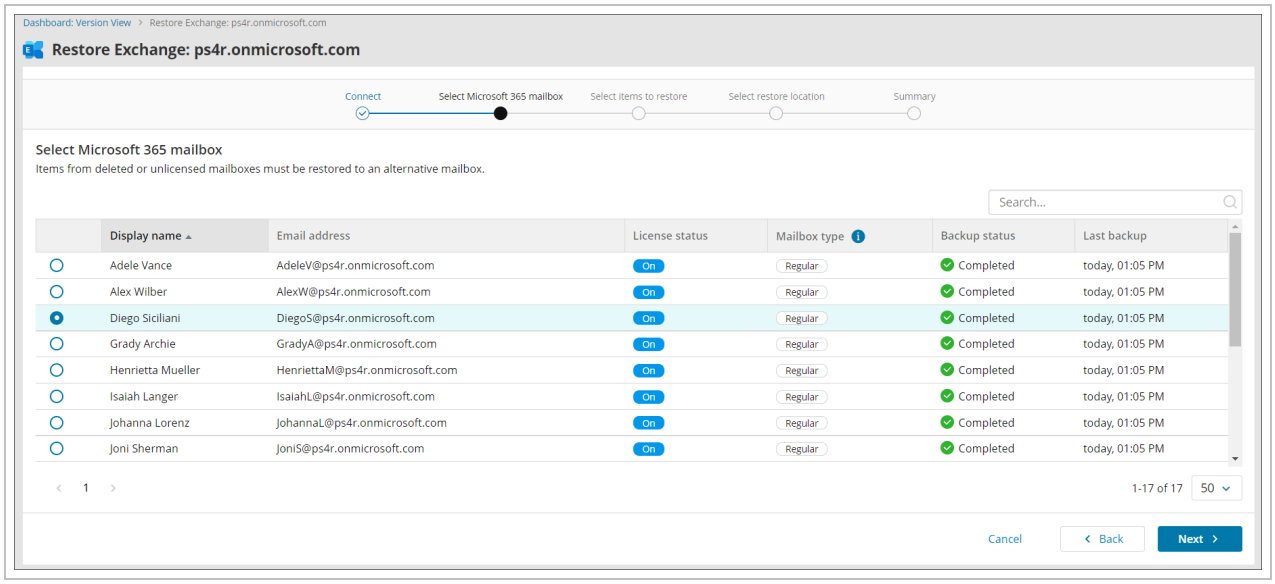
4. Accept the required permissions



5. You will receive a confirmation that the connection has been successful for the restore



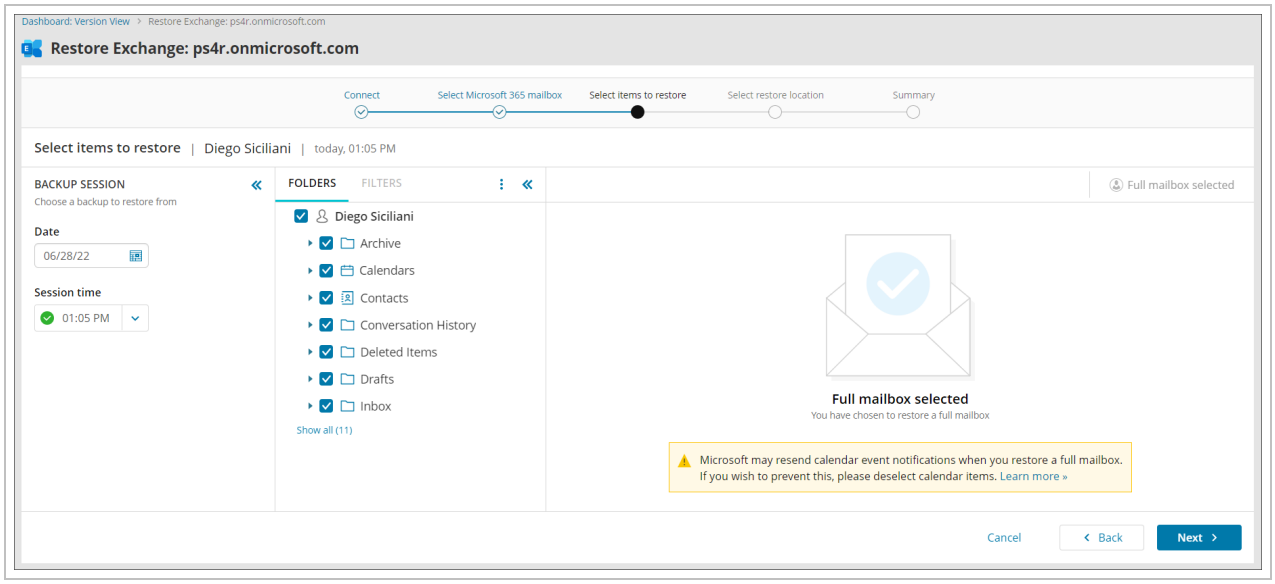
6. Select the mailbox you wish to restore items from. You will see the list of backed up mailboxes and their types (Regular, Shared and Deleted)



7. Select the backup session you wish to restore from

8. Select the data to restore and click **Next**
   a. From the Folders tab:
      - Whole mailbox (by ticking the mailbox name)
      - Calendars
      - Contacts
      - Deleted items
      - Drafts
      - Inbox
      - Junk Email
      - Outbox
      - Recoverable items
      - Sent items

> Microsoft may resend calendar event notifications when you restore a full mailbox. If you wish to prevent this, please deselect calendar items.

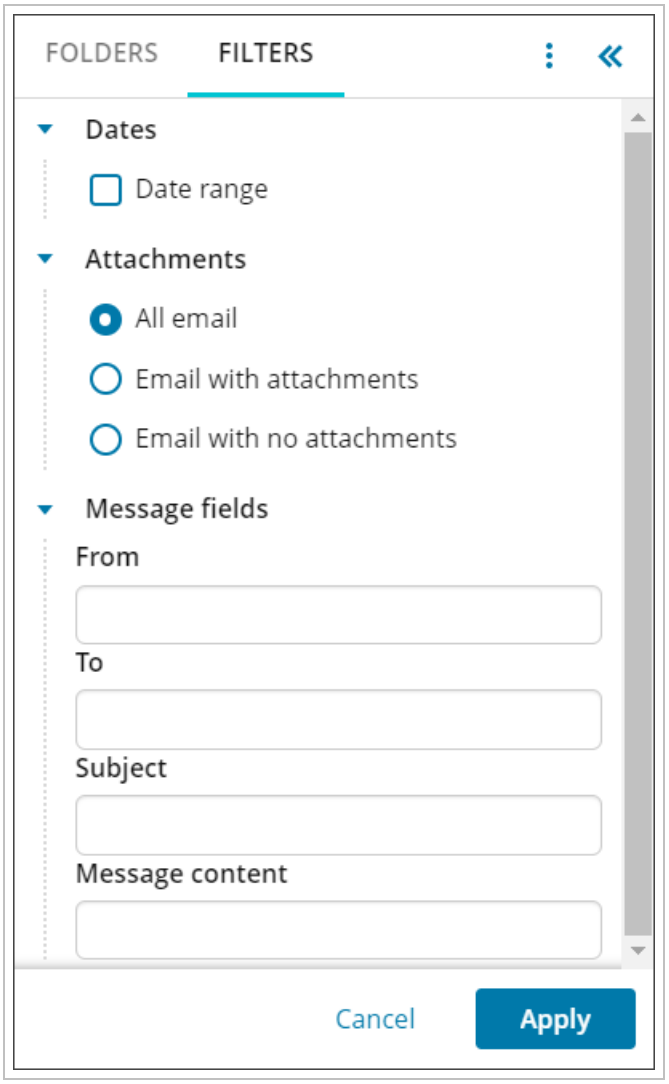


Or

b. Select the folder you wish to filter from the list and move to the filters tab

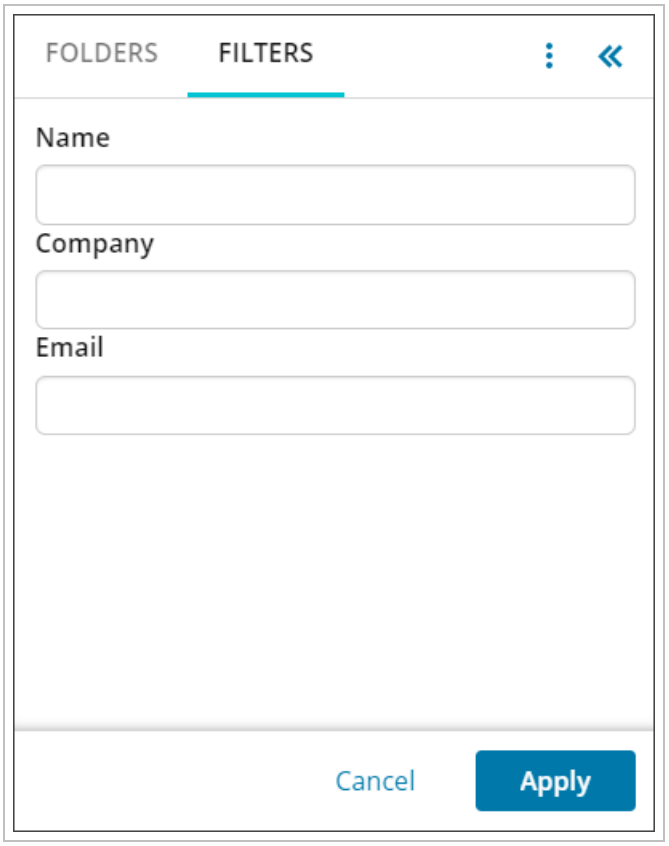
   It is possible to filter for **Inbox**, **Deleted Items**, **Drafts**, **Junk Email**, **Outbox**, **Recoverable items**, **Sent items** or **any additional folders** by:

   - Date range
   - Attachments
     - All email
     - Email with attachments
     - Email with no attachments
   - Message fields
     - From
     - To
     - Subject
     - Message content



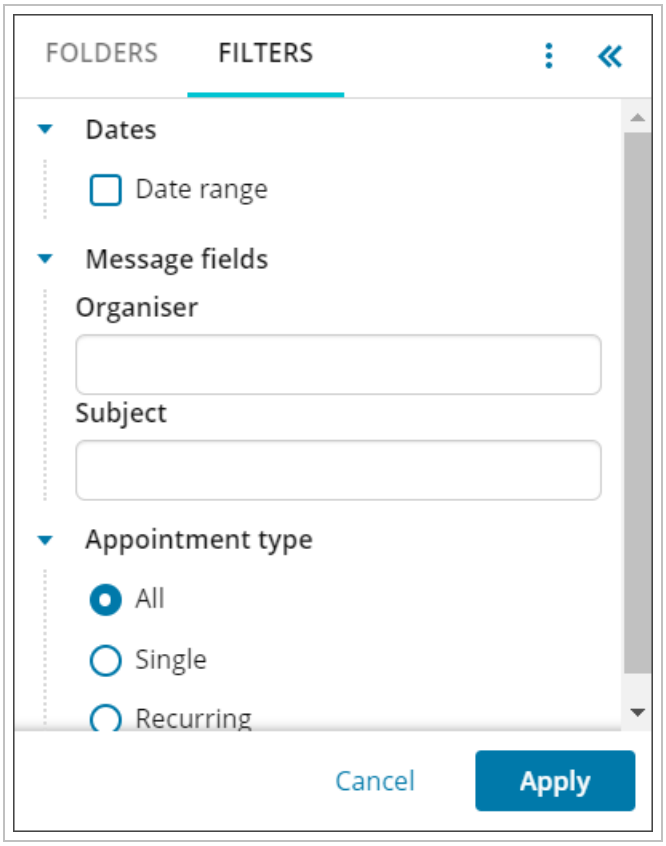
It is possible to filter for **contacts** by:

- Name
- Email
- Company



It is possible to filter for **calendars** by:

- Date range
- Message fields
  - Organiser
  - Subject
- Appointment type
  - All
  - Single
  - Recurring



When restoring Calendar items, these will not be placed back into the original calendar location. Instead these will be placed in a folder titled "Restored_DD-MM-YYYY", where "DD-MM-YYYY" is the recovery date, in the mailbox.name/Calendar/ folder.

9. Select the restore location for items

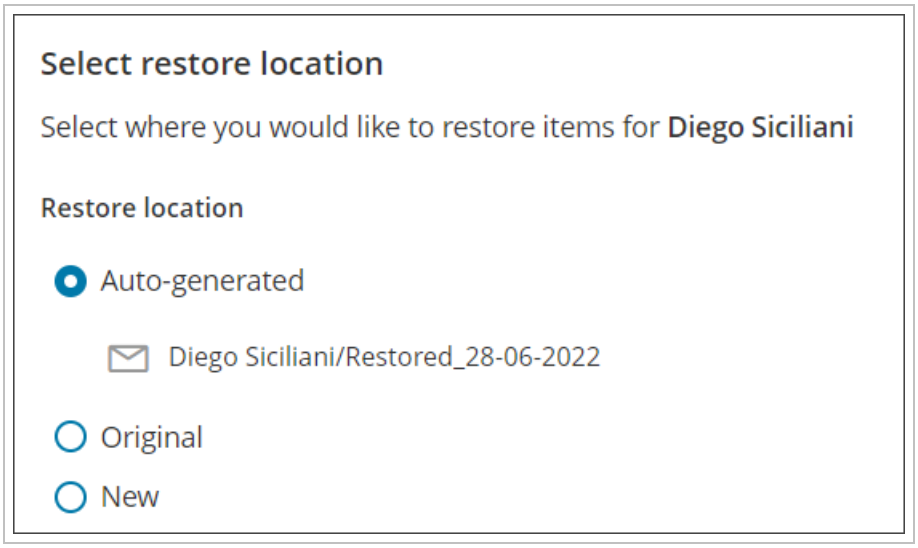
   You can choose an **auto-generated location**, the **original location** or a **new location** which you will be required to specify.

   > If you select multiple types of data to restore in Exchange (e.g. calendar events and emails) you will not be able to restore to a **new location**. You will only have access to restore to the **auto-generated location** or the **original location**.

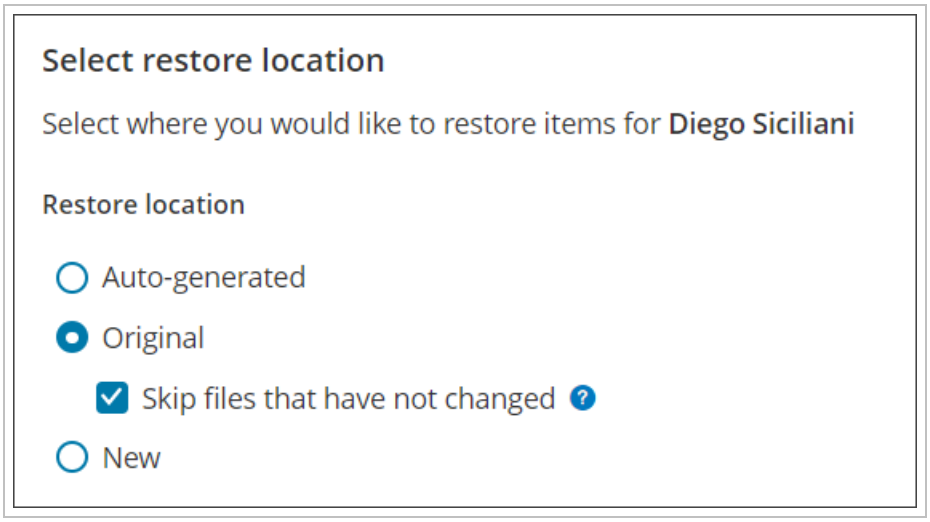
Regular and Shared Accounts

- **Single type of data selected for restore:**

  Auto-Generated location



  Original location



  New location

Select restore location

Select where you would like to restore items for **Diego Siciliani**

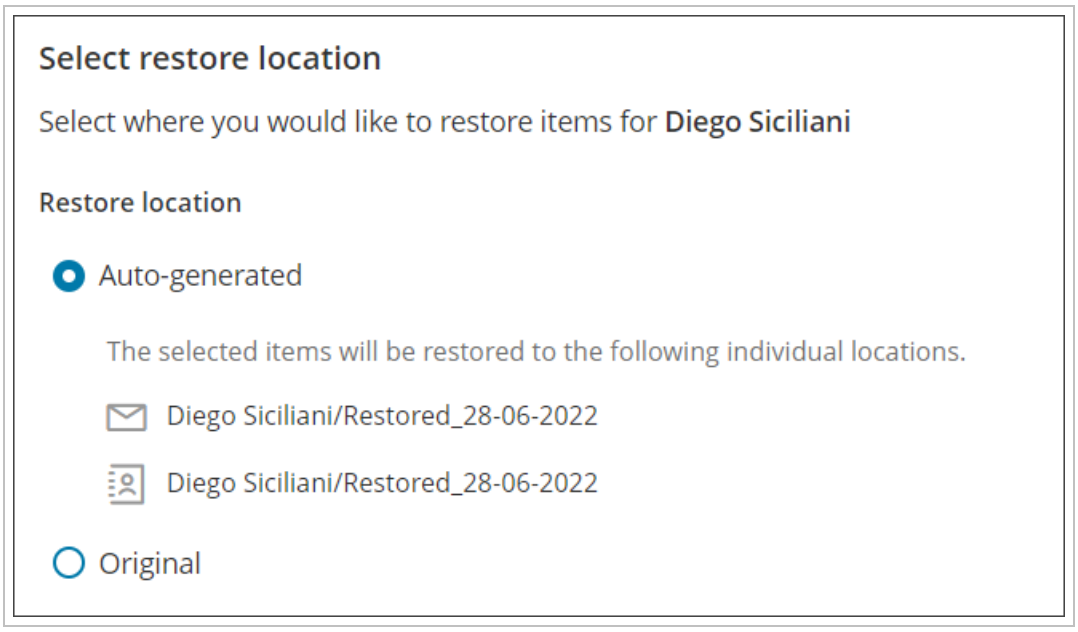
Restore location

- ○ Auto-generated
- ○ Original
- ◉ New

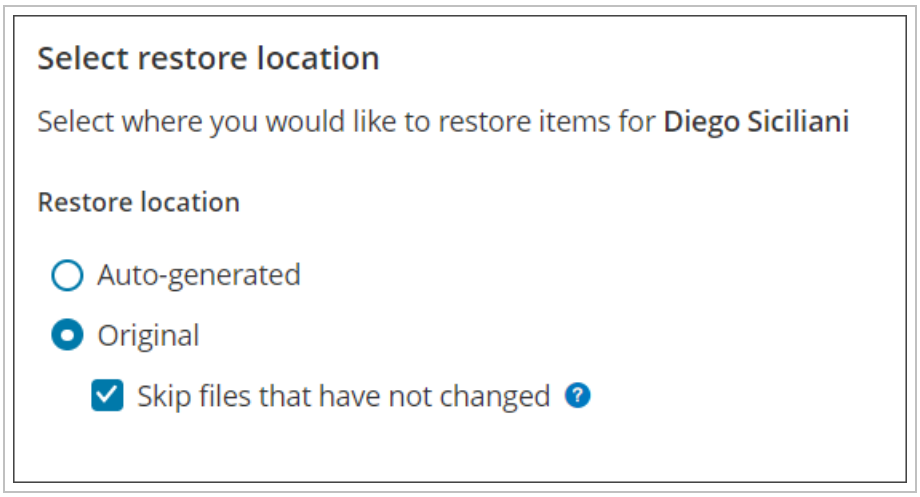
- Diego Siciliani
  - Archive
  - Conversation History
  - Deleted Items
  - Drafts
  - Inbox
  - Junk Email
  - Outbox
  - Sent Items

- **Multiple types of data selected for restore:**

  Auto-Generated location



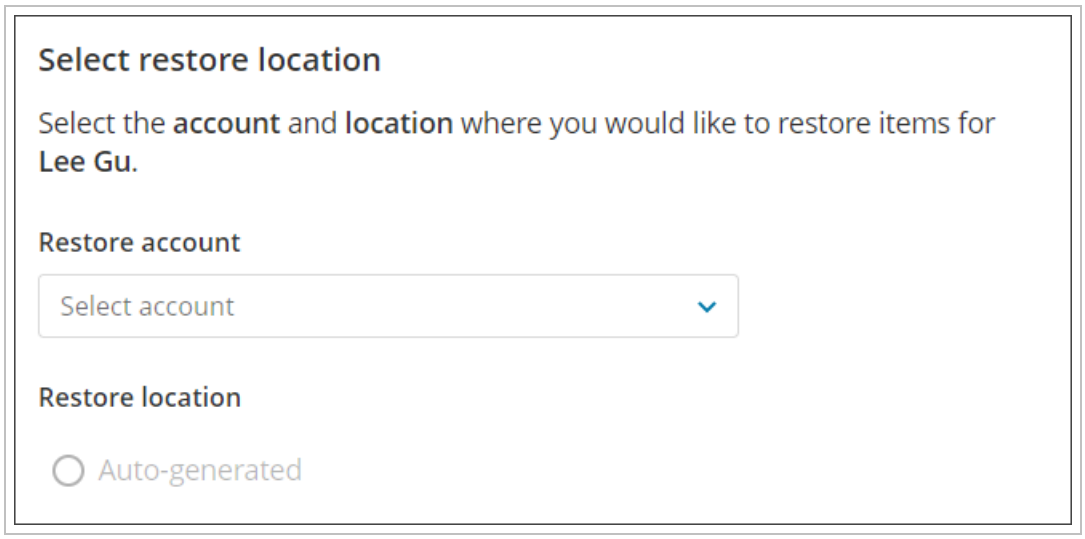
  Original location

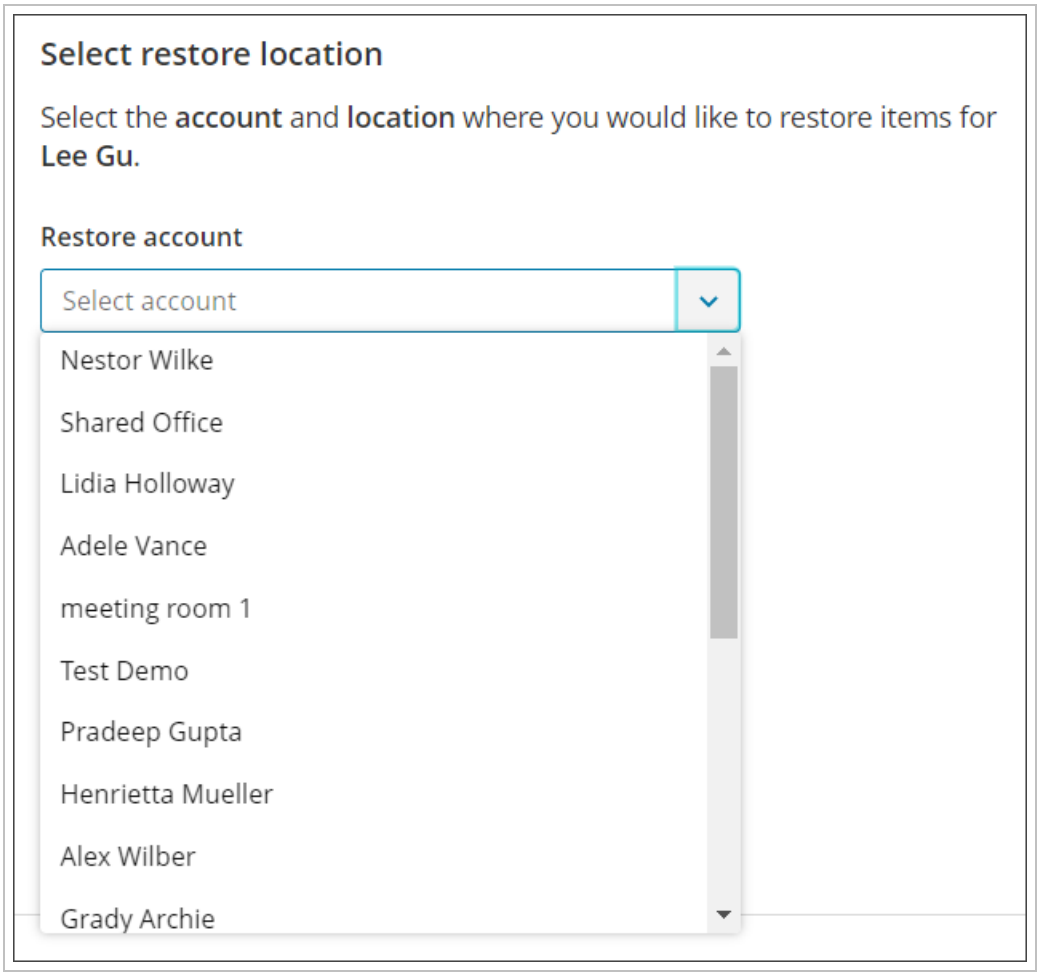


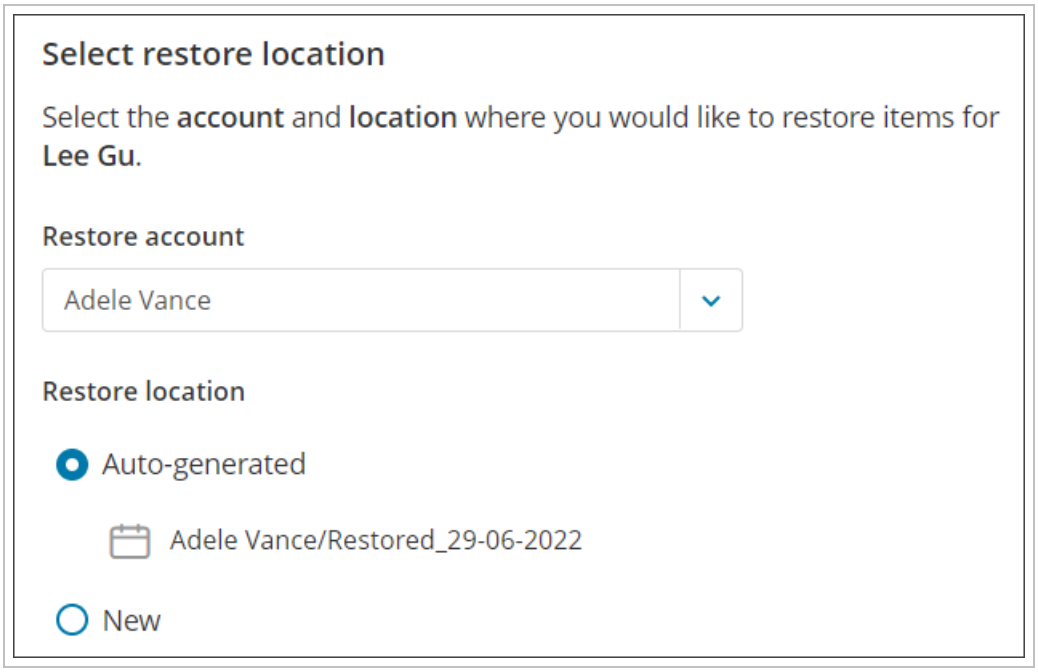
Deleted or Unlicensed Accounts

- Where a mailbox has been deleted or is unlicensed, you will only have access to restore to an **Auto-Generated** or a **New** location.

  Use the dropdown to select the mailbox you wish to restore the **deleted or unlicensed** mailbox to:

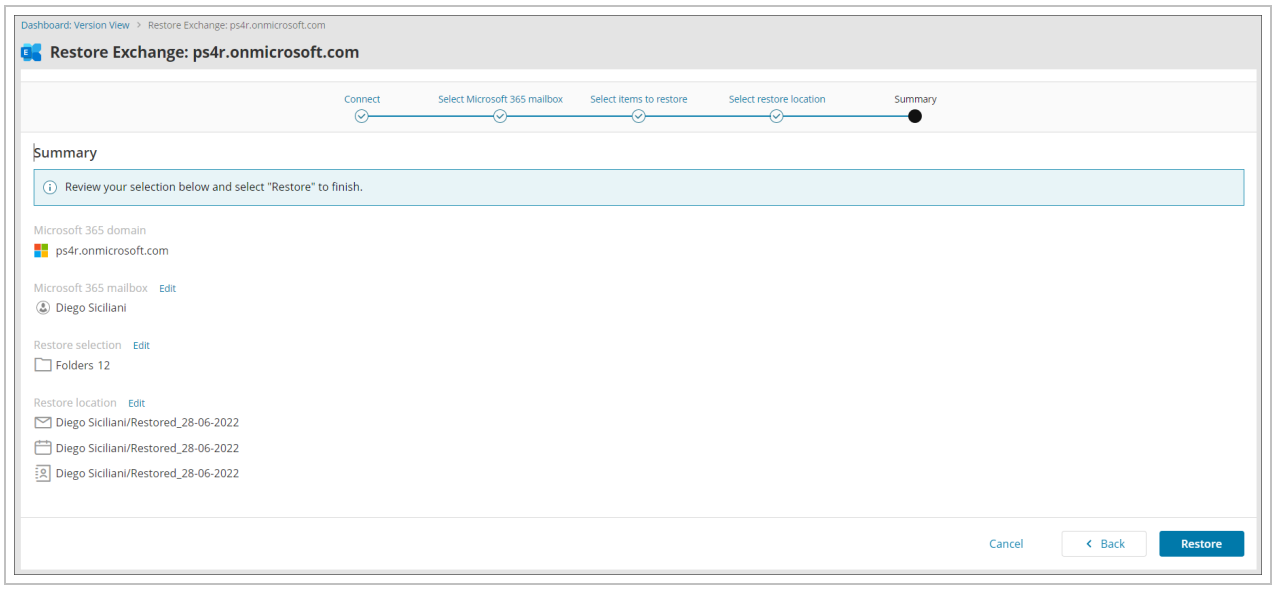


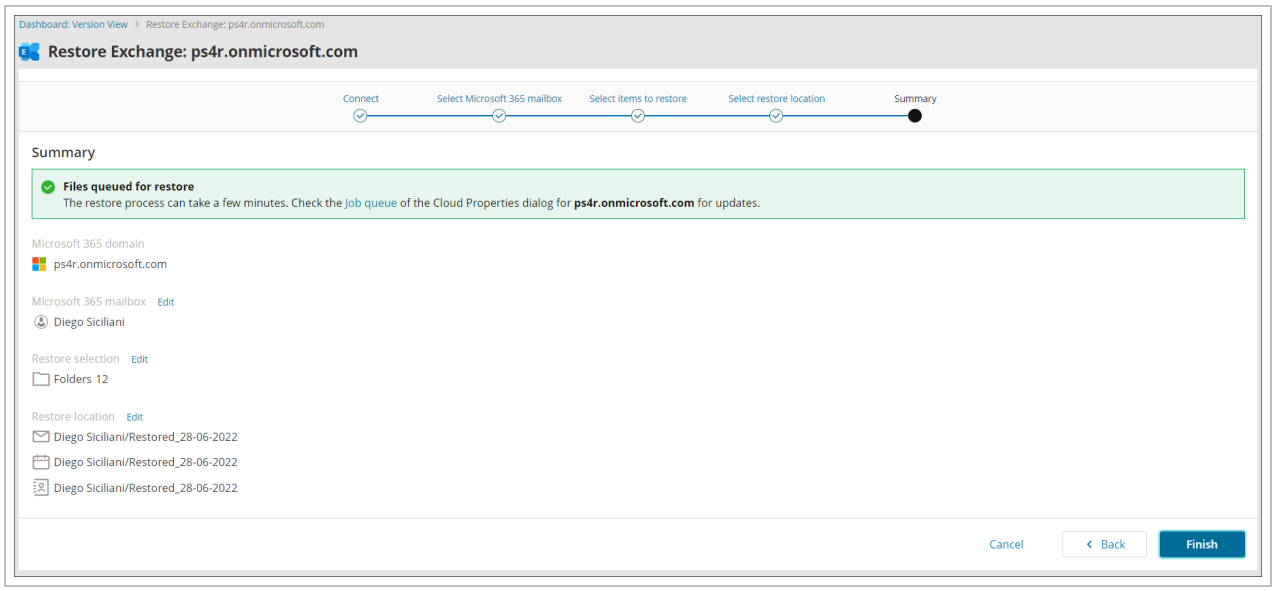

Select restore location
Select the account and location where you would like to restore items for Lee Gu.
Restore account
Select account
Nestor Wilke
Shared Office
Lidia Holloway
Adele Vance
meeting room 1
Test Demo
Pradeep Gupta
Henrietta Mueller
Alex Wilber
Grady Archie


Select restore location
Select the account and location where you would like to restore items for Lee Gu.
Restore account
Adele Vance
Restore location
Auto-generated
Adele Vance/Restored_29-06-2022
New

10. Confirm your intention to start the recovery and close the wizard

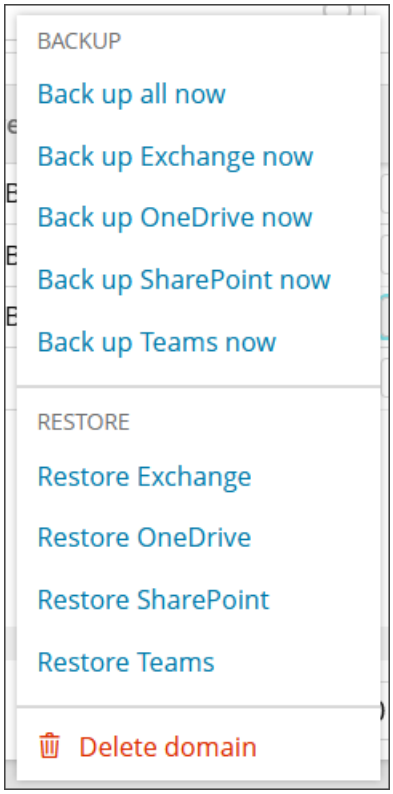
> Microsoft may resend calendar event notifications when you restore a full mailbox. If you wish to prevent this, please deselect calendar items Learn.



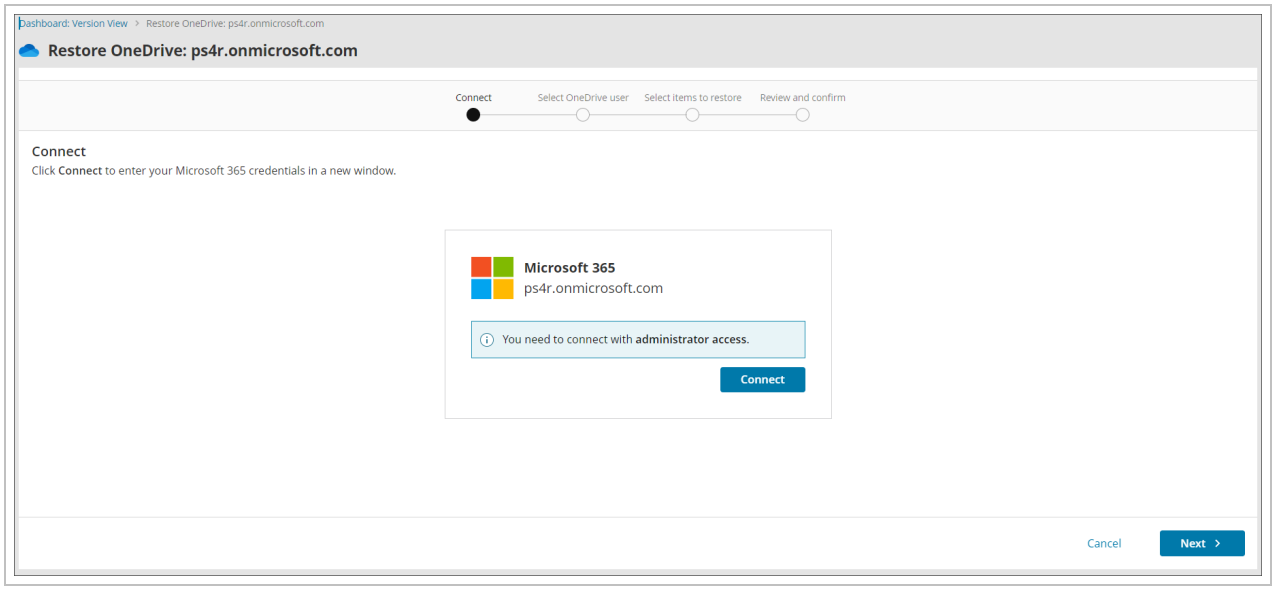


OneDrive

1. Log in to the Management Console under a SuperUser account
2. Open the action menu for the domain and click **Restore OneDrive**

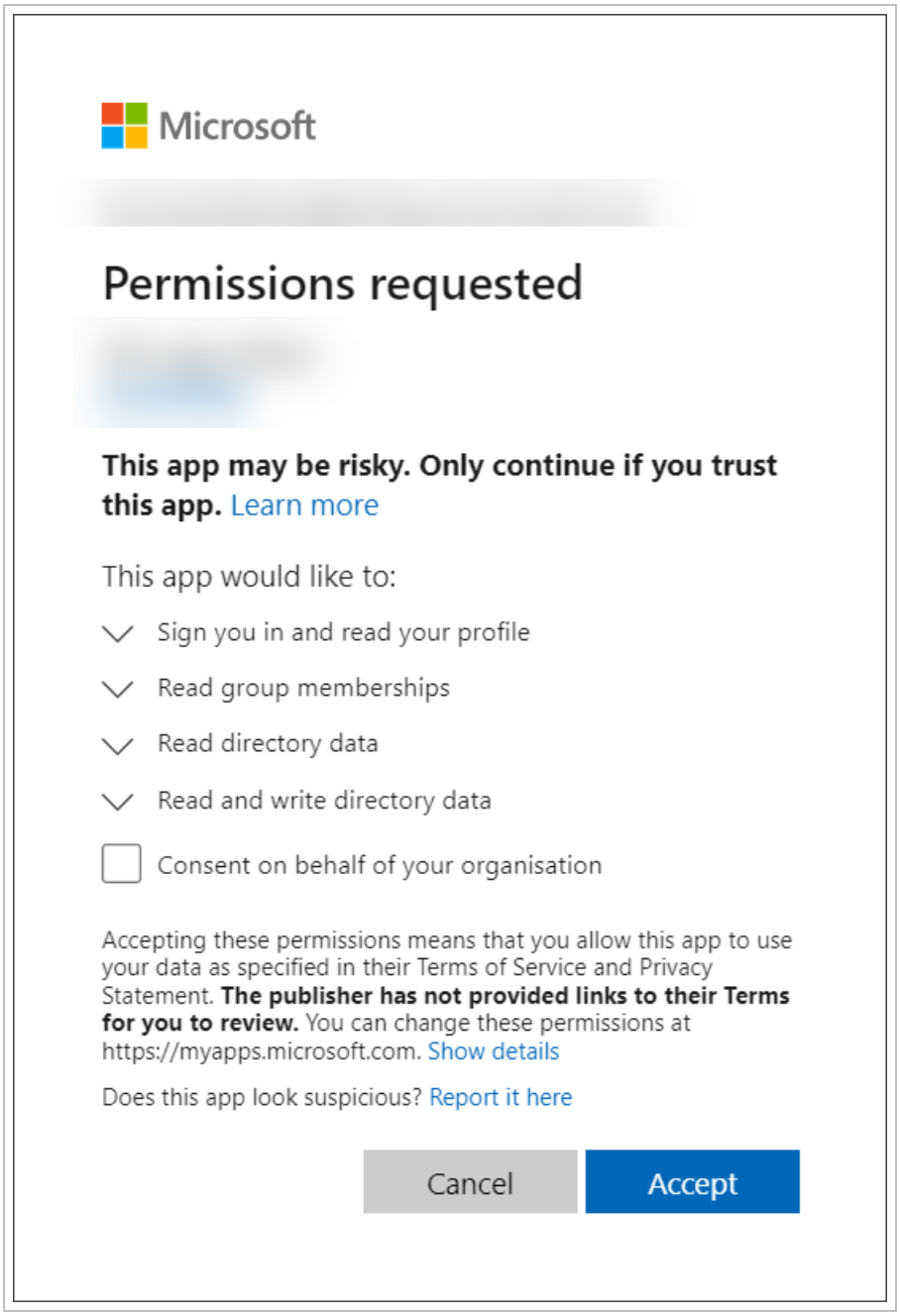


3. Connect to the Microsoft 365 OneDrive account with administrative account credentials



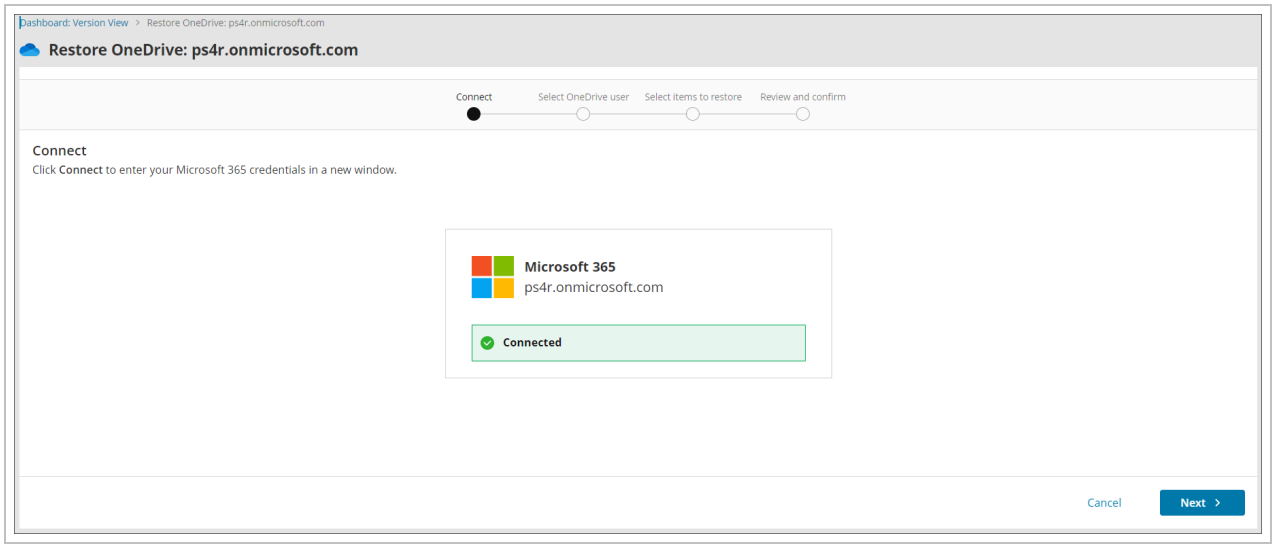
If you do not see the authentication page, make sure your browser is not blocking **pop-up windows**.

4. Accept the required permissions

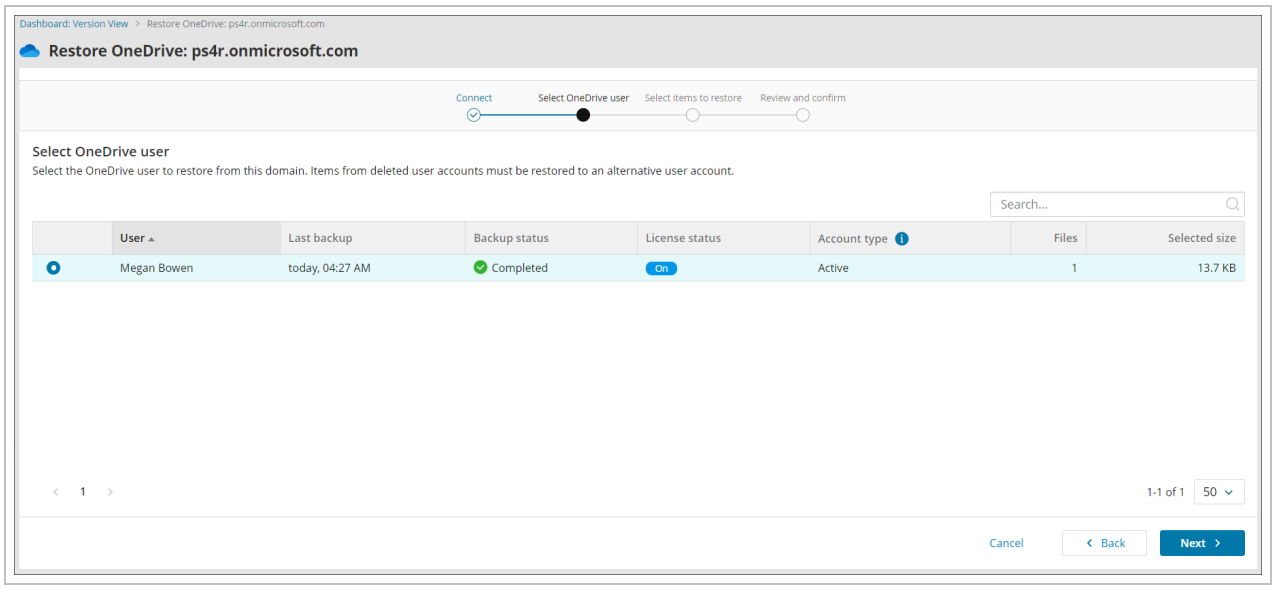


Tick **Consent on behalf of your organisation** if you wish to allow this app access to the specified resources for all users in your organisation. No one else will be prompted to review these permissions.

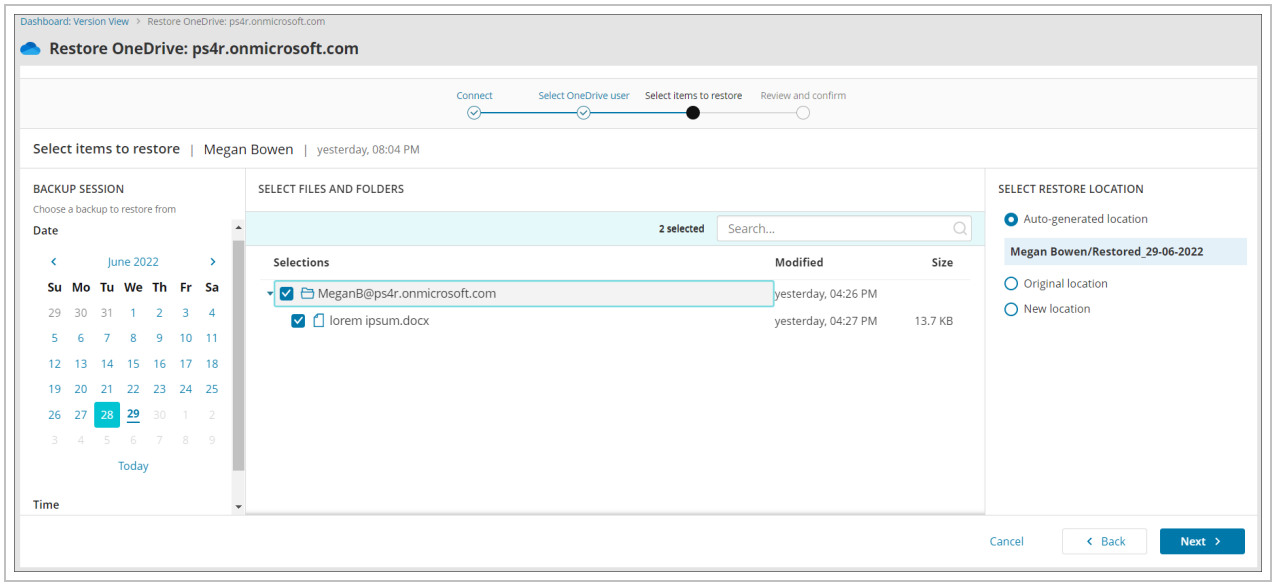
5. You will receive a confirmation that the connection has been successful for the restore



6. Select the account you wish to restore items from and click **Next**. You will see the list of backed up accounts, backup status of the account, the account type (Active or Deleted), number of files and the size of the accounts selection.



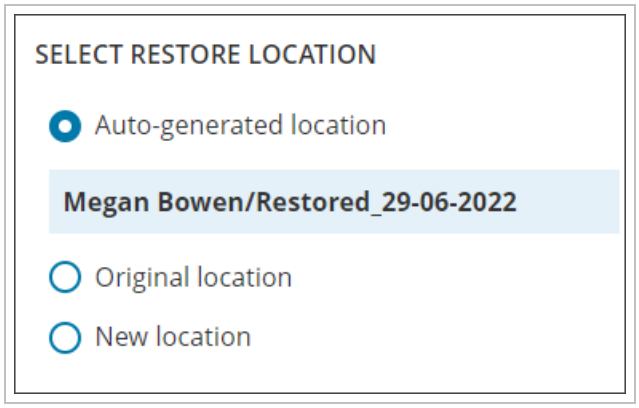
7. Select the backup date on the left and backup session from the dropdown below if more than one backup was completed on that date. Then choose the files and folders to restore from the backup tree



8. Select the restore location for items, which will be in a panel to the right or below the data selection

Active Accounts

- You can choose an **auto-generated location**, the **original location** or a **new location** which you will be required to specify

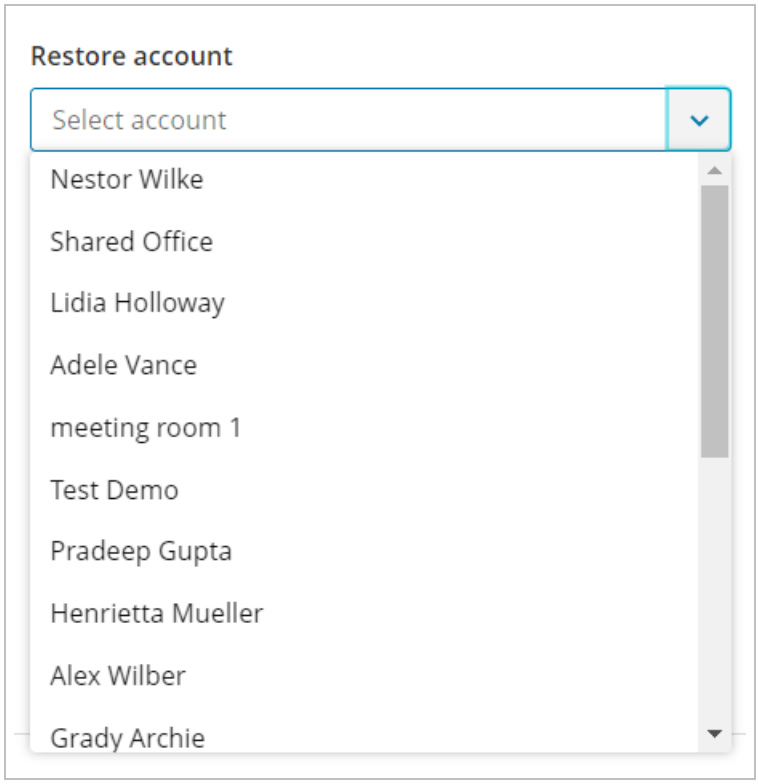


When restoring to a **new location**, you may select nested sub-folders

Deleted or Unlicensed Accounts

- Where an account has been deleted or is unlicensed, you will only have access to restore to an **Auto-Generated** or a **New** location

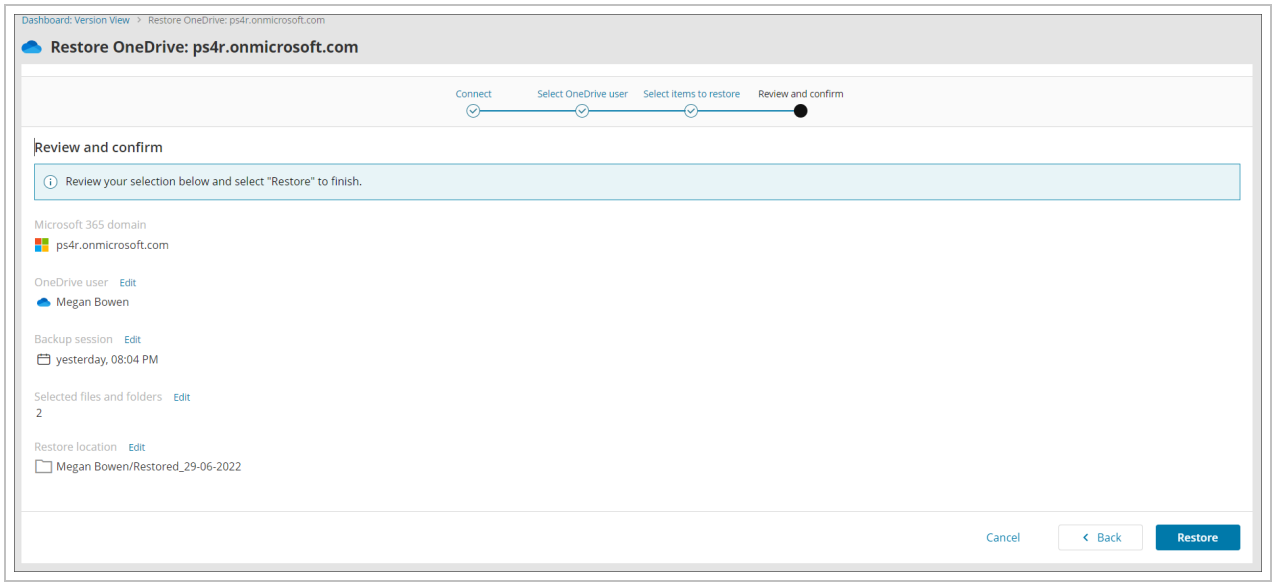
  Use the dropdown to select the account you wish to restore the **deleted or unlicensed** account to:

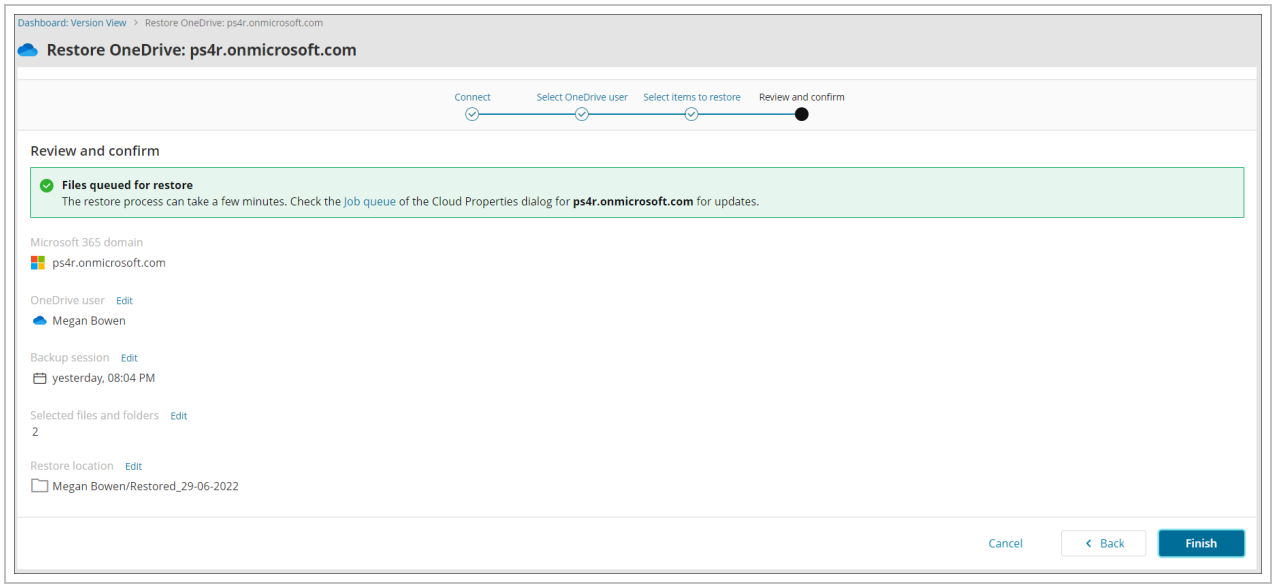


  Then choose either the automatically generated location, or browse through the tree to select a new location

> Selected items restored to the **auto-generated location** are restored to a new sub-directory created in account.name/ titled "Restored_DD-MM-YYYY", where "DD-MM-YYYY" is the recovery date.

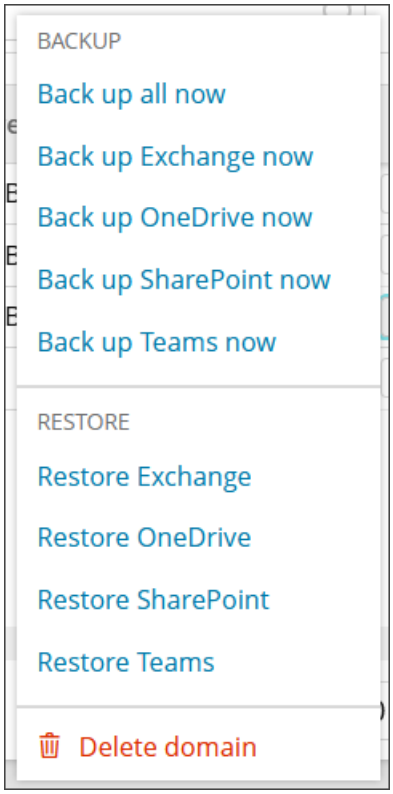
9. Confirm your intention to start the recovery and close the wizard



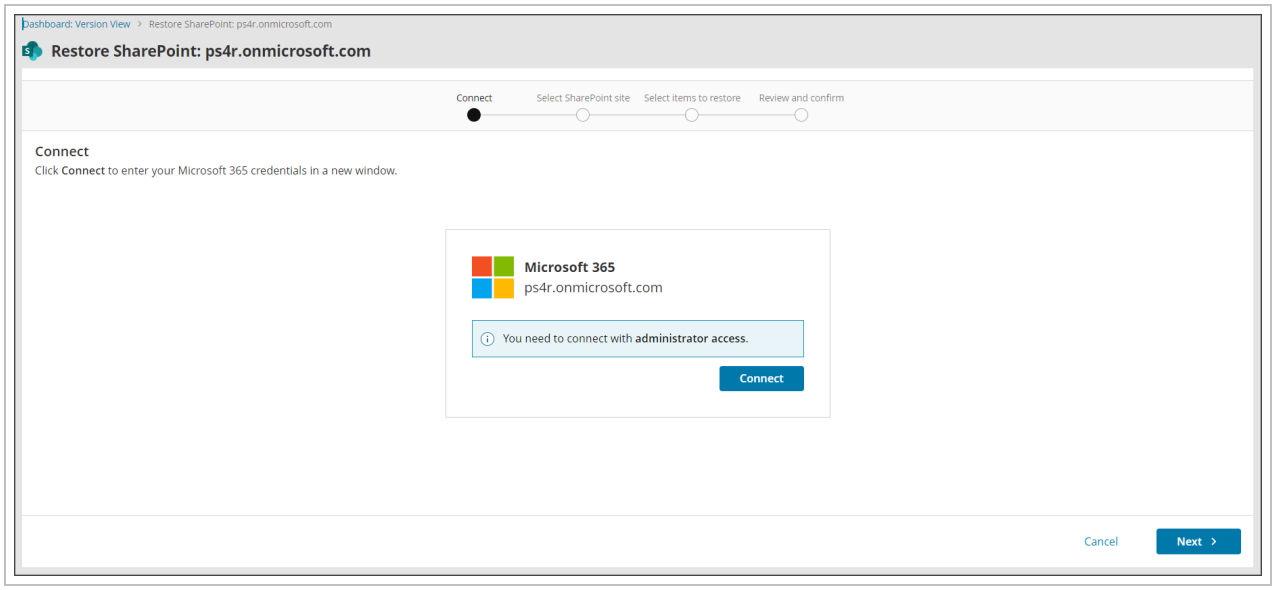


SharePoint

1. Log in to the Management Console under a SuperUser account
2. Open the action menu for the domain and click **Restore SharePoint**

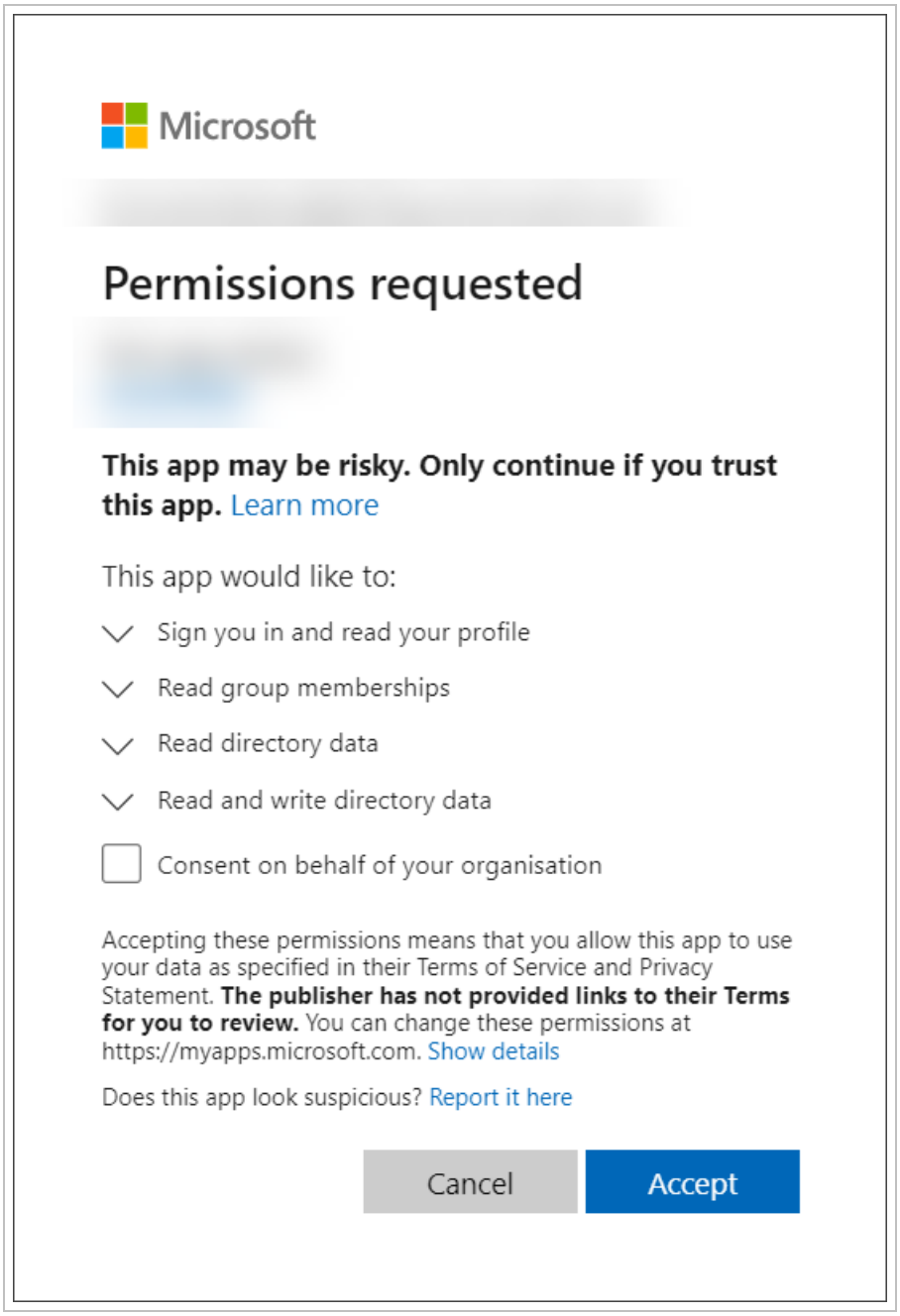


3. Connect to the Microsoft 365 SharePoint account with administrative account credentials

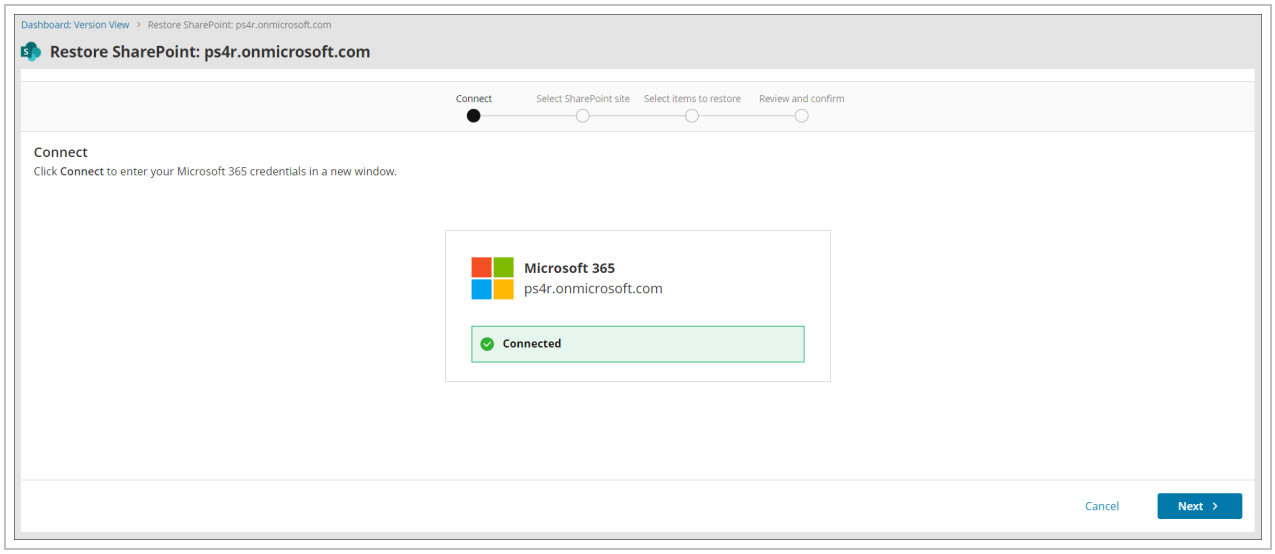


If you do not see the authentication page, make sure your browser is not blocking **pop-up windows**.

4. Accept the required permissions

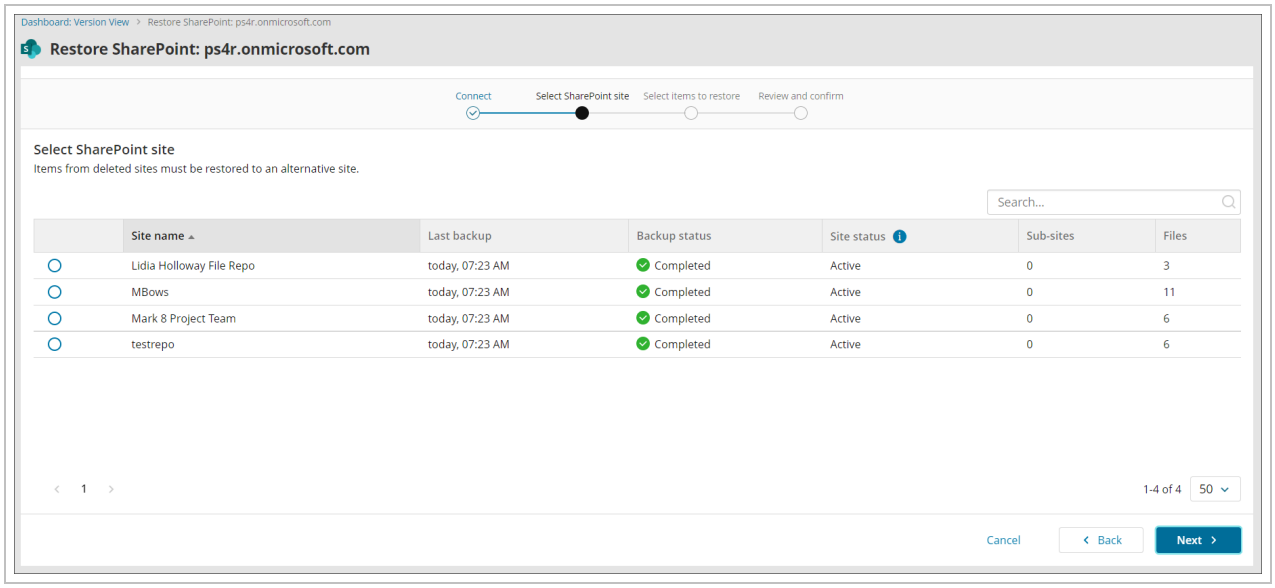


5. You will receive a confirmation that the connection has been successful for the restore

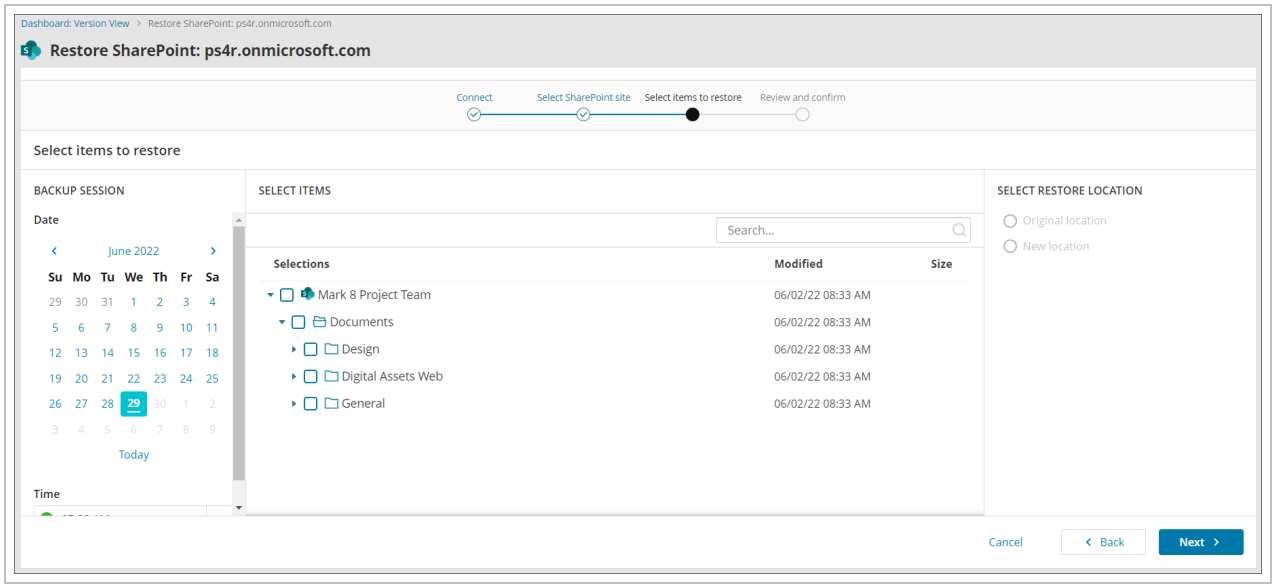


6. Select the site you wish to restore from

   You will see the list of backed up sites, backup status of the site, the site status (Active or Deleted), number of Sub-sites and number of files.



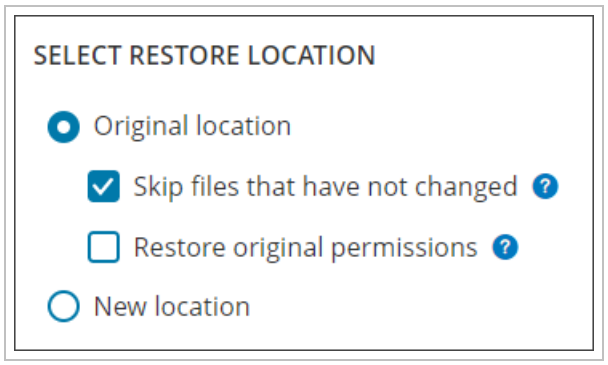
7. Select the backup date, backup session and then the items restore from the backup tree


Dashboard: Version View > Restore SharePoint: ps4r.onmicrosoft.com
Restore SharePoint: ps4r.onmicrosoft.com
Connect
Select SharePoint site
Select items to restore
Review and confirm
Select items to restore
BACKUP SESSION
Date
June 2022
Su Mo Tu We Th Fr Sa
Today
Time
SELECT ITEMS
Search...
Selections
Modified
Size
Mark 8 Project Team 06/02/22 08:33 AM
Documents 06/02/22 08:33 AM
Design 06/02/22 08:33 AM
Digital Assets Web 06/02/22 08:33 AM
General 06/02/22 08:33 AM
SELECT RESTORE LOCATION
Original location
New location
Cancel
Back
Next

8. Select the restore location for items, which will be in a panel to the right or below the data selection

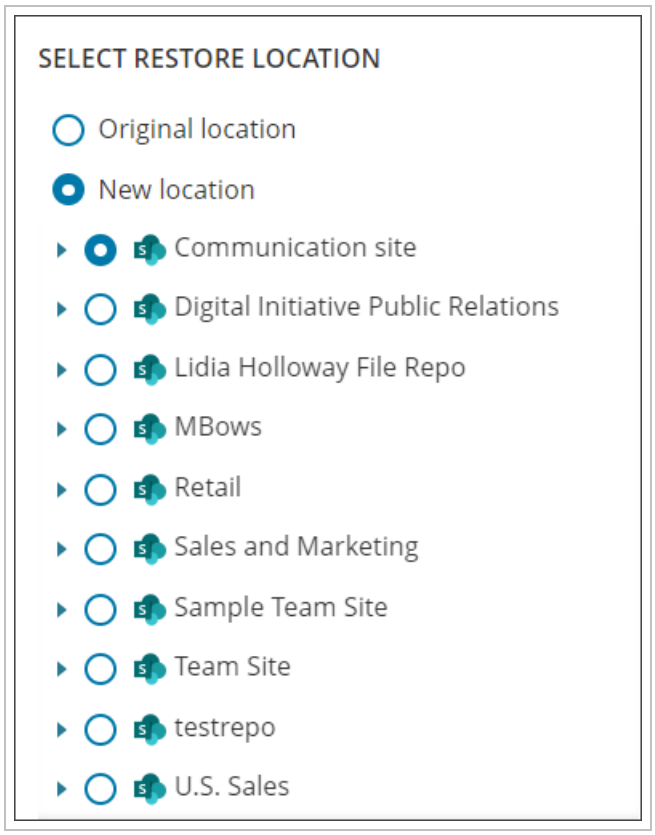
Regular Sites

- You can choose to restore to the **Original Location**



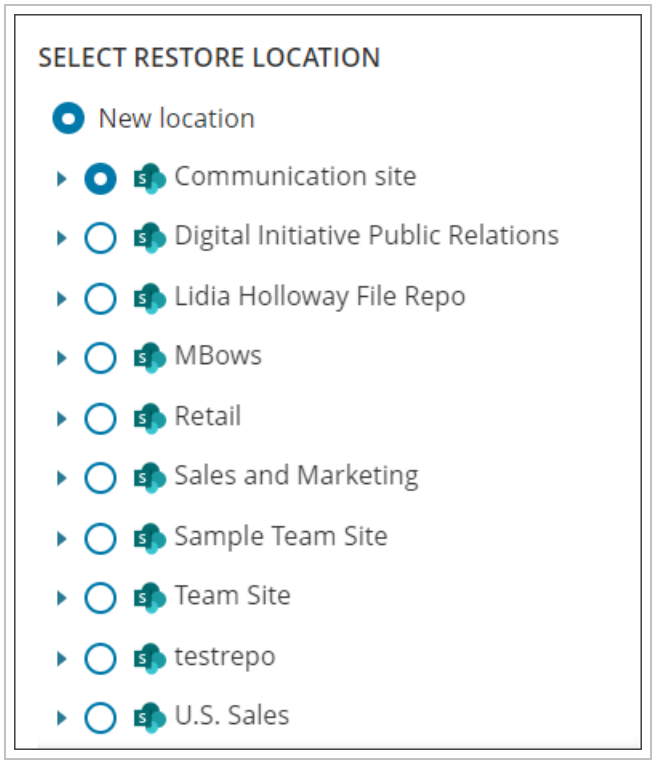
> When restoring to the **Original Location**, you will also see an option to **restore original permissions**. You can find information on Microsoft 365 SharePoint Permissions here.

- Or a **New Location** which you will be required to select from a list of locations.

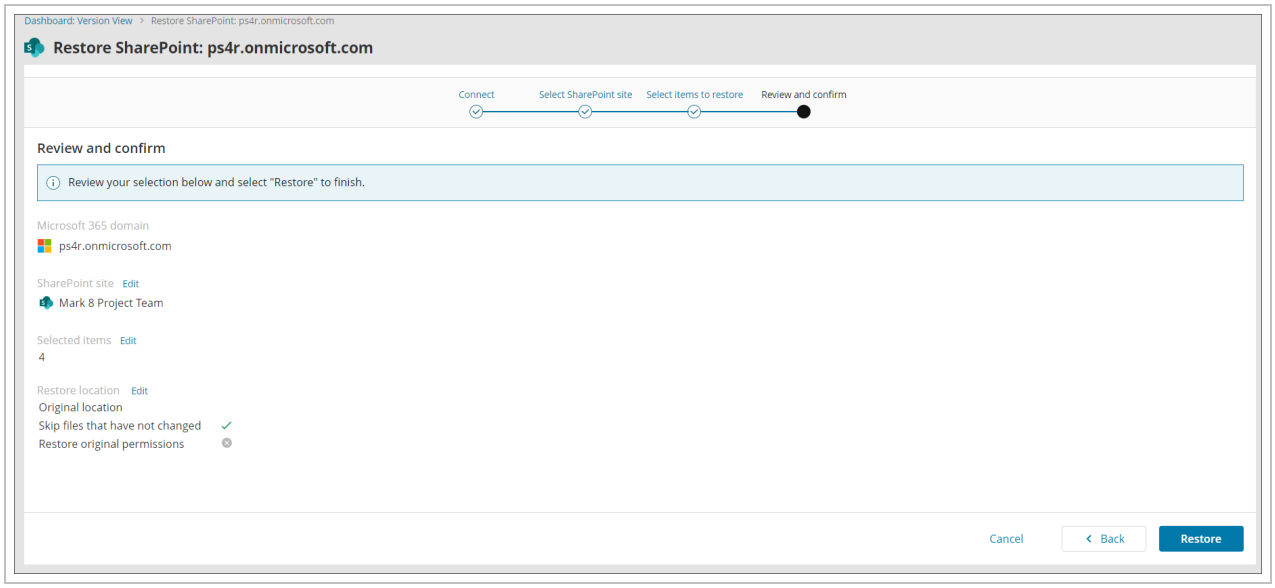


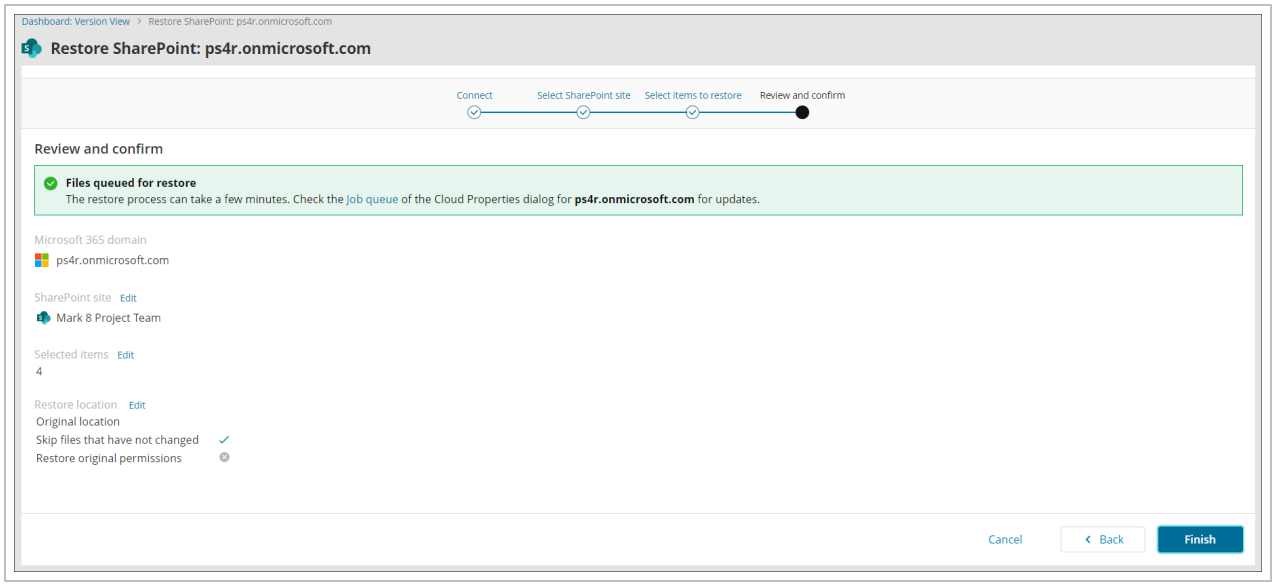
Deleted Sites

- For deleted site collections, you will only have the option to restore to a **New Location**



9. Confirm your intention to start the recovery and close the wizard

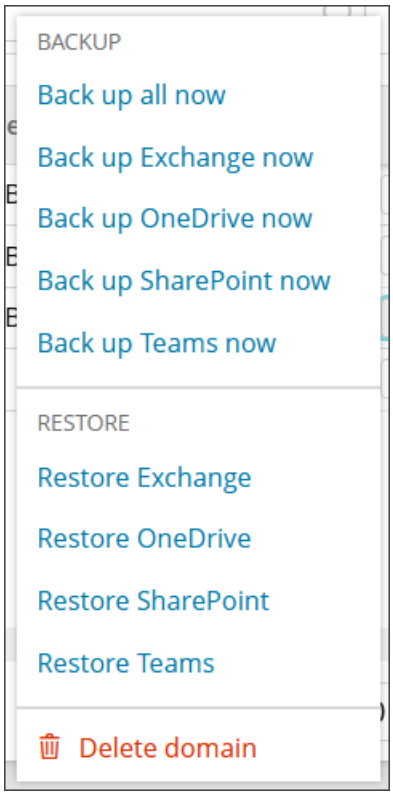




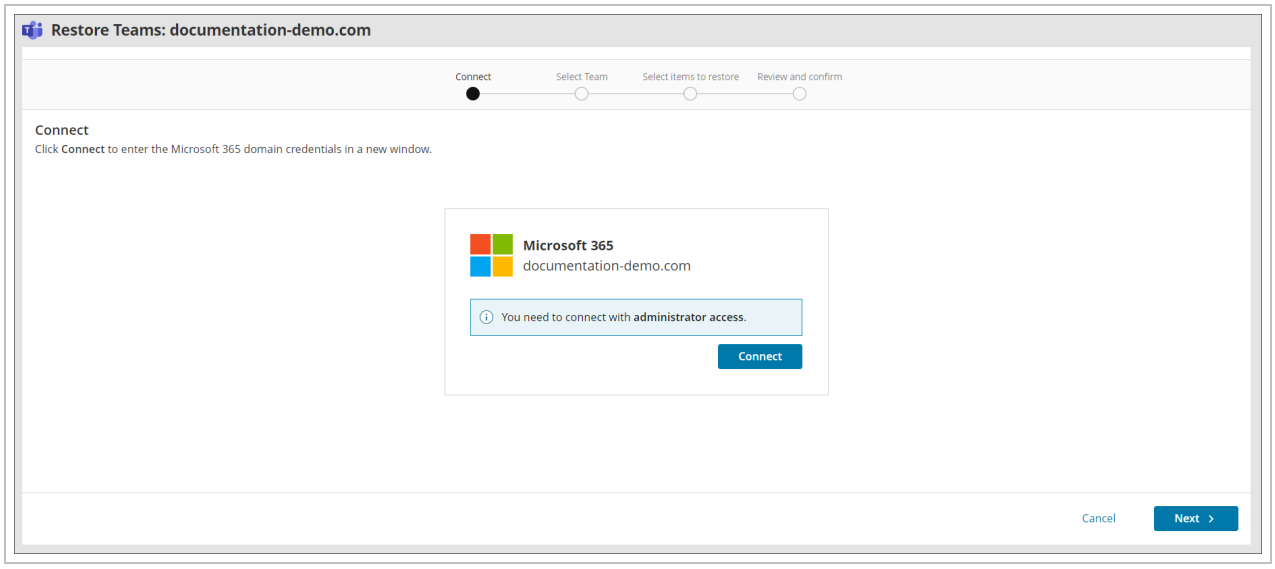
> We cannot restore SharePoint site collection. In cases where site collection has been deleted, you will need to recreate this manually.

Teams

1. Log in to the Management Console under a SuperUser account
2. Open the action menu for the domain and click **Restore Teams**

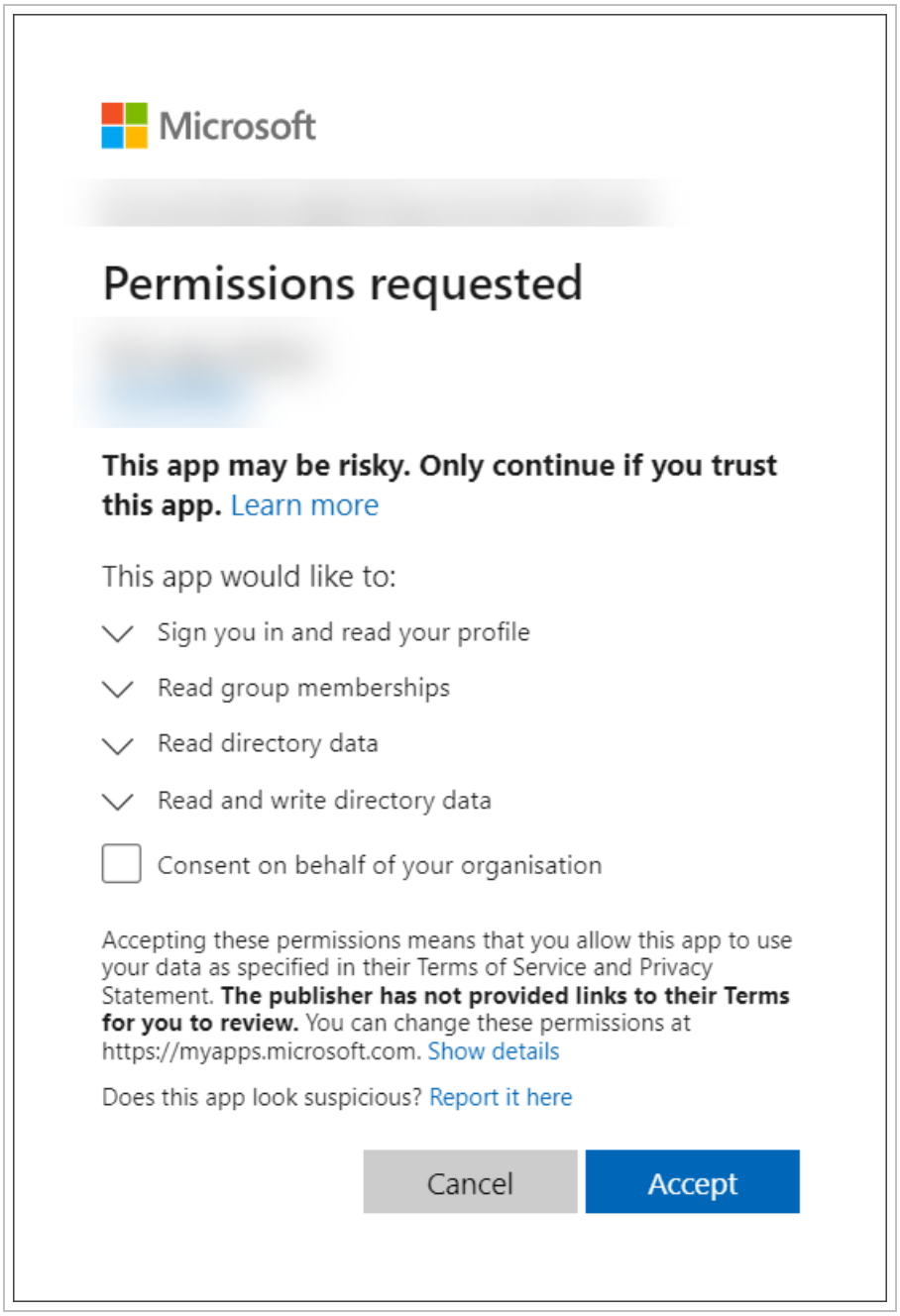


3. Connect to the Microsoft 365 Teams account with administrative account credentials

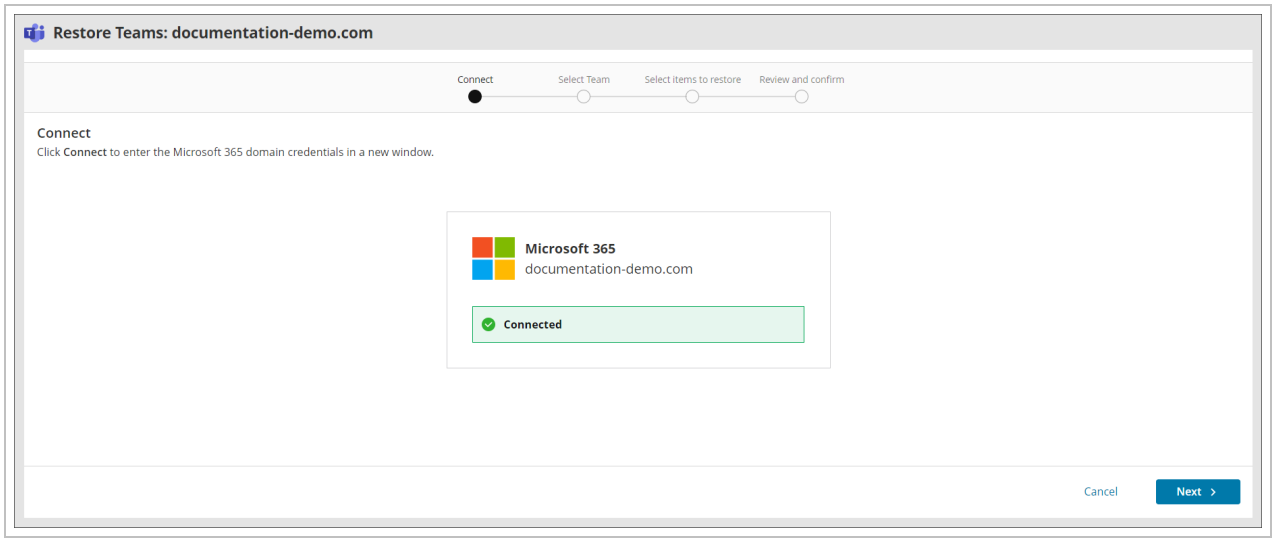


If you do not see the authentication page, make sure your browser is not blocking **pop-up windows**.

4. Accept the required permissions

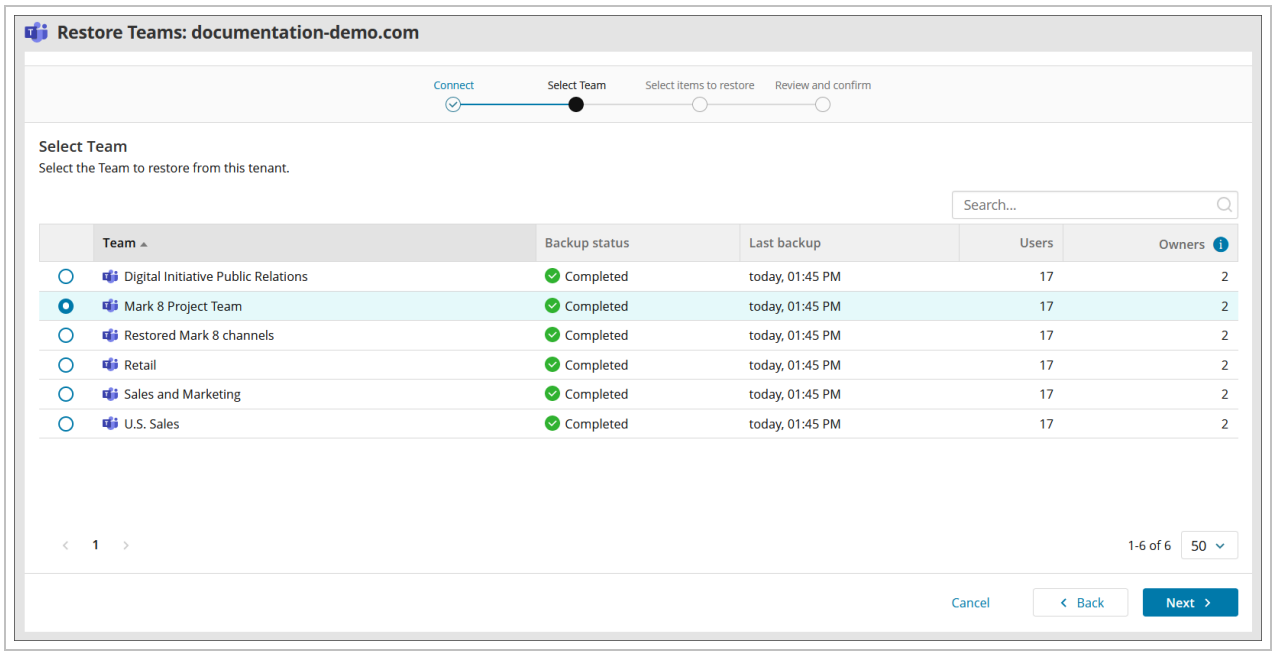


5. You will receive a confirmation that the connection has been successful for the restore, click **Next** to proceed

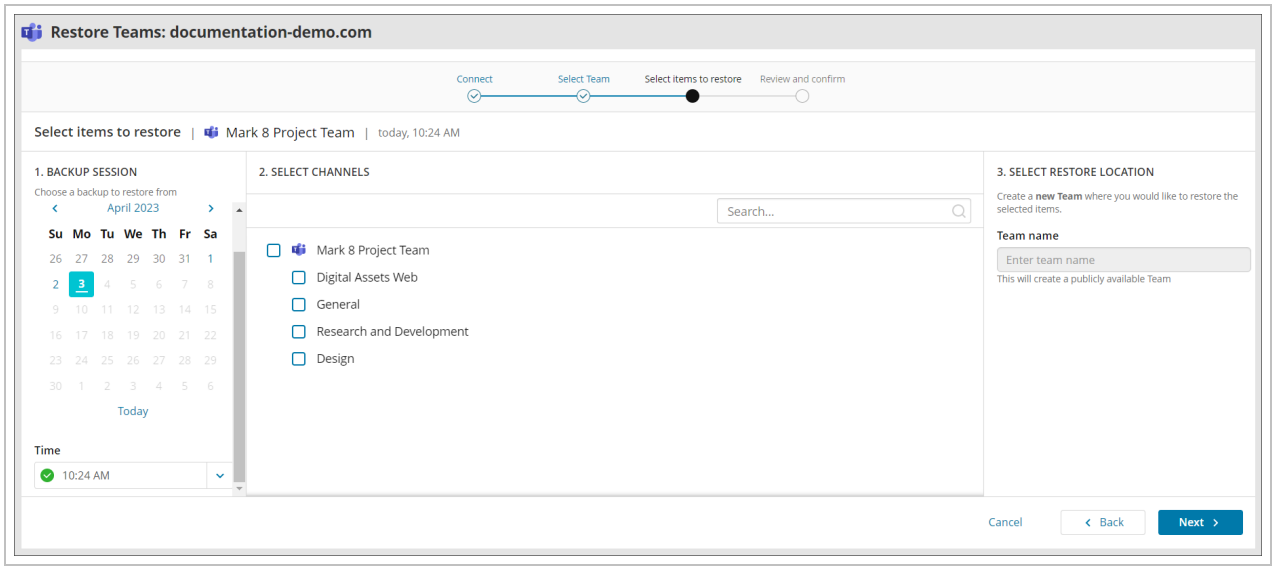


6. Select the Team you wish to restore from and click **Next**

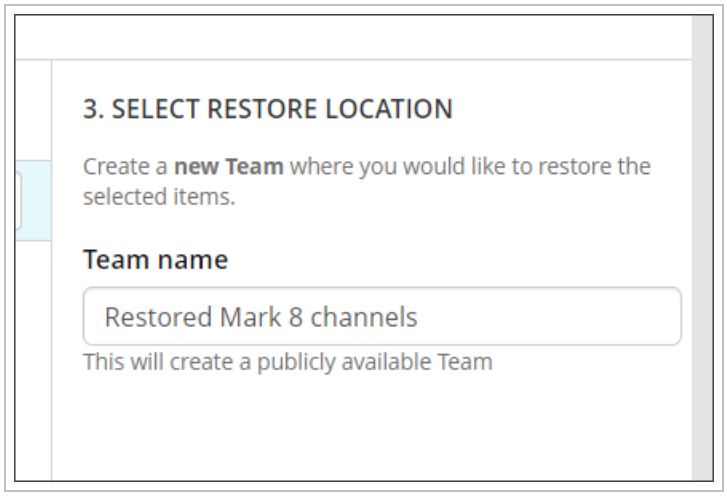
   You will see the list of backed up teams, the backup status of the team, the time and date of last backup, number of users and number of owners



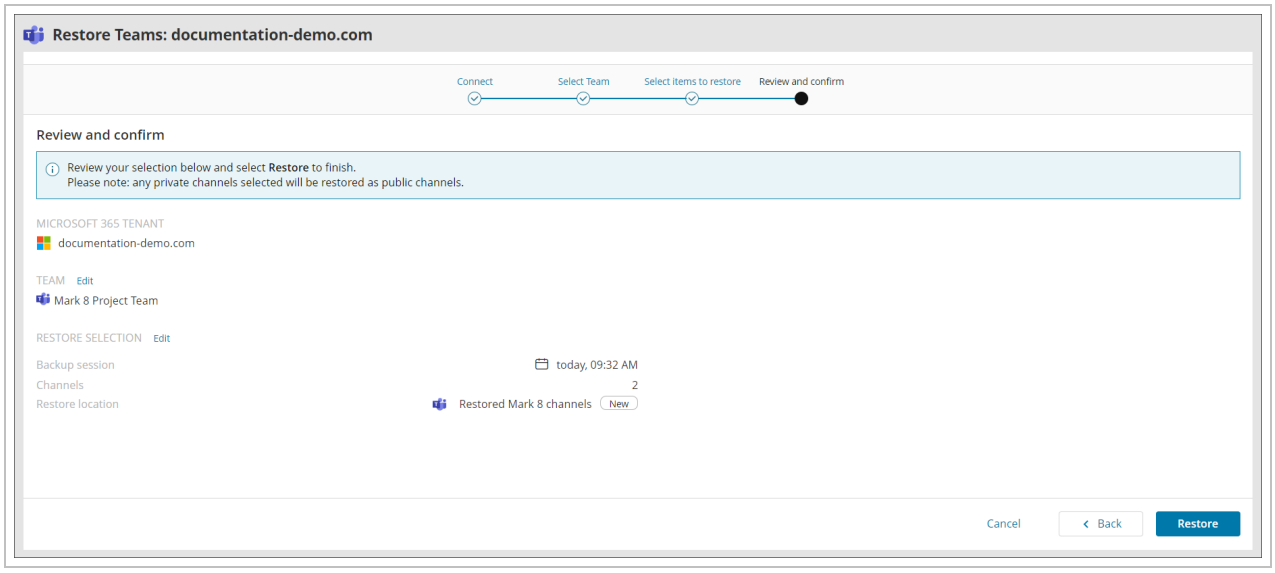
7. Select the backup session using the calendar and time dropdown and then select the channels to restore from the backup tree

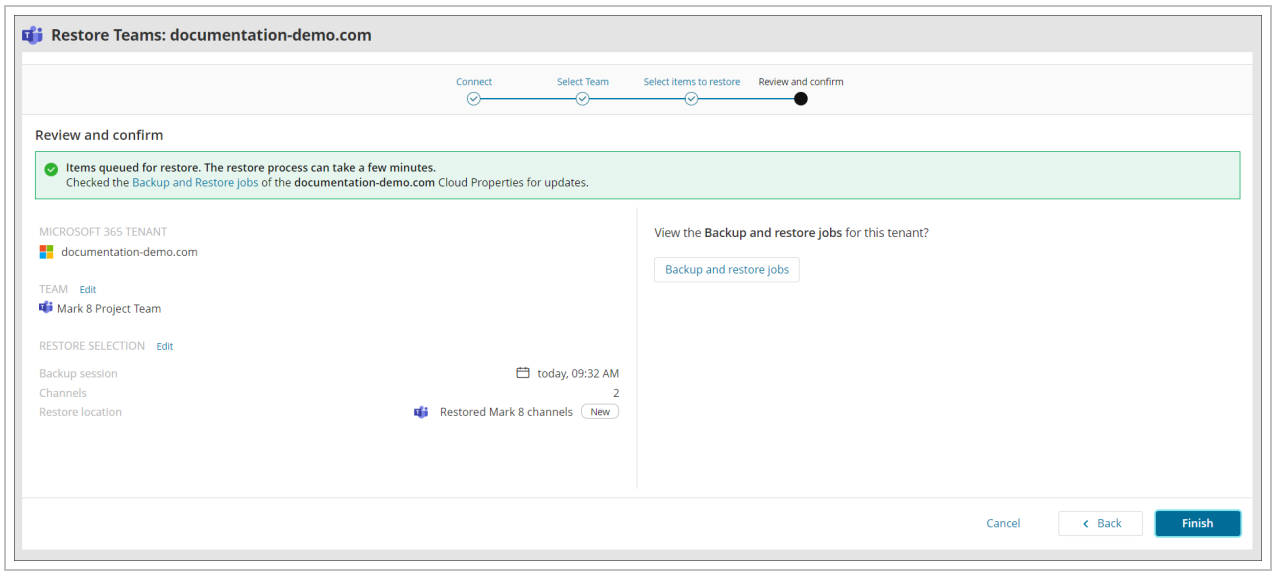


8. Provide a new **Team Name** of the recovery location where you would like to restore the selected items



9. Click **Next**
10. Confirm your intention to start the recovery and close the wizard

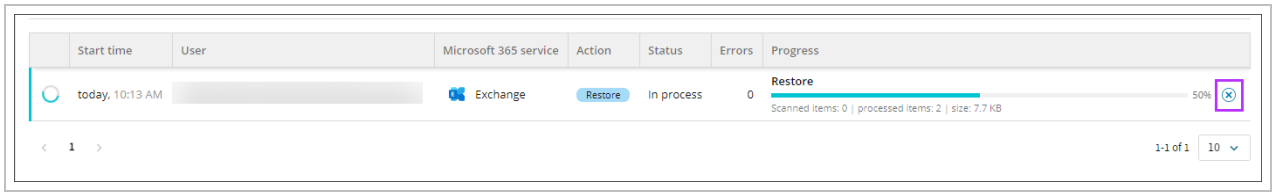




Cancel Restore

To cancel a currently running restore:

1. View the devices job queue
2. Click cancel to the right hand side
3. Refresh the tab to remove the job



Only restores can be canceled, backups cannot.

Microsoft 365 SharePoint Permissions

From version 19.12, SharePoint Online permissions are now protected during the backup process. This allows you to restore SharePoint items from the backup session with their original permissions.

This is **not** retroactive, so any backups made before 19.12 was released will not contain permissions.

These permissions are only relevant for backups done via Microsoft 365 protection, not when backing up the MS SharePoint data source via Backup Manager

Restore Permissions Processes

Below are examples of how the restore permissions process works and how you should work around the permissions for a successful restore.

- See the Microsoft page for information on What is permissions inheritance?
- See the Microsoft Customize SharePoint site Permissions page for information on how to configure permissions.

Permissions restore is turned off

When permissions restore is disabled, all items created during a restore will inherit permissions from their parent.

Permissions restore is turned on

When permissions restore is enabled, the permissions inheritance is determined as below:

Restore to the original location

Permissions Inheritance settings on SharePoint Item	Permissions Inheritance of data to restore	Expected response by system
Enabled	Disabled	1. Inheritance disabled 2. All permissions cleared 3. Only backed up permissions restored
	Enabled	Permissions restore for such items skipped
Disabled	Disabled	Permissions merged
	Enabled	Inheritance Enabled

Restore to new location

Permissions Inheritance settings on SharePoint Item	Permissions Inheritance of data to restore	Expected response by system
Enabled	Disabled	Inheritance Enabled
	Enabled	
Disabled	Disabled	Inheritance Enabled
	Enabled	

Permissions restore is turned on (overwrite)

There are a number of different situations you may find yourself in with regards to restoring items which inherit role assignments from their parents. In these situations, you should only break inheritance when the parent role assignments are changed. After the parent role assignments are changed, you then need to restore the new role assignments from the backup. When permissions are not changed, permissions inheritance should be turned on.

How it works:

If the original permissions differ from the backed up set:

Role Assignments	Action taken by the system
If it isn't identical:	1. Inheritance disabled 2. All permissions cleared 3. Only backed up permissions restored
If the item has another set of role assignments:	▪ Role assignments are merged Merging means adding new permissions to the existing, without duplicating and overwriting.

Role Assignments	Action taken by the system	
If the item has role assignments which depend on one or several users:	▪ If all users exist	▪ All role assignments restored
	▪ If none of those users exist	▪ Role assignments not restored. In this case the item won't have explicit role assignments and it won't have inheritance, e.g. item won't have any access permissions set to it
	▪ If some users still exist	▪ Role assignments restored only to those users
	▪ If some users don't exist anymore	▪ Recreation of this user is not tried
If the item has role assignments which depend on one or several groups:	▪ The role assignments are restored only for existing groups	

Glossary of Cove Data Protection (Cove) terms

Documents guide

Documents is a purpose-built data protection solution for Windows and macOS workstations and laptops. It provides highly automated data protection of key office files (every Word doc, spreadsheet, presentation, text file, .pdf, .csv) at a price point similar to antivirus software.

- Installation is done in a click
- Backups run twice a day without user interference
- All backup settings are predefined and cannot be changed
- Users can recover selected files and folders at any time

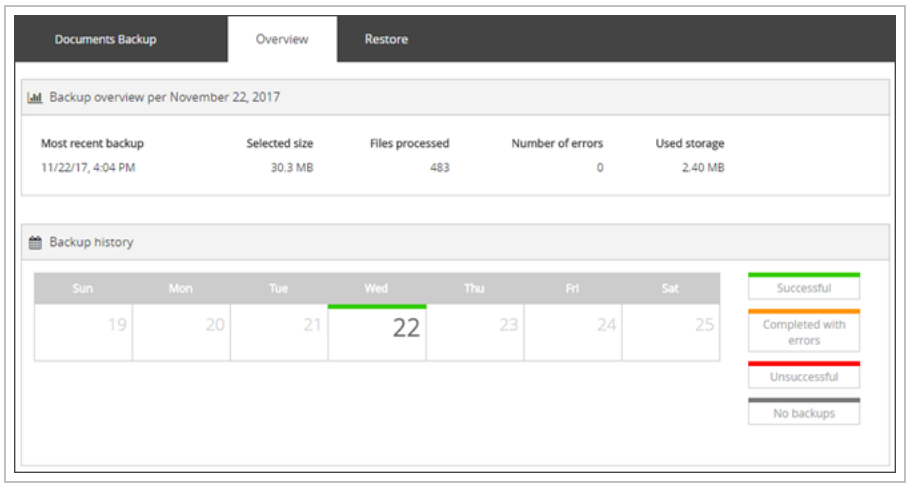
> There is no limit to the size of files that can be backed up.

How it works

There is just one data source for backup and recovery – **Files & Folders** (not named explicitly in the user interface). All local drives on the device are scanned for eligible files which are detected automatically by the system (see the full list of supported file types here and the list of exclusions here). The Documents backups start right after the installation and are repeated twice a day:

1. At **night** between 9 pm and 6 am
2. At **lunchtime** between 12 noon and 2 pm

No backup settings are available; the **Preferences** module is hidden. Also it is not possible to change the backup settings through remote commands.

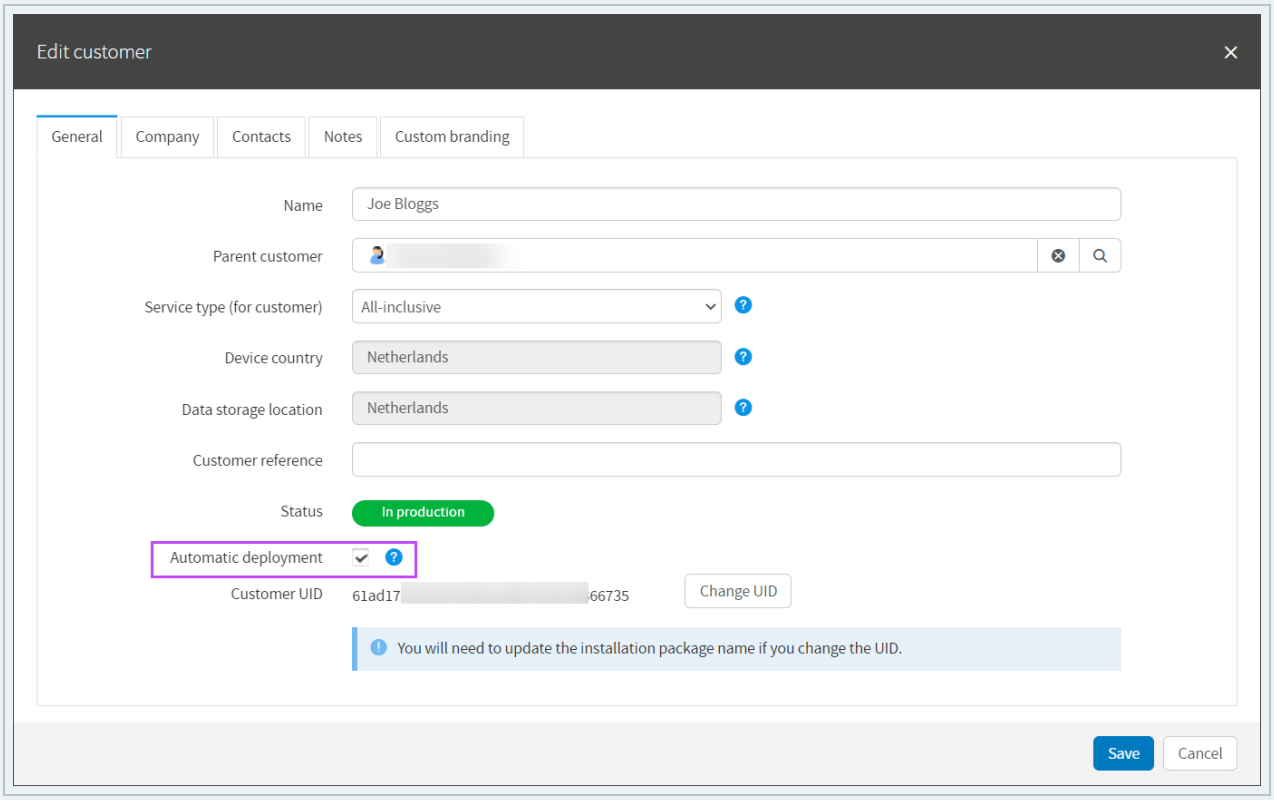


> Documents devices are not associated with any **email addresses**. Therefore it is not possible to set up the delivery of email dashboards on the statuses of recent backup and recovery activities for these devices.

Requirements

- Documents is available to the following types of customers: **resellers** and **end-customers**. A SuperUser account is required to activate the installation. Please request assistance from your service provider if your access permissions are insufficient

  This must be enabled by ticking **Automatic deployment on Windows** in the Customers > Edit Customer screen



- If the system has Microsoft **OneDrive** installed, the **Files On-Demand** feature must be disabled. When the feature is on, the contents of the directory are not physically available on the hard drive. This makes them inaccessible for backup. Learn more

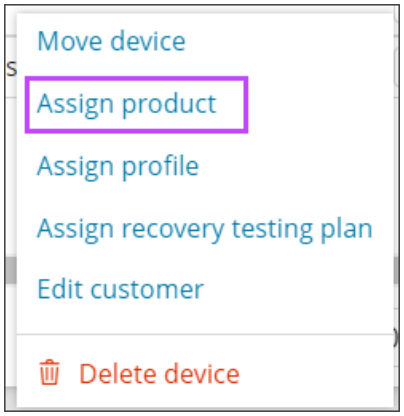
Limitations

- Documents is for the **client versions of Windows and macOS** only. If the installation is performed on a Linux machine or a Windows server, it will not be functional (backups will be blocked)
- It is not possible to change a regular Backup Manager installation to Documents

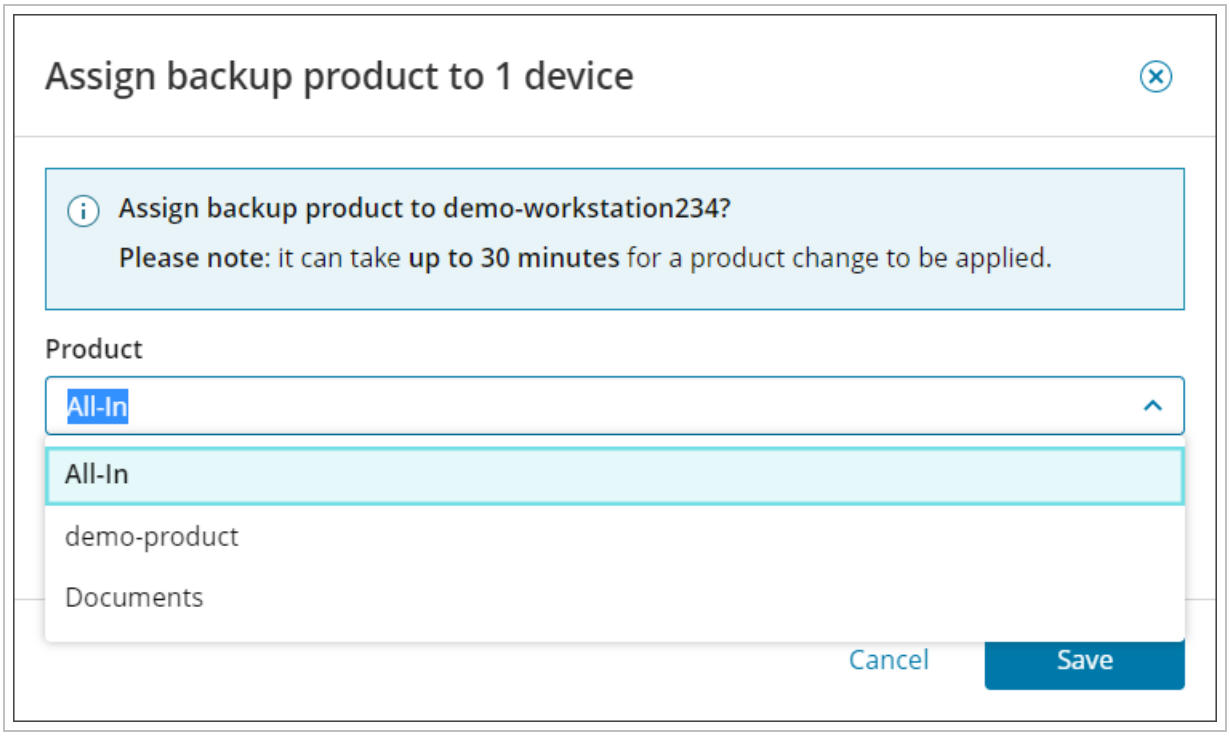
Upgrading options

For more options and flexibility, you can upgrade any Documents device to the standard version.

1. Click the action menu icon to the right of the device you want to upgrade (three vertical dots)
2. Select **Assign Product**



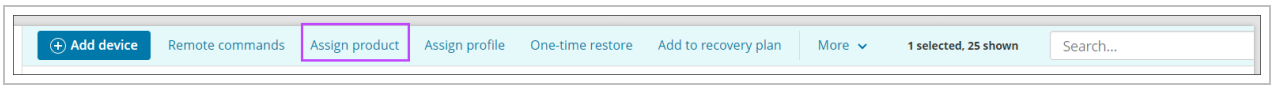
3. Choose a new profile for the device



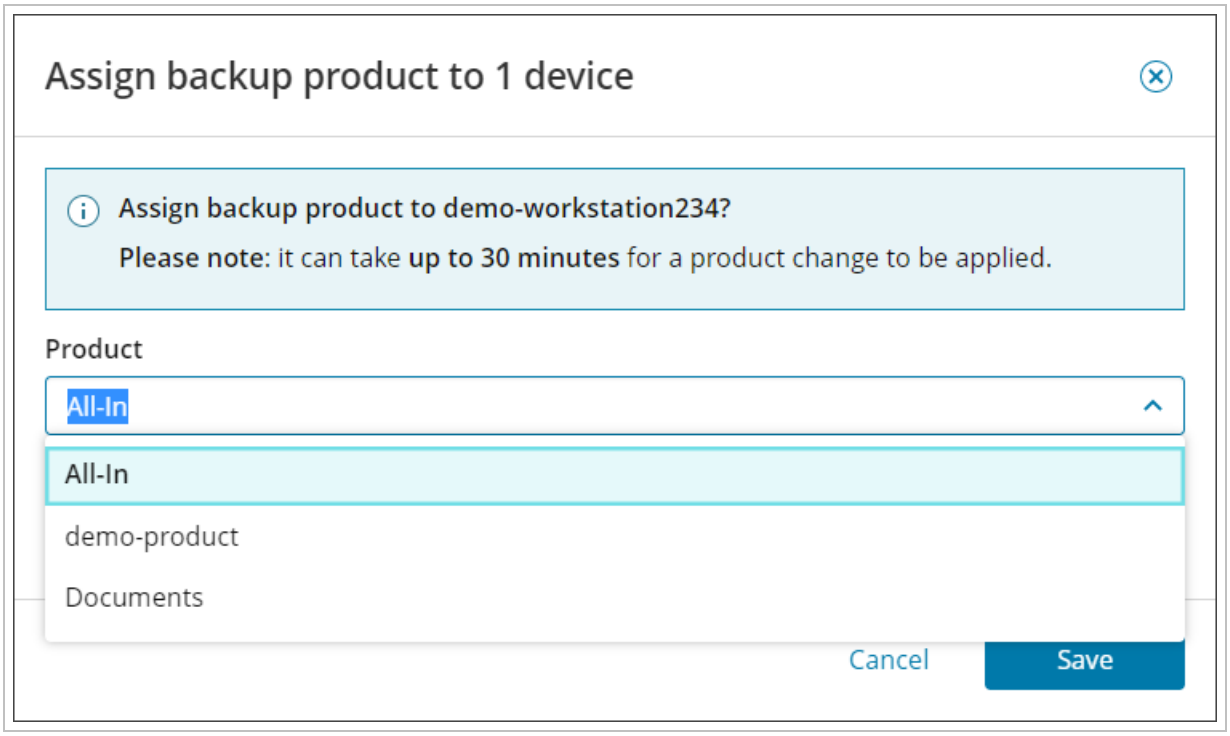
4. Click **Save** to apply the changes

You may also apply a new profile to devices(s) by:

1. Placing a tick in the check box of the device(s) you need to update
2. Select **Assign Product** from the Toolbar



3. Choose a new profile for the device

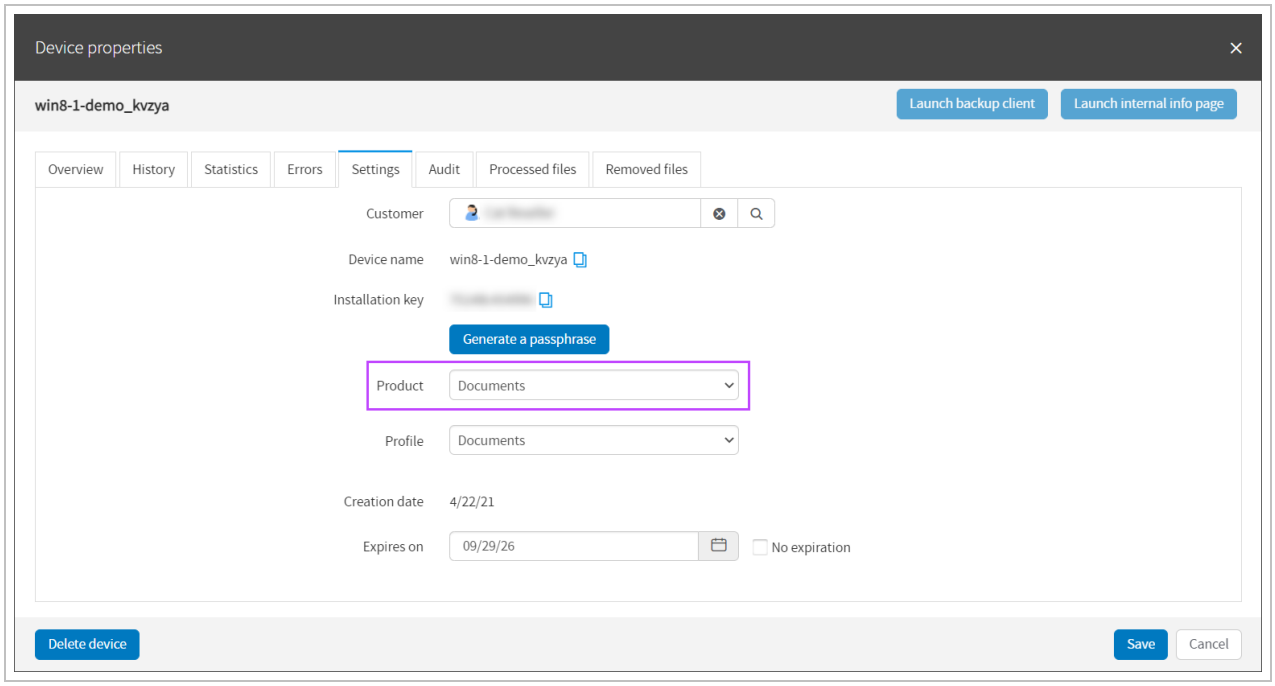


4. Click **Save** to apply the changes

Alternatively, you may upgrade a device by changing its product selection from the **Device Properties** > **Settings** tab.

1. Click on the device name to open its properties
2. Go to the **Settings** tab

3. Change the product selection using the dropdown provided



4. Click **Save** before closing the Device Properties window

A standard Backup Manager device **cannot be downgraded** to Documents.

If the device is turned off, the backup cannot run. It will run when the device has been turned back on.

Features supported by Documents

Documents is the **simplified version** of the Backup Manager. See the tables below for the list of features supported by these versions.

Key

The following icons indicate availability:

Key	Status	Description
✅	Available	Is available for *all*
⚠	Available if additional criteria met	Is available for all, so long as an additional criteria is met (see * for additional information)
⛔	Not Available	Is **not** available

Installation

Feature	Documents	Backup Manager
Compatibility with different operating systems	* [1]	* [2]
Installation wizard	⛔	✅
Quick Installation	* [3]	* [4]
Unlimited number of installations	✅	✅

Backup-related features

Feature	Documents	Backup Manager
One-time backups (initiated manually)	⛔	✅
Scheduled backups	✅ (twice a day)	✅ (user-defined)
Backup profiles	⛔	✅
Flexible backup selection[5]	⛔	✅
Unlimited number of files to back up	✅	✅
Unlimited file size for backup	✅	✅
Support of all file extensions	* [6] - full list	✅
Automatic file selection[7]	⛔	✅
Seed loading backups	⛔	✅

---

[1] Windows client versions and macOS only
[2] Windows client and server versions, macOS and GNU/Linux
[3] initiated by double click or through command-line
[4] initiated through command line
[5] Manual file selection, exclusion filters, priority files
[6] only text files, PDFs, etc
[7] Adding certain types of files to the backup selection automatically (documents, images and videos)

Feature	Documents	Backup Manager
Pre- and post-backup scripts[1]	⛔	✅
LocalSpeedVault[2]	⛔	✅
Archiving[3]	⛔	✅
Detailed reports[4] on the statuses of backup sessions	✅	✅
Backup of open files[5]	⛔	✅
Backup of encrypted files	⛔	✅
Backup of archived files[6]	⛔	✅
Backup of data located on local disks	✅	✅
Backup of data located on removable storage drives	⛔	⚠ *[7]
Backup Accelerator[8]	⛔	✅

Recovery-related features

Feature	Documents	Backup Manager
One-time restores (initiated manually)	✅	✅
Continuous restores (synchronous with backups)	⛔	✅
Flexible data selection	✅	✅

---

[1]For example, shut down the system after backup
[2]A backup copy on a local drive or a network share for faster backups and restores
[3]Archived backup sessions are never deleted from the Cloud
[4]Displayed on the "Overview" tab
[5]Especially files belonging to MS SQL, MS Exchange, MS Hyper-V and MS SharePoint
[6]All common types of archives are supported
[7]if mounted as fixed drives
[8]Speedy subsequent backups of large files

Feature	Documents	Backup Manager
Choice of target location[1]	✅	✅
Detailed reports[2] on the statuses of restore sessions	✅	✅
Bare metal recovery[3]	⛔	✅
Virtual disaster recovery[4]	⛔	✅
Restore-only mode	✅	✅

> ⚠ Documents does not support the Virtual Drive: for quick access to backups feature

General features

Feature	Documents	Backup Manager
Multi-lingual support	⚠ * [5]	⚠ * [6]
Command line interface	⛔	✅
Graphic user interface	✅	✅
Custom branding	✅	✅
Multiple data sources for backup and recovery	⚠ * [7]	⚠ * [8]
Remote commands	⛔	✅
Proxy connection	⛔	✅
Email reports	⛔	✅

---

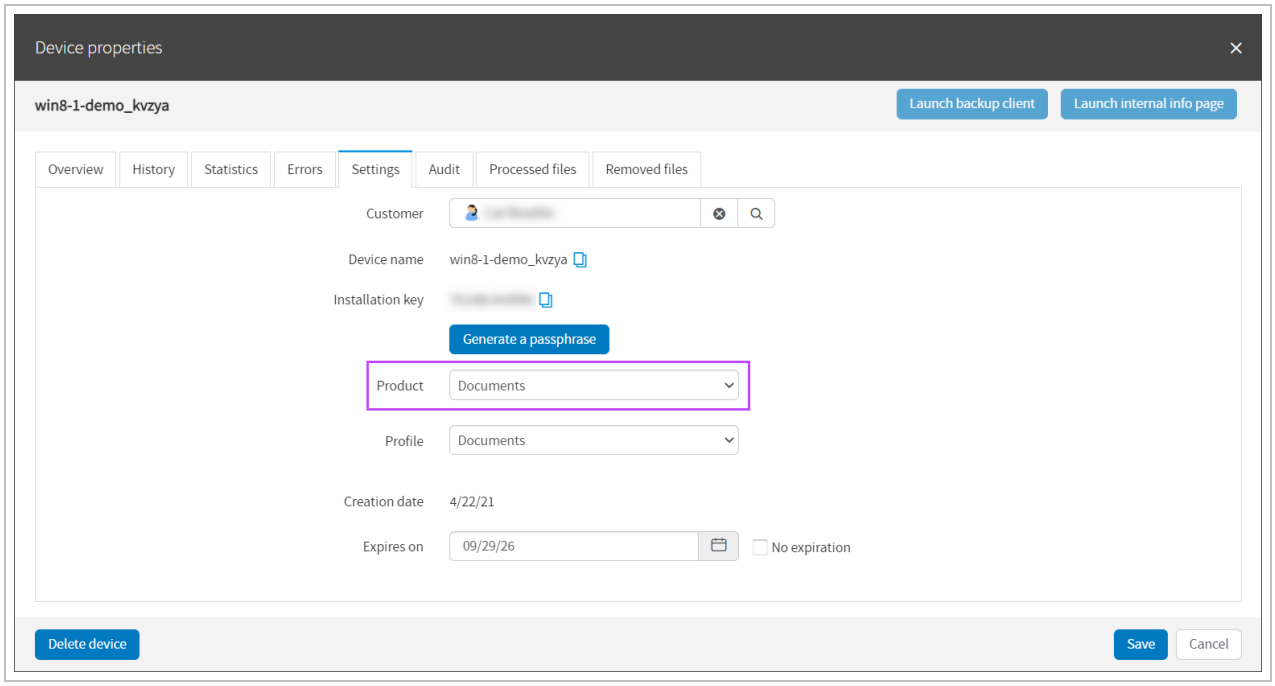
[1]The ability to recover data to the original location or a new one
[2]Displayed on the "Overview" tab
[3]Recovering a failed system directly to bare hardware without a prior OS installation
[4]Recovering a failed system to a virtual machine
[5]English version only
[6]7 interface languages
[7]Files and Folders only
[8]System State, Hyper-V, MS Exchange, etc.

Feature	Documents	Backup Manager
New version updates	✅	✅
Bandwidth usage control	⛔	✅
Advanced data processing technologies[1]	✅	✅

Upgrading options

For more options and flexibility, you can **upgrade** any Documents device to the standard version.

In the Console, open the device properties, go to the **Settings** tab and then change the product selection.



A standard Backup Manager device cannot be **downgraded** to Documents.

File types supported by Documents

All **local** drives are scanned for eligible files during the Documents process. Network Shares are **not** included in this.

Please find below the full list of file types supported by Documents.

This **cannot** be customised.

Images are not classed as key office files and are not included in Documents backup.

---

[1]Deep deduplication, delta slicing, directory hashing, compression, secure encryption, etc.

Text files

Microsoft Word (Office 97-2003)

File extension	File type name
.DOC	Word document
.DOT	Word document template
.WBK	Word backup document

Microsoft Word Open XML (introduced in Office 2007)

File extension	File type name
.DOCB	Word binary document
.DOCM	Word macro-enabled document
.DOCX	Word document
.DOTX	Word document template

Other types of text files

File extension	File type name
.ODT	OpenDocument text document
.PAGES	Pages document
.PSW	Pocket word document
.RTF	Rich text format file
.SDW	StarOffice Writer text document
.STW	StarOffice document Template
.SXW	StarOffice Writer document
.TXT	Plain text file
.UOF	Uniform Office document
.UOT	Uniform Office document
.VOR	StarOffice template
.WPD	WordPerfect document
.WPS	Microsoft Works word processor file

Data files

File extension	File type name
.CSV	Comma-separated values file
.ODC	Office data connection file
.ODF	Apache OpenOffice math file
.ONE	OneNote document
.PST	Outlook personal information store file
.SLK	Symbiotic link file
.XML	Extensible Markup Language data file

Page layout files

File extension	File type name
.ODG	OpenDocument drawing file
.PDF	Portable document format file
.PUB	Microsoft Publisher publication
.XPS	XML paper specification file

Presentation files

Microsoft PowerPoint (Office 97-2003)

File extension	File type name
.POT	PowerPoint template
.PPS	PowerPoint slide show
.PPT	PowerPoint presentation

Microsoft PowerPoint Open XML (introduced in Office 2007)

File extension	File type name
.POTM	PowerPoint macro-enabled presentation template
.POTX	PowerPoint template

File extension	File type name
.PPAM	PowerPoint macro-enabled add-in
.PPSM	PowerPoint macro-enabled slide show
.PPSX	PowerPoint slide show
.PPTM	PowerPoint macro-enabled presentation
.PPTX	PowerPoint presentation
.SLDM	PowerPoint macro-enabled slide
.SLDX	PowerPoint slide

Other types of presentation files

File extension	File type name
.KEY	Keynote presentation
.ODP	OpenDocument presentation
.OTP	OpenDocument presentation template
.SDD	StarOffice presentation
.STI	StarOffice presentation template
.SXI	StarOffice Impress presentation
.UOP	Uniform office presentation

Spreadsheet files

Microsoft Excel (Office 97-2003)

File extension	File type name
.XLM	Excel macro file
.XLS	Excel workbook
.XLT	Excel template

Microsoft Excel Open XML (introduced in Office 2007)

File extension	File type name
.XLSM	Excel macro-enabled workbook
.XLSX	Excel workbook
.XLTM	Excel macro-enabled template
.XLTX	Excel template

Misc. Excel formats

File extension	File type name
.XLA	Excel add-in file that contains macros
.XLAM	Excel add-in file
.XLL	Excel add-in file
.XLSB	Excel binary worksheet (BIFF12)
.XLW	Excel work space

Other types of spreadsheets

File extension	File type name
.DIF	Data interchange format
.NUMBERS	Apple Numbers application file
.ODS	OpenDocument spreadsheet
.PXL	Pocket Excel file
.SDC	Apache OpenOffice Calc spreadsheet
.STC	StarOffice Calc spreadsheet template
.SXC	StarOffice Calc spreadsheet
.UOS	Uniform Office spreadsheet
.XLR	Microsoft Works spreadsheet

Database files

Microsoft Access

File extension	File type name
.ACCDB	Access 2007 database file
.ACCDE	Access execute only database
.ACCDR	Access runtime application
.ACCDT	Microsoft Access database template
.MDB	Microsoft Access database

Other types of database files

File extension	File type name
.DBF	Database file
.PDB	Program database

Vector Image files

Microsoft Office Visio

File extension	File type name
.VDX	Visio Drawing XML file
.VSD	Visio Drawing file
.VDSM	Visio Macro-Enabled drawing
.VSDX	Visio Drawing
.VSL	Visio Add-on
.VSS	Visio Stencil file
.VSSX	Visio Stencil file
.VST	Visio Drawing template
.VSTM	Visio Macro-enabled drawing template
.VSTX	Visio Drawing template
.VSW	Visio workspace file

File extension	File type name
.VSX	Visio Stencil XML file
.VTX	Visio Template XML file

Other types of vector image files

File extension	File type name
.OTG	OpenDocument graphic template
.SDA	StarOffice drawing
.STD	Apache OpenOffice drawing template
.SXD	StarOffice drawing

Compressed files

File extension	File type name
.BDOC	Binary DigiDoc signature file

Backup files

File extension	File type name
.QBB	QuickBooks backup file

Web files

File extension	File type name
.OTH	OpenDocument HTML template

Exclusions for Documents

Certain directories and masks are automatically excluded from backup in Documents.

System data

- `C:\Windows`
- `C:\Program Files`
- `C:\Program Files (x86)`
- `C:\Temp`
- `C:\ProgramData`

- All files indicated in the registry subkey `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`. Typical examples: `\Pagefile.sys`, `\hiberfil.sys` and `%TEMP%\* /s`
- Files/folders matching the following masks:
  - `*\Local Settings\Temporary Internet Files\*`
  - `?:\RECYCLER`
  - `?:\System Volume Information`
  - `%systemdrive%\$WINDOWS.~??` (for example `C:\$WINDOWS.~BT` or `C:\$WINDOWS.~WS`
  - `%SYSTEM_ROOT%/Windows/*.config.cch`
  - `?:\swapfile.sys`
  - `?:\pagefile.sys`
  - `?:\hiberfil.sys`
  - `*\AppData\Local\Temp\*` (in Windows 7)

The exact location of these directories is **detected automatically** for each system.

Temporary files of no value

- `C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer\IconCacheToDelete`. There is such a file for every user account registered in the system.
- `C:\Users\<username>\AppData\Local\Microsoft\Internet Explorer\DomainSuggestions`. There is such a file for every user account registered in the system.
- `C:\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit`
- Files from the **Print Spooler** folder

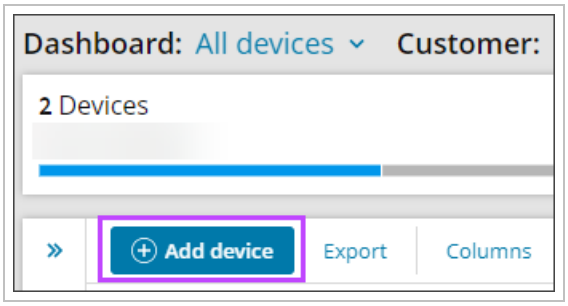
Other filters

Files from the Documents installation folder are not backed up.

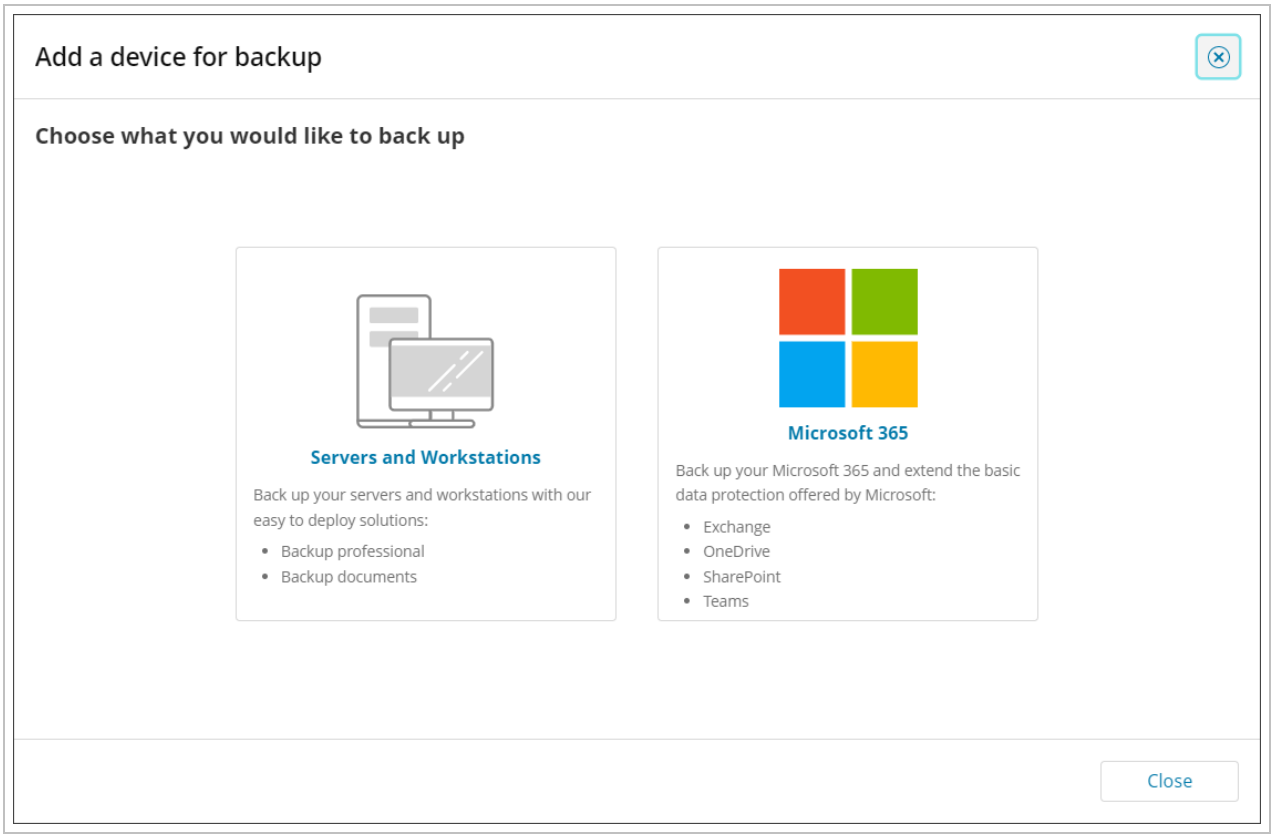
Documents installation instructions

In Documents, operations for device creation, installation and setup are automated. Here are steps to follow:

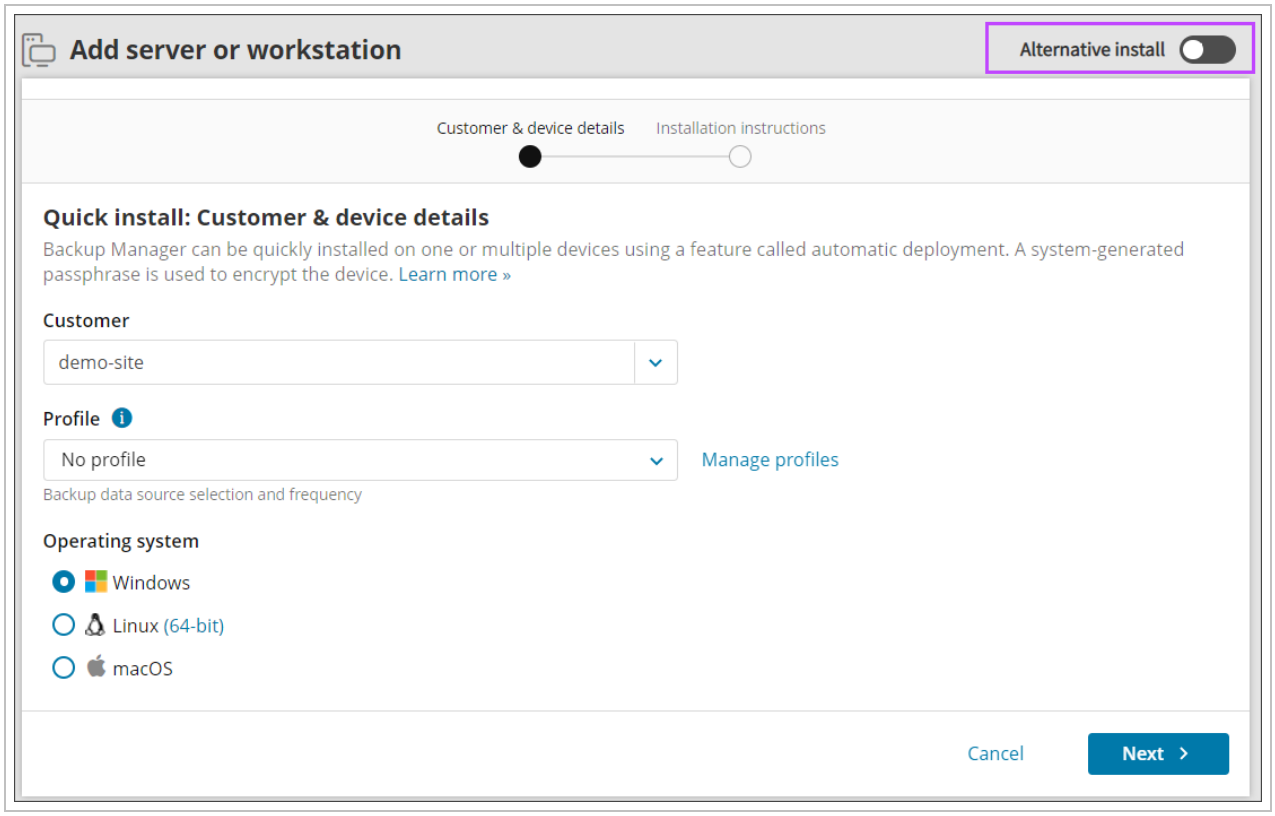
1. Log in to the Management Console under a SuperUser account belonging to a reseller or end-customer



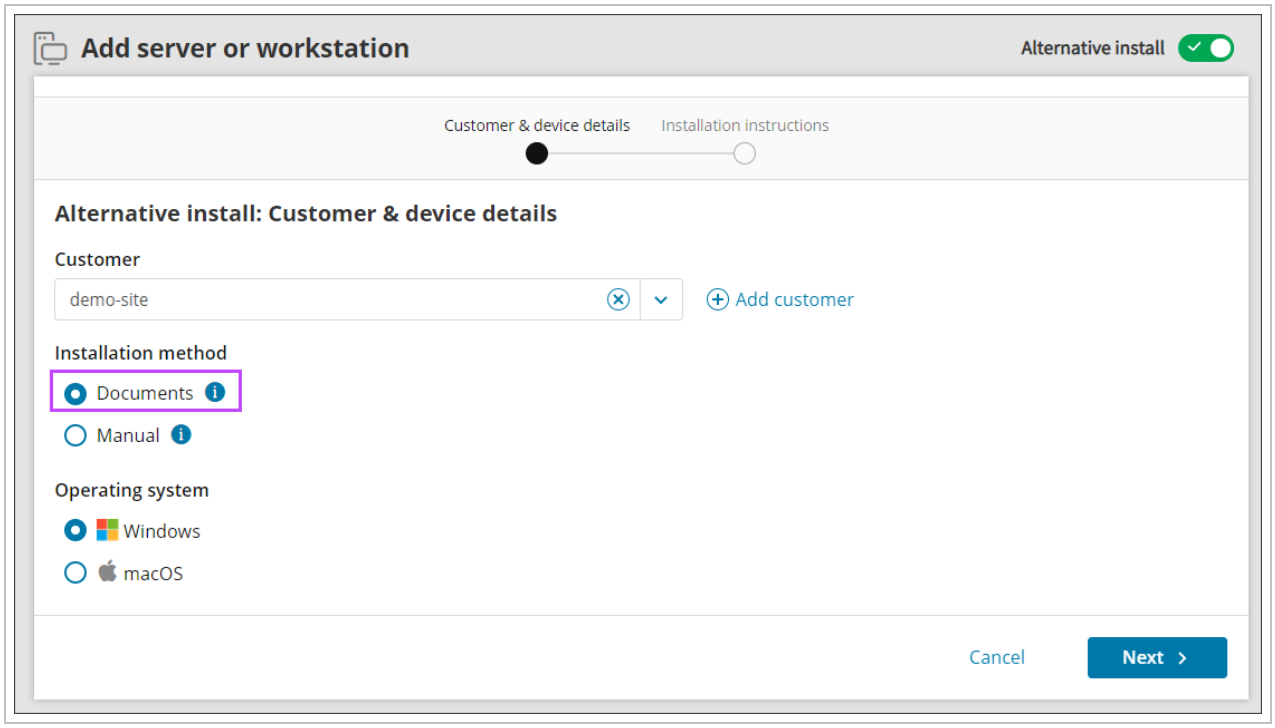
2. Click **Add device**, select **Servers of Workstations**



3. Using the toggle in the upper right-hand corner of the wizard, enable **Alternative install**

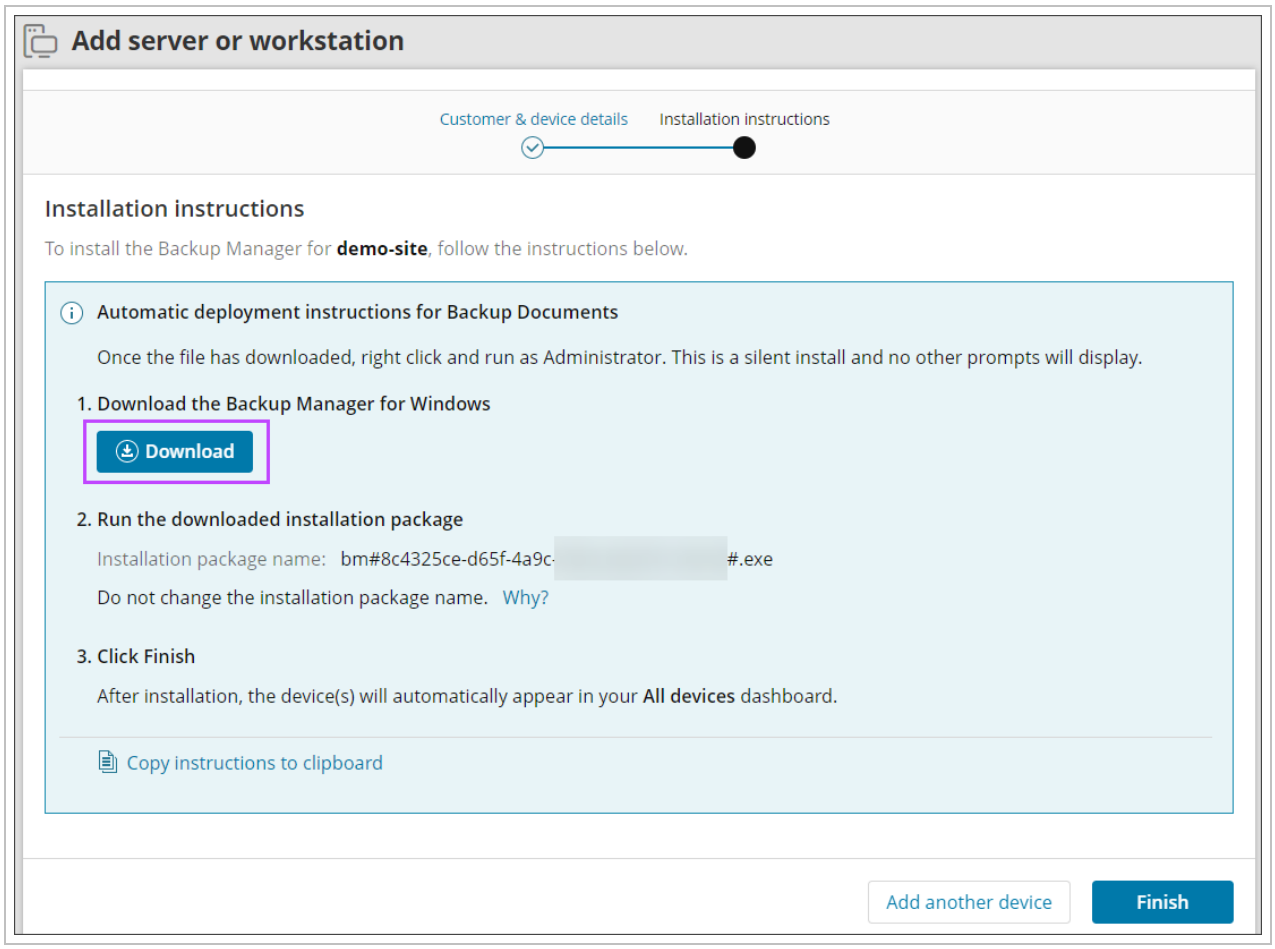


4. Select the **Customer** to install the device for from the dropdown
5. Choose the **Documents** Installation method



6. Select the Operating System for your device:
   - Windows
   - macOS
7. Click **Next**
8. Download the **installation package** from the download link and take a note of the **installation package name**

> Do **not** change the installation package name from the one provided on your dialog. This is because the package name is a unique identifier for the specific customer and doing so would stop the installation from functioning appropriately.



9. Click **Finish**
10. Run this installer on any number of machines to enable Documents

> If the installer does not run after downloading, check the file has not been renamed by your system and check properties of the install file to ensure that it has not been blocked by your system upon download. Attempt to run as the Administrator on the device.

Ways to **run the installation package**:

- Double-click on the installer executable
- Submit the name of the installer to a terminal emulator or a software distribution system. For example: `demobm#a55x00rf-d604-429e-1f87-n800004e755#5038#.exe`

> Please note, the installer name will be specific to you.

> If you ever need to re-install a Documents device, please follow instructions for automatically installed devices.

Restoring data in Documents

In Documents, all primary restore options are available:

- The ability to restore any file version from a backup in the last 28 days
- The ability to select files or directories for restore
- Search for files and directories available for restore
- Restoring data to the original location or to a new one
- The restore-only mode (activated through device re-installation with the `-restore-only` flag)

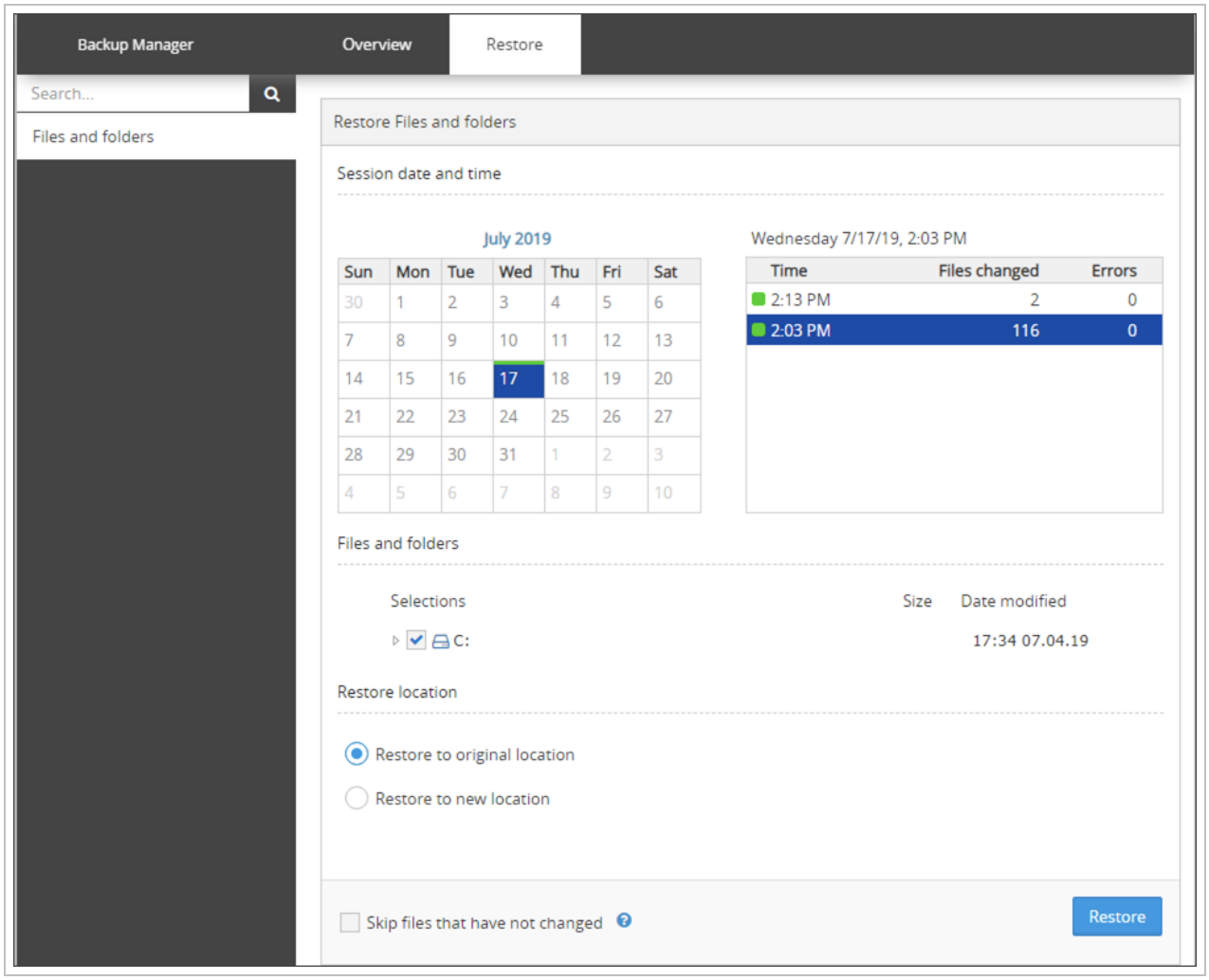
Instructions

Restoring data via the Backup Manager works the same way for Documents as it does for a full backup.

1. Launch the Backup Manager for the device

   > If you are restoring date to a new device, this can be done by using Backup Manager Restore-Only Mode

2. Open the **Restore** tab
3. Select the backup session you want to restore from using the **Session Date and Time** selection
   - **(A)**means that the session is archived (more on backup session archiving)
   - **(L)** means that the session has been saved locally in the LocalSpeedVault and the data is not synchronized with the cloud yet
4. Select the data you want to restore using the file tree to select the full data source or select individual files or directories
5. Specify where to restore the selected data:
   - to the original location
   - to a new location: enter the target location
6. Select **Skip files that have not changed** if you wish to only restore files which have been modified between the date of backup and the date of restore
7. Click **Restore** and wait until the restore process is completed



Some of the standard features are restricted:

- Restoring data through the Recovery Console
- Virtual disaster recovery
- Bare metal recovery
- Restoring data to network shares or remote servers

Glossary of Cove Data Protection (Cove) terms

Glossary of Cove Data Protection (Cove) terms

Backup Manager

The Backup Manager is the part of Cove Data Protection (Cove) installed on the backup devices which runs the backup and one method of recovery. The Client is a web application, or command line interface where you configure the backup selection and schedule, along with other additional settings.

What's inside:

Backup Manager installation guide

> We strongly **do not** recommend downgrading Backup Manager to a lower version after installation is complete. In cases where the Backup Manager has been downgraded, we cannot guarantee the application will function correctly.

Windows and macOS installers

The Backup Manager is installed with the help of an **installation wizard** on Windows and macOS computers. After the installation, the tool opens as a web application.

- Quick Installation of the Backup Manager
- Manual installation on Windows and macOS

The Backup Manager can be used in any of these 9 languages:

- English
- Dutch
- Russian
- German
- Spanish
- French
- Portuguese
- Norwegian
- Italian

GNU/Linux installers

Linux and FreeBSD users must install the Backup Manager software through the **command line**.

After the installation and initial set-up, the Backup Manager can be accessed both through the command line and as a web application like on Windows and macOS.

- Backup Manager Installation on GNU/Linux

System requirements for Backup Manager

Hardware requirements

- 2 GB of computer memory (RAM)
- Dual-core processor or better
- 150 MB of free disk space (for installation)
- Screen resolution of 1024 x 768 pixels or higher
- High-speed Internet connection

The amount of **free disk space** required for future usage depends on the size of your backup selection and whether you have enabled a local storage directory (LocalSpeedVault).

macOS requirements

Newer hardware macOS devices use M1 chips, running on Apple silicon. Backup Manager runs in Intel emulation mode on M1 chipped devices.

For the following models (and newer), Rosetta 2 be installed to allow for Intel emulation:

- iMac 21.2
- Mac mini 9.1
- MacBook Air 10.1
- MacBook Pro 17.1
- MacBook Pro 18.1
- MacBook Pro 18.2
- MacBook Pro 18.3
- MacBook Pro 18.4

Software requirements

Supported operating systems

You can back up and restore data located on Windows OS, macOS and GNU/Linux. Please see the table below for the full list of supported operating systems:

Windows versions	macOS versions	GNU / Linux versions
▪ Windows 8 / 8.1 ▪ Windows 10 ▪ Windows 11 ▪ Windows Server 2012 / 2012 R2 (limited[1])	▪ 10.15 Catalina ▪ 11 Big Sur ▪ 12 Monterey ▪ 13 Ventura	▪ CentOS 5, 6, 7 ▪ Debian 5, 6, 7, 8 ▪ OpenSUSE 11, 12

[1]New features such as Docker-based containers, Storage Spaces Direct and Shielded VMs are not.

Windows versions	macOS versions	GNU / Linux versions
▪ Windows Server 2016 (limited[1]) ▪ Windows Server 2019 (limited[2]) ▪ Windows Server 2022 (limited[3])	▪ 14 Sonoma	

Parallels are not officially supported for Backup Manager when backing up macOS with Windows parallels. If you wish to use Backup Manager in this situation, there may be abnormalities so please test the backup by doing a restore as soon as possible. Two backup accounts may be necessary to backup both the macOS Files and Folders and the Windows Files and Folders.

Backup on devices using Operating Systems which are not officially supported may still work, but as we no longer test these versions, we cannot guarantee full functionality. In situations where the device cannot be upgraded to a supported OS, you may encounter issues with new features, or there may be abnormalities so please test the backup by doing a restore as soon as possible.

Note for Windows:

On Windows devices, Backup Manager supports 32 or 64-bit architecture.

Note for macOS:

Pre 10.14 Mojave: as of version 21.10 of Backup Manager, macOS versions prior to 10.14 are no longer officially supported.

10.14 Mojave and later releases: Ensure you enable macOS Full Disk Access for the Backup Manager *before* running backups.

Note for GNU/Linux:

In addition to the major Linux distributions that are regularly tested in-house, it is possible to run the Backup Manager practically on any GNU/Linux distribution that meets the following requirements:

- Architecture: **x86** or **x86_64/amd64**
- Kernel: **2.6.9+** with NPTL
- glibc: **2.4** or greater (all data sources except for MySQL); **2.5** or greater for the backup and recovery of MySQL
- LVM for the backup and recovery of the system state

Supported web browsers

Most web browsers that have **JavaScript** on are supported. We **recommended** the following browsers:

---

[1]Only the features compatible with Windows Server 2012 R2 are supported.
[2]Only the features compatible with Windows Server 2012 R2 are supported.
[3]Only the features compatible with Windows Server 2012 R2 are supported.

- Google Chrome
- Mozilla Firefox
- Safari for macOS (limitation[1])
- Microsoft Edge

TLS

Cove Data Protection (Cove) requires the use of Transport Layer Security Protocol (TLS), the supported versions of this being:

- 1.2
- 1.3

> Previous versions of TLS have been deprecated and are no longer supported.

Firewall

The Backup Manager relies on the following ports:

1. Port **443** TCP outbound. It is almost always open on workstations but may be closed on servers
2. Local port **5000**. If this port is unavailable, the Backup Manager detects a free port automatically (starting from 5001, 5002 and up)

> In most cases, no firewall configuration is required.

DNS

The DNS should also be accepted if router or firewall rules are in place to allow full communication to all storage nodes:

- *.cloudbackup.management
- *.iaso.com
- *.backup.management
- *.mob.system-monitor.com

Antivirus

The following paths and executables should be added to the antivirus exclusions list of any device where Backup Manager is installed:

---

[1]If the name of a directory contains a letter with the "umlaut" symbol (ä, ü, ö), it may not be possible to view the contents of the directory in the restore selection. If you experience the issue, please open the Backup Manager in another browser, for example Google Chrome.

- Paths:
  - C:\Program Files\Backup Manager
  - C:\ProgramData\Managed Online Backup
  - C:\ProgramData\MXB
  - Virtual drive location (typically B:)
- Executables:
  - C:\Program Files\Backup Manager\ClientTool.exe
  - C:\Program Files\Backup Manager\ProcessController.exe
  - C:\Program Files\Backup Manager\BackupFP.exe
  - C:\Program Files\Backup Manager\BackupIP.exe
  - C:\Program Files\Backup Manager\BackupUP.exe
  - C:\Program Files\Backup Manager\BRMigrationTool.exe

Note - the device must be online and the **BackupFP.exe** process must be running

Quick Installation of the Backup Manager

We strongly **do not** recommend downgrading Backup Manager to a lower version after installation is complete. In cases where the Backup Manager has been downgraded, we cannot guarantee the application will function correctly.

System administrators can quickly install the Backup Manager on multiple machines using the **Automatic Deployment** method (also known as **quick installation**).

This automates the operations for device creation, installation and – optionally – setup.

A single executable file is good for an **unlimited** number of installations for the specified customer

Quick Installation is available on Windows, macOS and Linux operating systems.

Quick Installation vs. Silent installation vs. Manual installation

Three installation methods available are:

1. **Quick Installation** – The Automatic Deployment feature lets you install Backup Manager on multiple devices simultaneously
2. **Silent Installation** – lets you install one device at a time using the command line on Windows
3. **Manual Installation** - lets you install one device at a time manually

Please see the table below for the differences between these options.

	Quick Installation	Silent installation	Manual Installation
Supported versions	All Windows, macOS and Linux on which Backup Manager works (full list)	All Windows, macOS and Linux on which Backup Manager works (full list)	All Windows, macOS and Linux on which Backup Manager works (full list)
Feature availability	Only resellers and end-customers	All types of customers	Only resellers and end-customers
Number of installations	Multiple devices simultaneously	One device at a time	One device at a time
Details required for installation	Installation command (generated automatically)	1. Device name 2. Device password/installation key 3. security code/encryption key	1. Device name 2. Device password/installation key 3. security code/encryption key

We **do not** store the Security Code/Encryption Key of a device, this must be kept by yourself as it **cannot** be retrieved in our system if lost.

Requirements

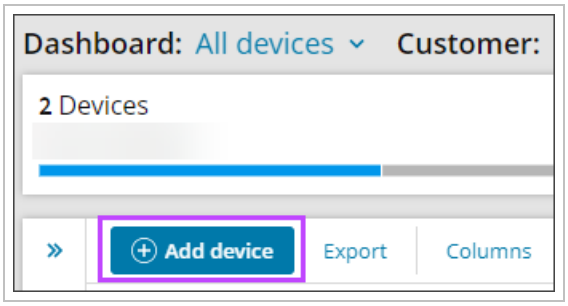
- A **SuperUser** account is required at the reseller or end-customer level

  Please request assistance from your service provider if your access permissions are insufficient.
- The Automatic Deployment option must be enabled at the customer level. See Enable Automatic Deployment for further details

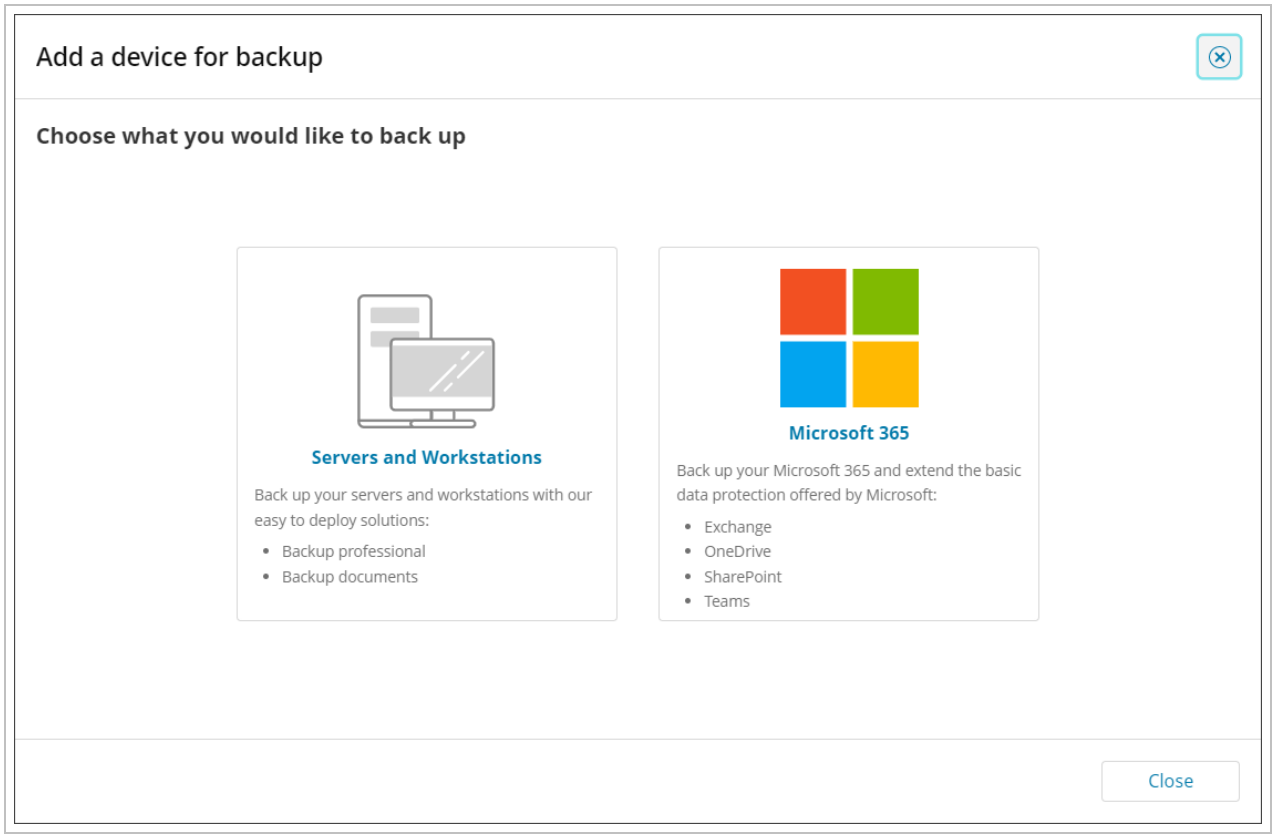
Instructions

Adding devices for installation:

1. Log in to the Console under a SuperUser account belonging to a reseller or end-customer



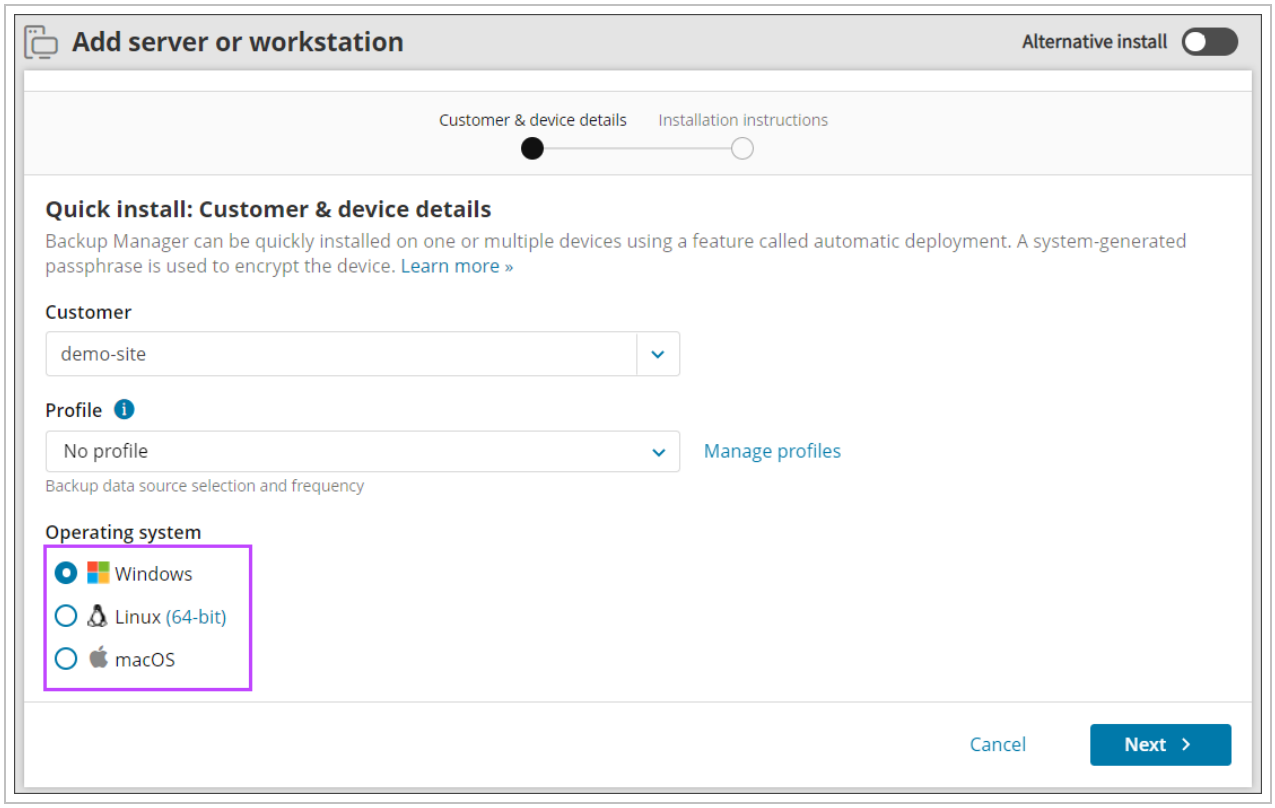
2. Click **Add devices**, select **Servers of Workstations**



3. Select the customer to install the device for from the dropdown
4. Select a backup profile (optional)

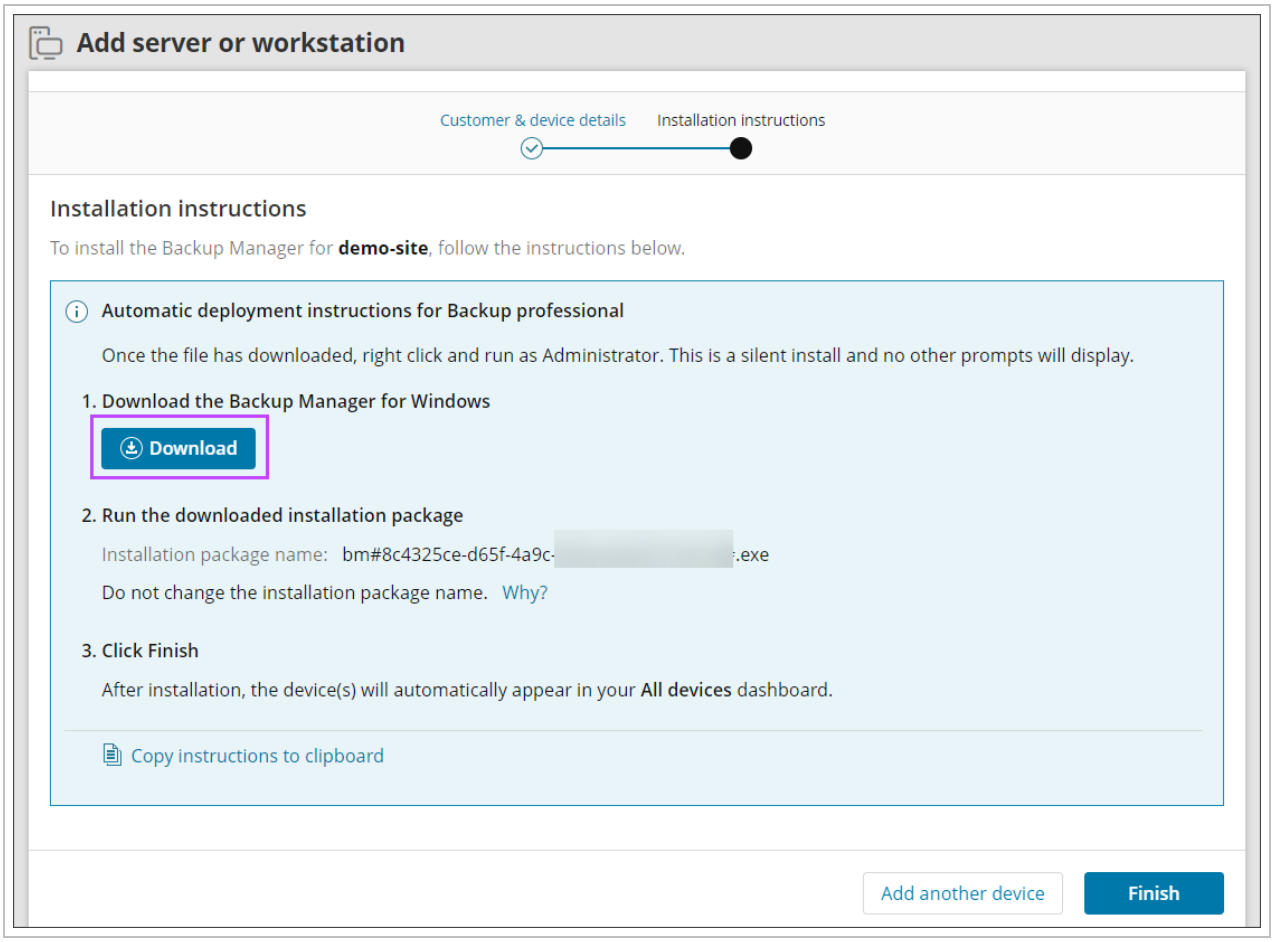
> Backup profiles let you configure multiple devices for backup simultaneously (learn more).

5. Select the operating system for the device



6. Click **Next**
7. Download the **installation package** from the download link and take a note of the **installation package name**

> Do **not** change the installation package name from the one provided on your dialog. This is because the package name is a unique identifier for the specific customer and doing so would stop the installation from functioning appropriately.



8. Click **Finish**
9. Run the Installation package on the device where the backup is required

> If the installer does not run after downloading, check the file has not been renamed by your system and check properties of the install file to ensure that it has not been blocked by your system upon download. Attempt to run as the Administrator on the device.

Ways to **run the installation package**:

- Double-click on the installer executable
- Submit the name of the installer to a terminal emulator or a software distribution system. For example: `demobm#a55x00rf-d604-429e-1f87-n800004e755#5038#.exe`

> Please note, the installer name will be specific to you.

Windows Only

On Windows devices you can run the installation command as-is or, optionally, you can add additional parameters to it if required.

Parameters

Required parameters

Parameter	Description	Supported values
`-unattended-mode`	This flag activates the Quick Installation feature. It also prevents the Backup Manager from starting automatically after the installation.	N/A (enter the parameter as is)
`-partner-uid`	This is a unique ID generated for the partner (required for authorization). You can regenerate the UID[1] as often as necessary. This will not affect any of the previous installations.	Text (copied from the management console)
`-unattended-mode-partner-uid` (legacy)	This is the parameter used instead of `-partner-uid` prior to the May 2017 release. It is still supported and can be used in the same way as `-partner-uid`.	Text (copied from the management console)

Proxy settings (optional)

Parameter	Description	Supported values
`-use-proxy`	This setting prompts the Backup Manager to connect to the Internet through a proxy server.	▪ `1` (use a proxy connection) ▪ `0` (do not use a proxy connection) - default
`-proxy-type`	The type of the proxy server	▪ `HTTP` ▪ `SOCKS4` ▪ `SOCKS5`
`-proxy-address`	The host name or IP address of the proxy server	IP address or host name, for example `192.188.33.55` or `some.server.com`
`-proxy-port`	The port number of the proxy server	Number (0 by default)
`-use-proxy-authorization`	Prompts the Backup Manager that the proxy requires authorization by username.	▪ `1` - the proxy requires authorization ▪ `0` - the proxy does not require authorization (default)
`-proxy-user-name`	A username for access to the proxy server	Text, for example `domain\username` or `username`
`-proxy-pass-word`	A password for access to the proxy server	Text

[1] In the Console, click to edit the customer to change the UID for. On the "General" tab, click "Change UID".

Misc. optional parameters

Parameter	Description	Supported values
`-profile-name`	The name of the backup profile you want to assign to the new device (s). This setting lets you configure devices for backup during installation.	Text
`-profile-id`	The ID of the backup profile you want to assign to the new device(s). To use the parameter, you need Backup Manager installer version **17.4** or later. Profile IDs are generated automatically when the automatic deployment is enabled. You can use the profile ID and profile name interchangeably.	Number (copied from the management console)
`-product-name`	The name of the product to assign to the new device(s). To use the parameter, you need Backup Manager installer version **17.4** or later.	Text (copied from the Console)
`-storage-id`	The ID of the storage pool used for the device(s).	Number (automatically inserted during the executable creation)

Re-installing automatically deployed devices

When re-installing a regular backup device, the process is the same as when installing a device for the first time. However, the process is slightly different when re-installing a device that was created and installed through **Quick Installation**. This is because the security codes/encryption keys for automatically deployed devices are generated by the system and so no-one knows these details.

In order to re-install an automatically deployed device you must:

1. Get the passphrase (Instructions on this can be found here - Getting passphrases for automatically installed devices)
2. Run the installation using the passphrase instead of the security code/encryption key

You can run the installation through the set-up wizard or in the silent mode.

Silent mode re-installation instructions

Silent mode can be used for devices using both Windows and Linux operating systems. In the silent mode, there are three required parameters:

1. `-user` - the name of the device you are re-installing (copied from the Console)
2. `-password` - the installation key associated with the device name (copied from the Console)
3. `-passphrase`- a system-generated security code for automatically deployed devices

The list of optional parameters is the same as for a new installation.

Here is a sample command on Windows:

```
mxb-windows-x86_x64.exe -silent -user "support_win_jab67v" -password
"Secureh0982b2bxgt" -passphrase "914hahdgf-0000-example"
```

Here is a sample command on Linux:

```
mxb-linux-x86_64.run -- --user=" support_win_jab67v" --password="
Secureh0982b2bxgt" --passphrase=" 914hahdgf-0000-example"
```

Please make sure you submit all values with punctuation characters in **straight double quotes**

Getting passphrases for automatically installed devices

Access to automatically deployed devices is given via passphrase-based (system-generated security code) encryption.

Use the passphrase in any field asking for an **Encryption key** or **Security Code**

Passphrases are required to perform operations requiring security permissions:

- Re-installing devices
- Installing devices on a different computer for restore purposes
- Adding devices to the Recovery Console
- Adding a Recovery Testing plan to a device

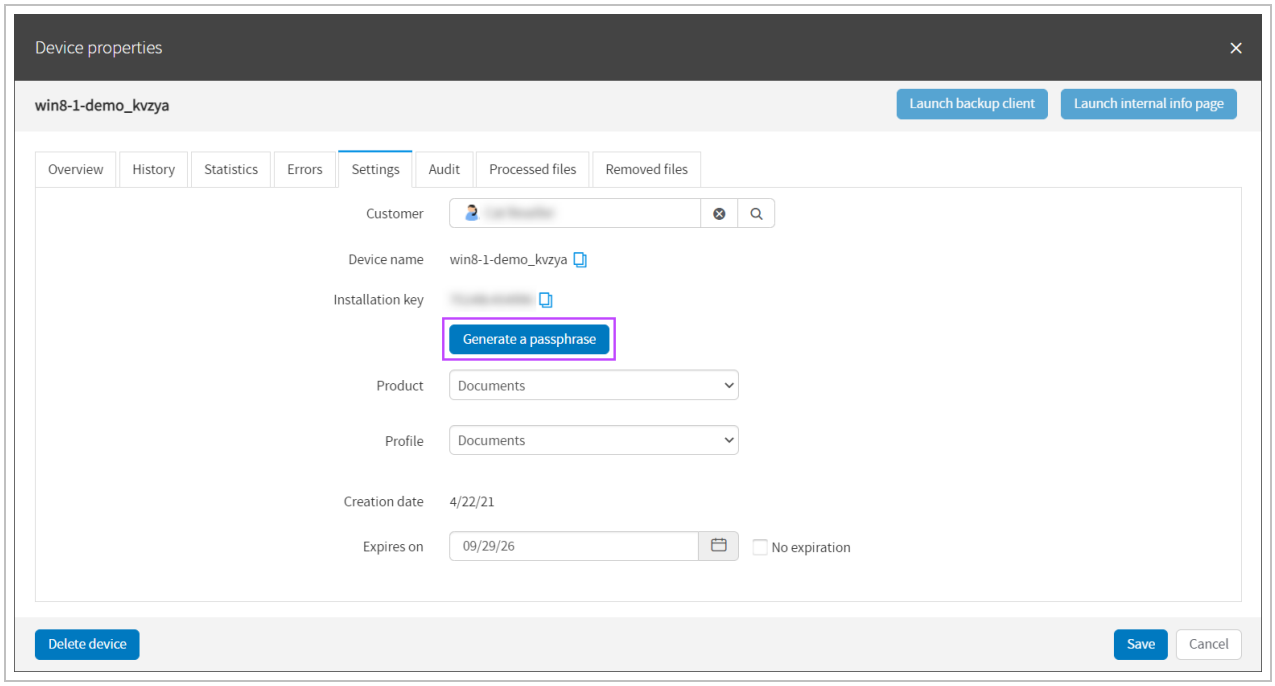
Passphrases are generated upon request and are valid for 24 hours, but for **one-time use only**.

Get Passphrase

Passphrases are securely accessible from the Management Console:

1. Log in to the Management Console as a user with Security officer permissions
2. Click the name of the device that you need a passphrase for to open the **Device Properties** window
3. Switch to the **Settings** tab
4. Click **Generate passphrase**

5. Once the passpgrase is generated, take a copy of this to carry out the required work



If you do not have the **Generate passphrase** option, go to **User management** and make sure you are logged in under the right user account and that the device was installed using Automatic Deployment.

Convert devices to passphrase-based encryption

If you have lost or forgotten the security code/encryption key for a backup device, or simply no longer wish to individually manage security codes/encryption keys for your list of backup devices, Backup Manager offers the function to convert backup devices to use a passphrase-based encryption method.

Please be aware that once this change is made, you **cannot** change back to use the original security code/encryption key if found at a later date.

Differences between encryption methods

- **Private key encryption** relies on encryption keys/security codes that are defined by users during Backup Manager installation. The encryption key/security code is set once and cannot be changed or retrieved afterward
- **Passphrase-based encryption** uses a system-generated encryption key that is securely accessible from the management console

Requirements

1. Backup Manager version 17.11 or later must be installed and functional on the system you wish to convert
2. The system must be running on Windows
3. The system must be intact (the conversion process will not work after a system is lost, destroyed or infected)

4. Access to run the Command Prompt as an administrator is required on each system you wish to convert
5. Backups should not be actively running during this process

Instructions

Step 1. Get a partner UID for conversion

1. Log in to the Console as a user with security officer permissions
2. In the Management section of the vertical menu, click **Customers** to open the **Customer Management** window
3. Find the customer containing backup devices you want to convert
4. Click the three dots to the right to access the Action Menu
5. Click **Edit Customer**
6. On the General tab, scroll down and enable the **Automatic Deployment** option (if it is disabled)
7. Click **Save**
8. Copy the **Customer UID** for later use as the `-partner-uid` parameter

> You can re-use the UID for any number of devices belonging to the customer.

Step 2. Perform conversion on each device

Windows devices

Run the below command on each Windows device you plan to convert to passphrase-based encryption.

1. Log in to the system on which the backup device is installed
2. Start the Command Prompt as an administrator
3. Run the following command

```
"C:\Program Files\Backup Manager\ClientTool.exe" takeover -partner-uid
[Customer UID from Management Console] -config-path "c:\Program Files\Backup
Manager\config.ini"
```

The components contained in the command are:

- `C:\Program Files\Backup Manager\` - is the default installation directory of the Backup Manager. Make sure you edit the path if the Backup Manager is installed at a custom location
- `ClientTool.exe` - an executable file included into all Backup Manager installations. It lets you operate the Backup Manager through the command line
- `takeover` - a command that moves a backup device to another category (to another customer or to passphrase-based encryption)
- `partner-uid` - the **Customer UID** you copied at step 1.6

Linux devices

Run the below command on each Linux device you plan to convert to passphrase-based encryption.

1. Log in to the system on which the backup device is installed
2. Start the terminal
3. Run the following command

```
"/opt/backup-manager/bin/ClientTool" takeover -partner-uid [Customer UID from
Management Console] -config-path "/opt/MXB/etc/config.ini"
```

The components contained in the command are:

- `/opt/backup-manager/` - is the default installation directory of the Backup Manager. Make sure you edit the path if the Backup Manager is installed at a custom location
- `ClientTool` - an executable file included into all Backup Manager installations. It lets you operate the Backup Manager through the command line
- `takeover` - a command that moves a backup device to another category (to another customer or to passphrase-based encryption)
- `partner-uid` - the **Customer UID** you copied at step 1.6

MacOS devices

Run the below command on each MacOS device you plan to convert to passphrase-based encryption.

1. Log in to the system on which the backup device is installed
2. Start the terminal
3. Run the following command

```
"/Applications/Backup Manager.app/Contents/MacOS/ClientTool" takeover -
partner-uid [Customer UID from Management Console] -config-path
"/Library/Application Support/MXB/Backup Manager/config.ini"
```

The components contained in the command are:

- `/Applications/Backup Manager.app/` - is the default installation directory of the Backup Manager. Make sure you edit the path if the Backup Manager is installed at a custom location
- `ClientTool` - an executable file included into all Backup Manager installations. It lets you operate the Backup Manager through the command line
- `takeover` - a command that moves a backup device to another category (to another customer or to passphrase-based encryption)
- `partner-uid` - the **Customer UID** you copied at step 1.6

Step 3. Test the conversion (optional)

Now you can run a test to make sure the device has been successfully converted to passphrase-based encryption. Here are steps to follow:

1. Get a passhprase (instructions)
2. Add the device to the Recovery Console with that passphrase or install the device on an additional machine in the restore-only mode

If you have at least one backup session completed on the device, you can go even further and **run a test restore**.

> It is a good practice to periodically test your security codes or passphrases this way.

Backup Manager Installation on GNU/Linux

> We strongly **do not** recommend downgrading Backup Manager to a lower version after installation is complete. In cases where the Backup Manager has been downgraded, we cannot guarantee the application will function correctly.

> By default Linux devices are recognised as server licenses on any invoices for Backup Manager. This **cannot** be changed.

To install Backup Manager on GNU/Linux devices, three installation methods are available:

1. RUN installer - The command line interface requires minimum settings and suits **all** modern Linux distributions
2. DEB - This method is available for modern **Debian** and **Ubuntu** distributions
3. RPM - This method is available for modern **CentOS**, **RHEL** and **SUSE** distributions

After the installation is complete, you will be able to run Backup Manager using:

- The command line interface
- The graphical user interface, e.g. Backup Manager client

Manual Installation on GNU/Linux

> We strongly **do not** recommend downgrading Backup Manager to a lower version after installation is complete. In cases where the Backup Manager has been downgraded, we cannot guarantee the application will function correctly.

The most convenient way to install the Backup Manager on a GNU/Linux device is using the RUN installer.

The RUN installer comes in 2 versions:
1. i386 - for 32-bit systems
2. amd64 - for 64-bit systems

> Ensure you use the correct one for the system before beginning

Precursor check:

Before beginning, check the bitness of your system first by running the following command in the command line of the device:

```
# uname -m
```

The response will be one of two:

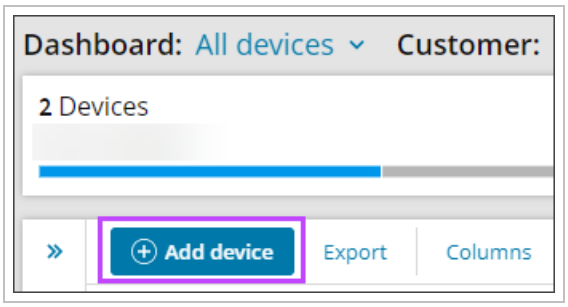
- `x86_64` - you have a 64-bit system so you require the **amd64** installer
- `i686`- you have a 32-bit system so you require the **i386** installer

Installation steps

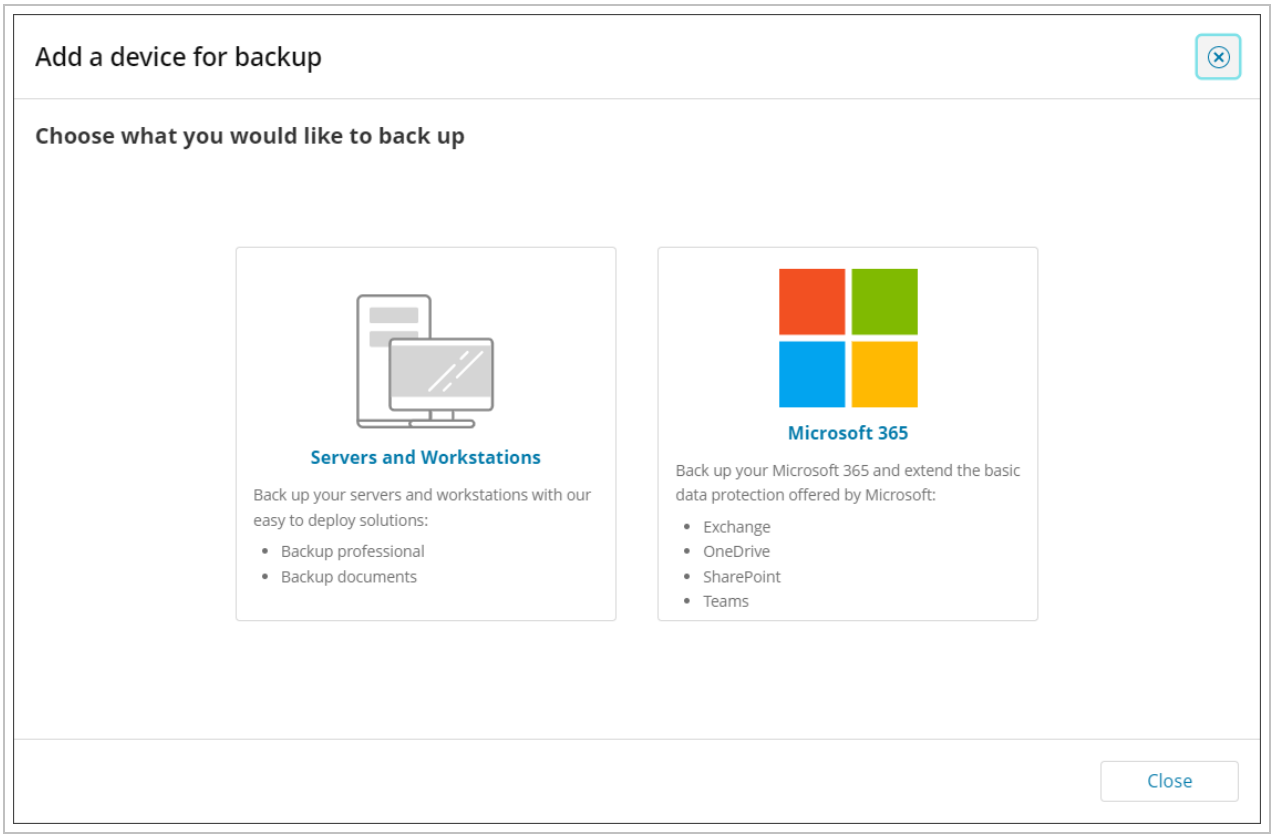
> These steps detail running commands for a 32-bit system. If your device is a 64-bit system, replace `i686` everywhere below with `x86_64`

Step 1: Add device

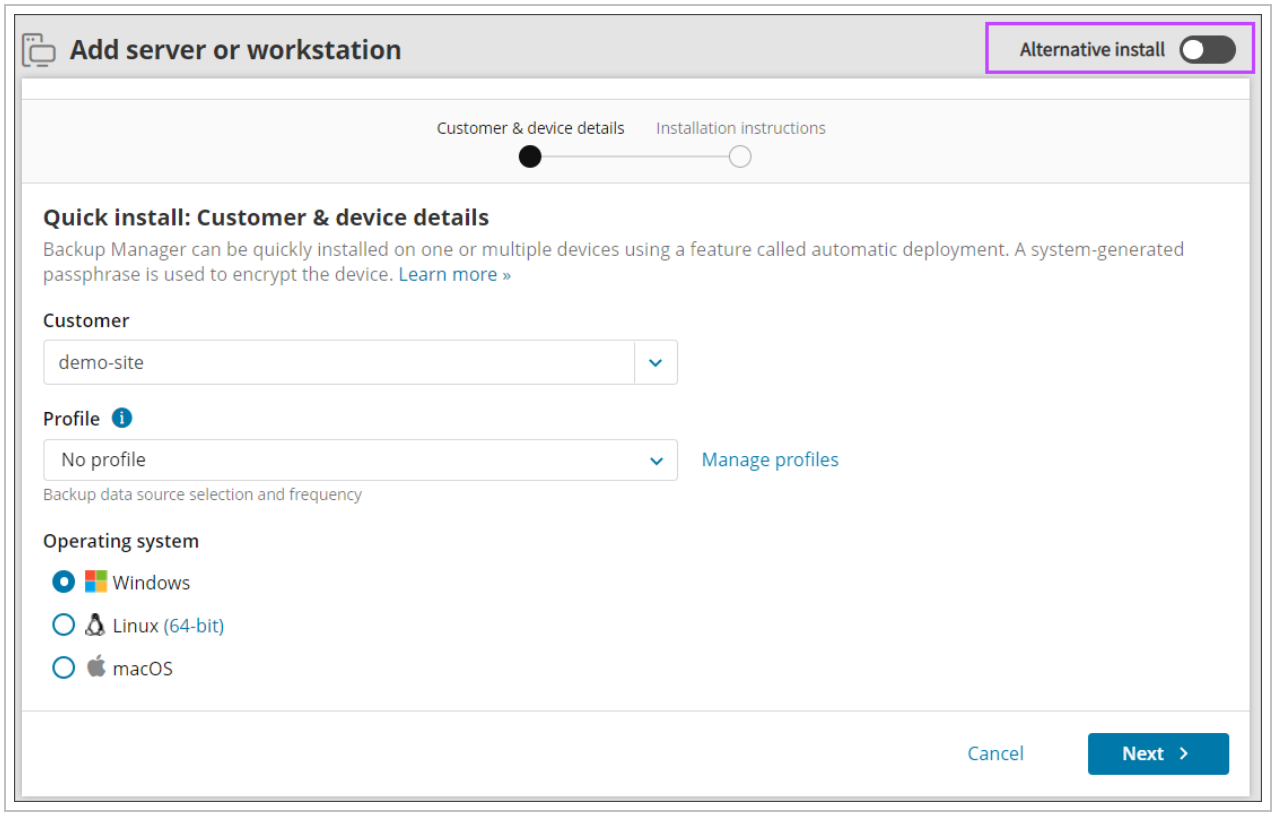
1. Log in to the Console under a SuperUser account belonging to a reseller or end-customer



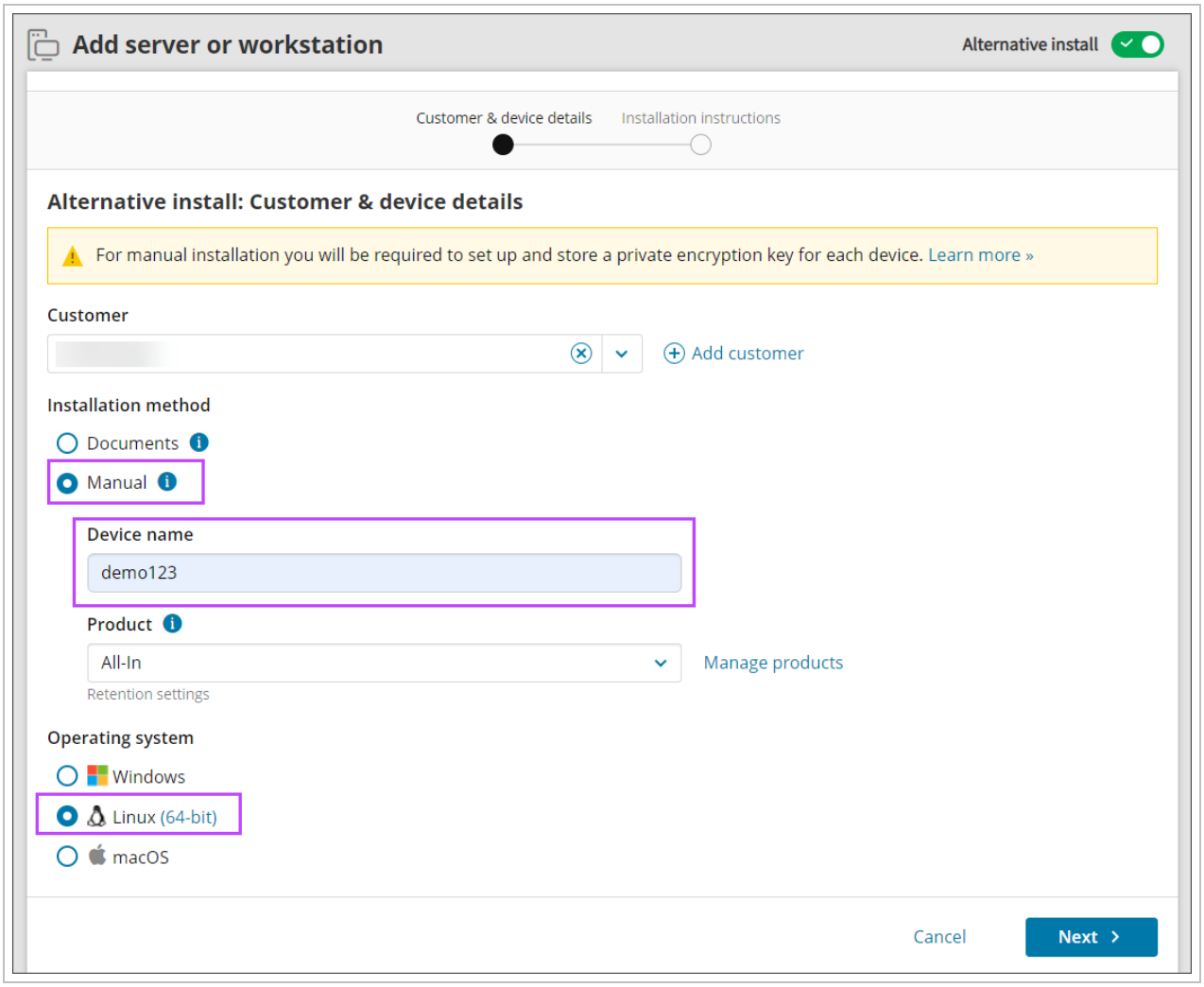
2. Click **Add devices**, select **Servers of Workstations**



3. Using the toggle in the upper right-hand corner of the wizard, enable **Alternative install**

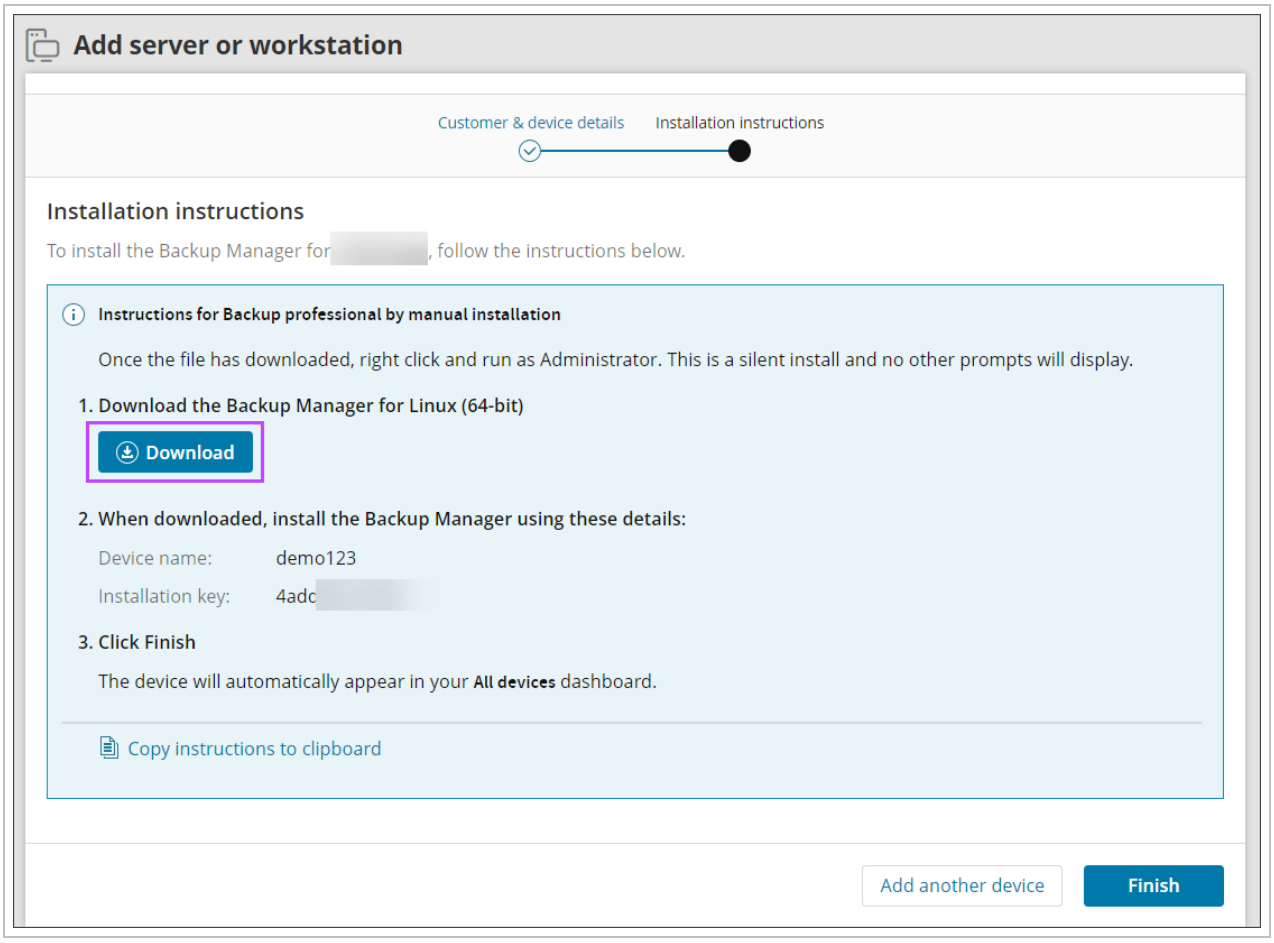


4. Select the **Customer** to install the device for from the dropdown
5. Choose the **Manual** Installation method



6. Give the device a memorable name
7. Select a product for the device (if applicable). The product determines the set of features and storage options allocated to the device (learn more).
8. Select Linux as the operating system
9. Click **next**

10. Download the Backup Manager installer



> You will need the **Device name** and **Installation key** for installation, so it is recommended you take a copy here, though these can be found at a later date from the device properties Settings tab if this is closed before taking a note.

11. Click **Finish** to close the window

Step 2: Run installation commands

1. Log in to the device as a root user:

```
% sudo -i
```

2. Take a copy of the installer file downloaded in step 1: 10 above onto the device

   Or

   Download the RUN installer suitable for your distribution from the Management Console's Downloads page:

```
# wget https://cdn.cloudbackup.management/maxdownloads/mxb-linux-i686.run
```

3. Grant the installer execute permissions:

```
# chmod +x mxb-linux-i686.run
```

4. If required, you may change the predefined installation folder:

```
# ln -s /usr/local/MXB /opt/MXB
```

> By default, the Backup Manager is installed to `/opt/MXB`. If you wish to install the software to the `/usr` mount (for example because it has more free space), you should create symlinks for it. For example:

5. Start the installer and submit your installation parameters.

> Additional parameters can be found in the Installation parameters on GNU/Linux page

> Do not forget to enclose values containing spaces or punctuation inside quotation marks.

```
# ./mxb-linux-i686.run -- --user="ubuntu-admin" --password="dg224hs-0091" --
encryption-key="SECUR_ITY2014a" --use-proxy=false
```

> The `--` attribute after the command name means that the parameters after it are specific to the Backup Manager. If your query contains a combination of parameters, use `--` to separate the internal parameters of the RUN package from external ones belonging to the Backup Manager.

6. If you submit the command without the installation parameters, you will be prompted to enter them one at a time
7. Once all parameters have been entered the installer will run

Possible permission error

If the installer is extracted to your `temp` partition and that partition is mounted with the `noexec` option, it is possible to encounter a permissions error. To rectify the error, extract the installer to another directory that has execute permissions:

```
# ./mxb-linux-i686.run --target /other/tmp
```

As the `TMPDIR` is used for additional operations, directing this variable to the same location as the `--target` variable can help to avoid additional errors.

Bourne-based shells

For use with bash, ksh, zsh, etc. use the command:

```
# export TMPDIR=/path/to/target
```

C shells

For use with csh, tsch, etc. use the command:

```
# setenv TMPDIR /path/to/target
```

Alternative installation on GNU/Linux

> We strongly **do not** recommend downgrading Backup Manager to a lower version after installation is complete. In cases where the Backup Manager has been downgraded, we cannot guarantee the application will function correctly.

Some system administrators prefer using alternative installers instead of the recommended RUN installer. There are two alternative installers to chose from, the file format you need depends on your Linux distribution:

- DEB Instructions - This method is available for modern **Debian** and **Ubuntu** distributions
- RPM Instructions - This method is available for modern **CentOS**, **RHEL** and **SUSE** distributions

Both of the installers come in 32- and 64-bit versions.

> Backup on devices using Operating Systems which are not officially supported may still work, but as we no longer test these versions, we cannot guarantee full functionality. In situations where the device cannot be upgraded to a supported OS, you may encounter issues with new features, or there may be abnormalities so please test the backup by doing a restore as soon as possible.

Precursor check:

Before beginning, check the bitness of your system first by running the following command in the command line of the device:

```
# uname -m
```

The response will be one of the following:

- `amd64` for **DEB** - if you have a 64-bit DEB system you will require the **amd64** installer
- `x86_64` for **RPM** - if you have a 64-bit RPM system you require the **x86_64** installer
- `i386` - if you have an older 32-bit system you require the **i386** installer

Installation steps

DEB Instructions

> These steps detail running commands for a 64-bit system. If your device is a 32-bit system, replace `amd64` everywhere below with `i386`

1. Download the 32- or 64-bit installer from the Management Console's Downloads page

   ```
   % wget https://cdn.cloudbackup.management/maxdownloads/mxb_~linux-1_amd64.deb
   ```

2. Run the installer you have downloaded

```
# dpkg -i mxb_~linux-1_amd64.deb
```

3. Run `configure-fp.sh` and submit parameters for the current installation. Additional parameters can be found in the Installation parameters on GNU/Linux page

   > Do not forget to enclose values containing spaces or punctuation inside quotation marks.

```
# /opt/MXB/sbin/configure-fp.sh --user="admin-ubuntu-3a" --
password=f701a2ca3255 --encryption-key="SECUR_ITY2014a" --use-proxy=false
```

4. If you submit without entering the parameters, you will be prompted to enter them one at a time at the next step
5. Once all parameters have been entered the installer will run

RPM Instructions

> These steps detail running commands for a 64-bit system. If your device is a 32-bit system, replace `x86_64` everywhere below with `i386`

1. Install the "libaio" library if you don't have it on your machine

```
# yum -y install libaio
```

2. Download the 32- or 64-bit installer from the Management Console's Downloads page

```
% wget https://cdn.cloudbackup.management/maxdownloads/mxb_linux-1.x86_64.rpm
```

3. Run the installer you have downloaded

```
# rpm -ihv mxb-linux-1.x86_64.rpm
```

4. Run `configure-fp.sh` and submit parameters for the current installation. Additional parameters can be found in the Installation parameters on GNU/Linux page

   > Do not forget to enclose values containing spaces or punctuation inside quotation marks.

```
# /opt/MXB/sbin/configure-fp.sh --user="admin-ubuntu-3a" --
password=f701a2ca3255 --encryption-key="SECUR_ITY2014a" --use-proxy=false
```

5. If you submit without entering the parameters, you will be prompted to enter them one at a time at the next step
6. Once all parameters have been entered the installer will run

Restore-only installation steps

If you want to install the device in restore-only mode, installation is done through an interactive installation process.

1. Log in to the system as a root:

```
% sudo -i
```

2. Download the RUN installer suitable for your distribution from the Management Console's Downloads page:
   - For **DEB**

```
% wget https://cdn.cloudbackup.management/maxdownloads/mxb_~linux-1_
amd64.deb
```

   - For **RPM**

```
# wget https://cdn.cloudbackup.management/maxdownloads/mxb_linux-1.x86_
64.rpm
```

3. Grant the installer execute permissions:
   - For **DEB**

```
# chmod +x mxb_~linux-1_amd64.deb
```

   - For **RPM**

```
# chmod +x mxb_linux-1.x86_64.rpm
```

4. If required, you may change the predefined installation folder:

> By default, the Backup Manager is installed to `/opt/MXB`. If you wish to install the software to the `/usr` mount (for example because it has more free space), you should create symlinks for it. For example:

```
# ln -s /usr/local/MXB /opt/MXB
```

5. Start the installer *without* additional installation parameters:
   - For **DEB**

```
# mxb_~linux-1_amd64.deb
```

   - For **RPM**

```
# mxb_linux-1.x86_64.rpm
```

6. You will be asked to provide parameters for the installation including device name, installation key (previously known as password) and security code/encryption key/passphrase

> The device name and installation key can both be found in the Settings tab of the device in the Management Console.

7. If a previous installation is detected for the device details given, you will receive a message stating:

```
This contract is already in use
You can either use this contract, abort configuration or install application
in restore only mode [u/a/R]:
```

- **u**: use contract for normal backup install
- **a**: abort the configuration
- **R**: install device using restore-only mode

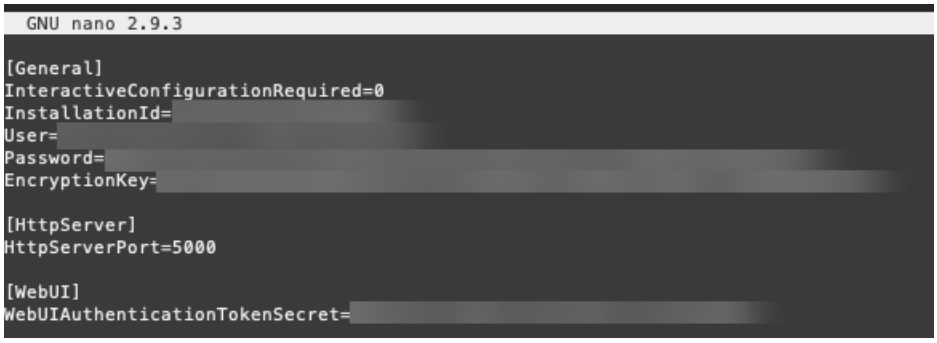
8. Select **R** here for **Restore-Only mode** installation
9. Allow the installation to complete, this will display **-- Done** once finished

Convert to restore-only mode

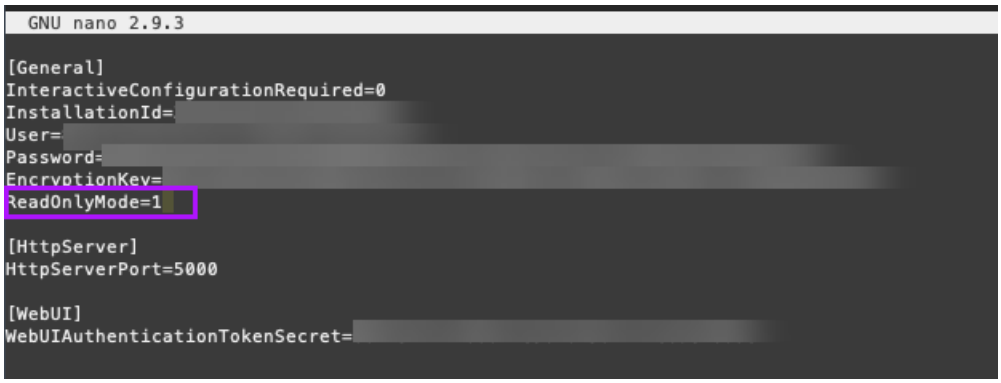
If you have installed Backup Manager on the device using the normal Installation steps steps above and wish to convert this normal version of backup to use restore-only mode, you can do this by following the below steps:

1. Open the the config.ini file. The following example command with Nano installed will open the config.ini file for editing:

```
sudo nano -w /opt/MXB/etc/config.ini
```



2. Under the **[General]** section check for an instance of `RestoreOnlyMode=0`
3. If this exists change `=0` to `=1`

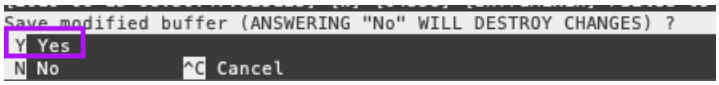


4. If this does not exist, add it as above to the **[General]** section

> This is case sensitive so please ensure it is added correctly and *without* spaces.

5. Close the file by using **Ctrl+X**
6. Save the changes to the file

```
Y
```



7. Restart the service

```
$  sudo service ProcessController restart
```

OR

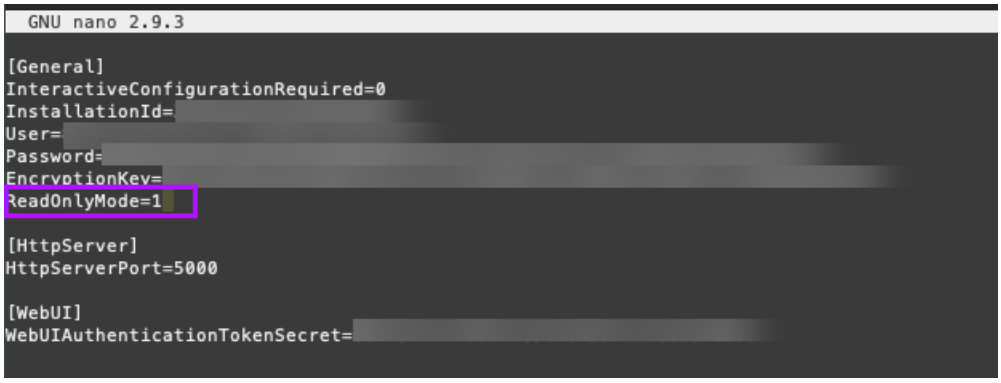
```
$  sudo /etc/init.d/ProcessController restart
```

Convert from restore-only mode to normal mode

If you have a device which has had Backup Manager installed in restore-only mode and you wish to convert this to a normal version of backup, this can be done by following these steps:

1. Open the the config.ini file. The following example command with Nano installed will open the config.ini file for editing:

```
sudo nano -w /opt/MXB/etc/config.ini
```



2. Under the **[General]** section check for an instance of `RestoreOnlyMode=1`
3. If this exists change `=1` to `=0` or remove the line entirely

```
  GNU nano 2.9.3

[General]
InteractiveConfigurationRequired=0
InstallationId=
User=
Password=
EncryptionKey=

[HttpServer]
HttpServerPort=5000

[WebUI]
WebUIAuthenticationTokenSecret=
```

4. Close the file by using **Ctrl+X**
5. Save the changes to the file

```
Y
```

```
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
Y Yes
N No          ^C Cancel
```

6. Restart the service

```
$  sudo service ProcessController restart
```

OR

```
$  sudo /etc/init.d/ProcessController restart
```

Installation parameters on GNU/Linux

When installing the Backup Manager on GNU/Linux devices, the command used to install and is made up of the initial command to run `configure-fp.sh`, and several required and optional parameters to set credentials and access.

> For the full instructions, please see Alternative installation on GNU/Linux

Please find below the parameters to use during the Backup Manager installation on GNU/Linux systems.

Required parameters

If you do not supply these parameters in the command used to run the installer, you will be prompted to supply these one at a time until all are complete before the installation will run:

Parameter	Definition
`--user`	The name of your backup device (issued by your service provider)
`--password`	Your installation key for the backup device (issued by your service provider)
`--encryption-method`	This setting lets you customize the data encryption method. From the 17.5 release onwards, **AES-256** has become the common encryption method for all installations.

Parameter	Definition
(legacy)	All previous installations retain their original encryption method selections.
`--encryption-key`	Set an Encryption Key/Security Code that will be used to encrypt your data. It can be any word or sentence of your choice. Using this, you can encrypt your files with a strong encryption algorithm, thus keeping your private data protected from unauthorized access. ❌ You must keep a note of the Encryption Key/Security Code yourself as this is **NOT** stored anywhere within our system and will be required to carry out several key tasks, such as recovering data, moving an backup to a different device, etc.
`--use-proxy`	This setting prompts the Backup Manager to connect to the Internet through a proxy server. Supported values: ▪ `1` - use a proxy connection ▪ `0` - do not use a proxy connection (Default)

Optional parameters

These parameters are optional extras which can be used within the command to provide additional configuration to your system:

Parameter	Definition
`--proxy-type`	The type of the proxy server: `HTTP`, `SOCKS4`, or `SOCKS5`
`--proxy-address`	The host name or IP address of the proxy server
`--proxy-port`	The port you access the proxy server through
`--use-proxy-authorization`	Defines if the proxy server requires authorization by username: `true` or `false`.
`--proxy-username`	Your username for proxy access
`--proxy-password`	Your password for proxy access
`-h, --help`	Gives access to help resources. This is an internal parameter of the RUN package (does not require `--` after the command name). Sample usage: `./bm-linux-i686.run -h` or `./bm-linux-i686.run --help`

Installation Verification on GNU/Linux

Once the Backup Manager has been installed to the `/opt/MXB` directory and started, this runs the `/etc/init.d/ProcessController` start-up script.

The script starts the `/opt/MXB/bin/ProcessController` binary. ProcessController then checks and restarts the Backup Functional Process (BackupFP) binary if necessary.

You can specify UID and GID for the BackupFP in the `/opt/MXB/etc/ProcessController.config` file. It is root by default:

```
<param key="user" type="int">0</param>
<param key="group" type="int">0</param>
```

Verify BackupFP

To verify that the BackupFP is initialized and bound to the right ports. The first port is 5314. The second port is one of the following, depending on your service provider:

- 5000
- 5001
- 4000

Run the following command to check the ports:

```
# netstat -nlp|grep BackupFP
```

A response will look like this:

```
tcp      0      0 0.0.0.0:5314          0.0.0.0:*       LISTEN      6586/BackupFP
tcp      0      0 0.0.0.0:5000          0.0.0.0:*       LISTEN      6586/BackupFP
```

The first part of the response displays a remote communication port for **legacy devices** powered by the desktop-based edition of the Backup Manager. The second part - for devices with a web interface.

If you get no response, it means that the BackupFP has not been initialized. In such a case it will be necessary to look into your log files to investigate the issue.

The ports can be changed if your network requires it. You can do it by changing 2 parameters in the Backup Manager configuration file:

- In the `[General]` section, add `CommunicationPort=7777`
- In the `[HttpServer]` section, find the `HttpServerPort` parameter and edit is value to the required port number e.g. `HttpServerPort=8001`

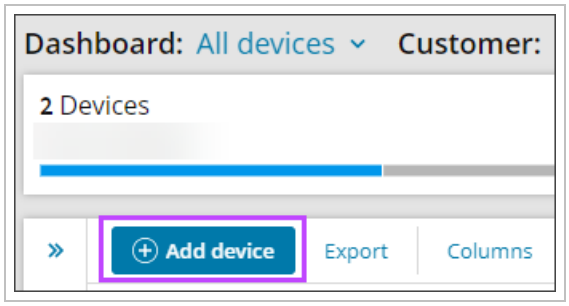
Manual installation on Windows and macOS

> We strongly **do not** recommend downgrading Backup Manager to a lower version after installation is complete. In cases where the Backup Manager has been downgraded, we cannot guarantee the application will function correctly.

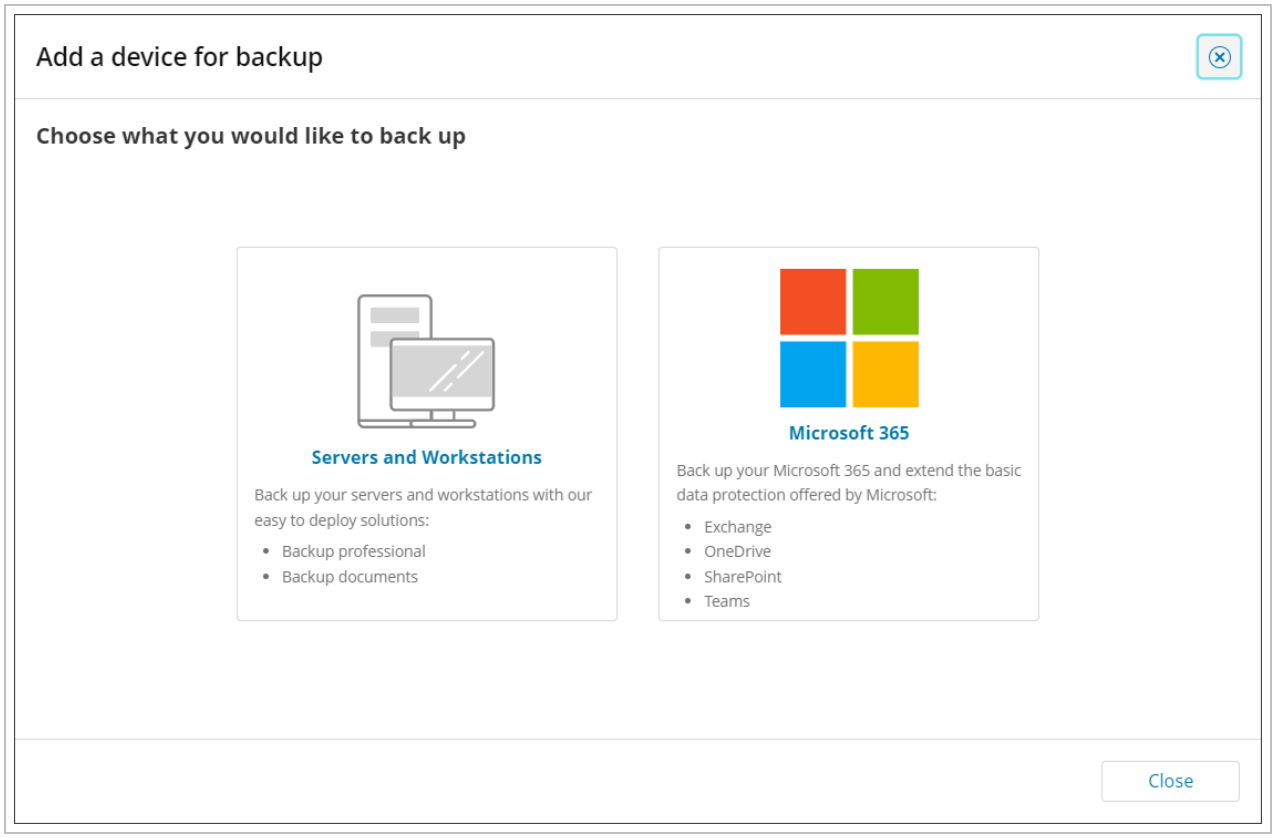
To start using the Backup Manager, using the Manual Installation method (also known as Legacy Install) for your operating system, this wizard guides your through several quick steps.

Step 1: Add device

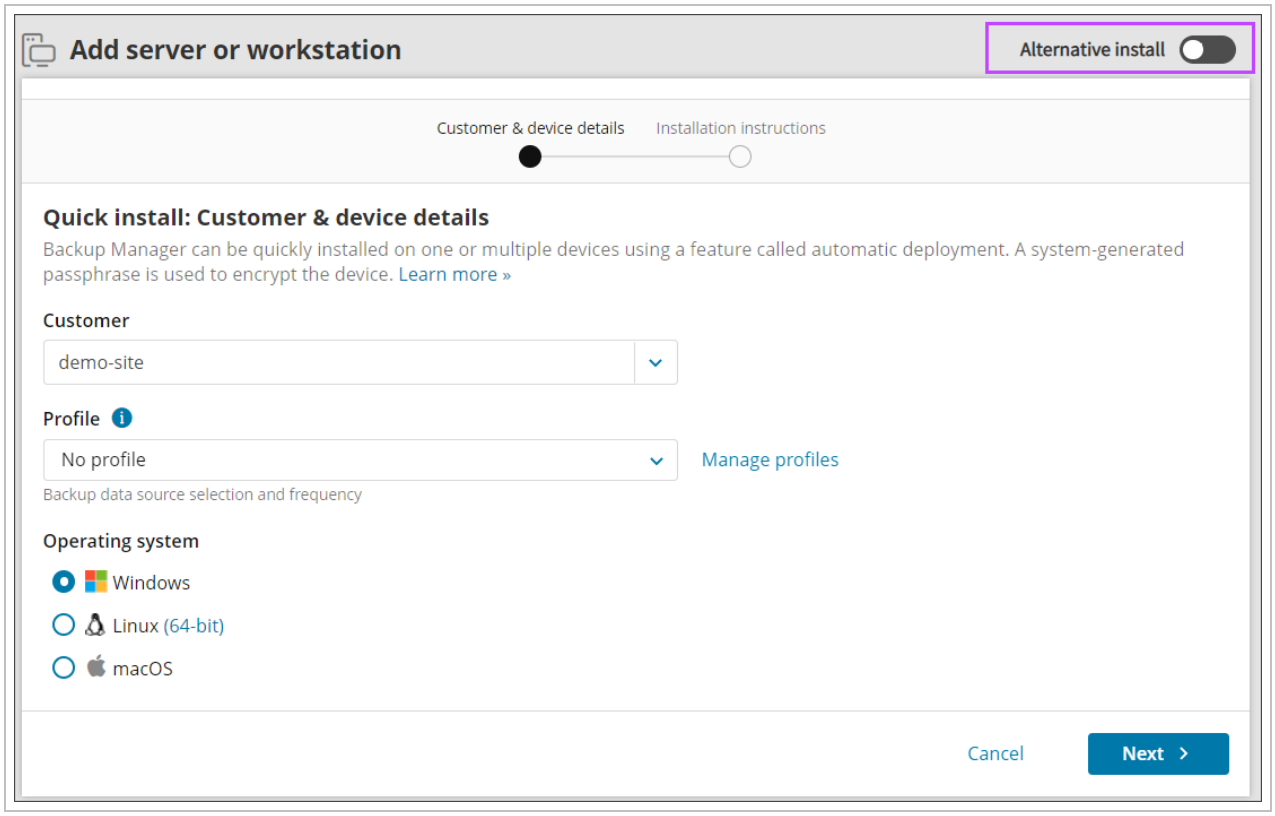
1. Log in to the Console under a SuperUser account belonging to a reseller or end-customer



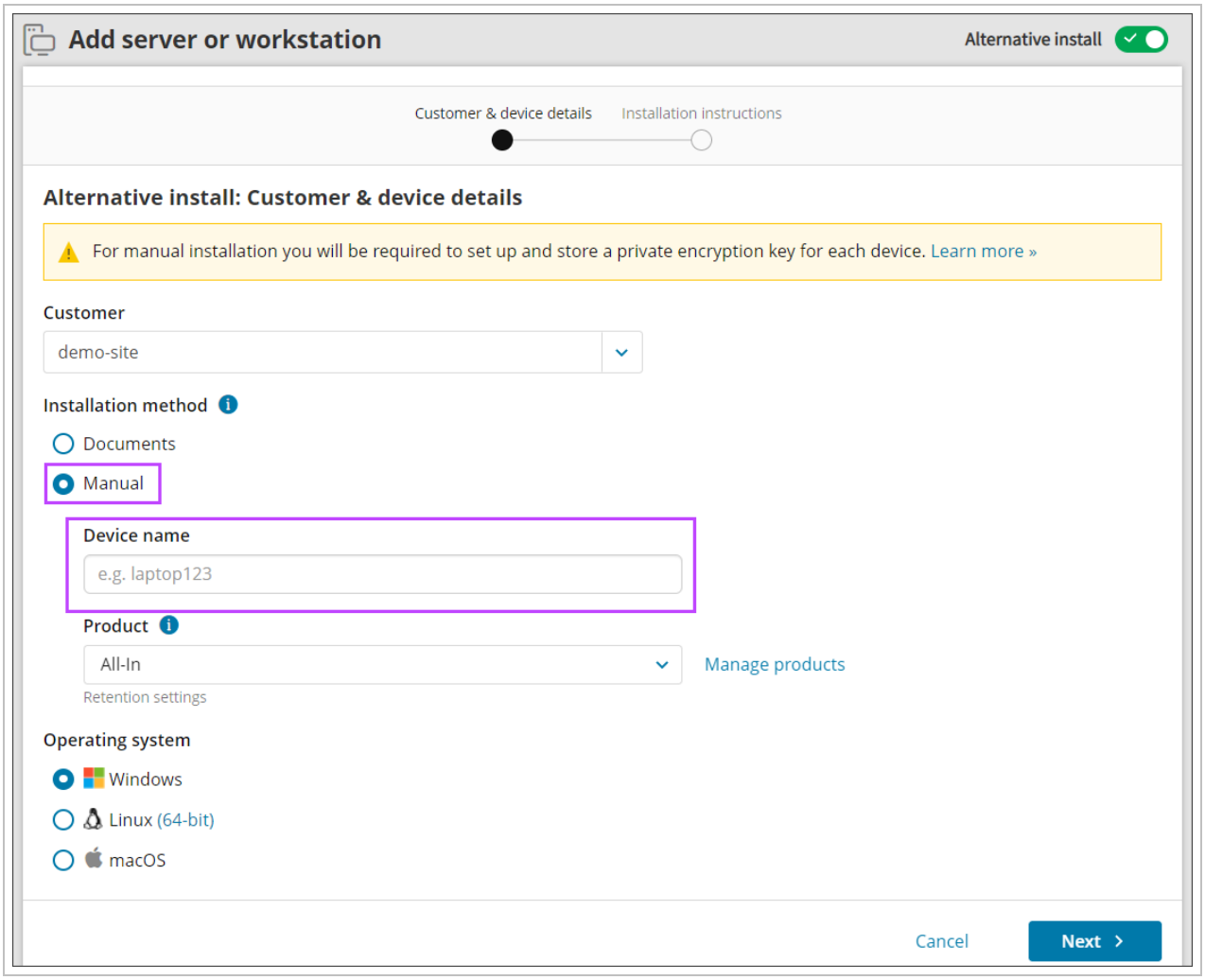
2. Click **Add devices**, select **Servers of Workstations**



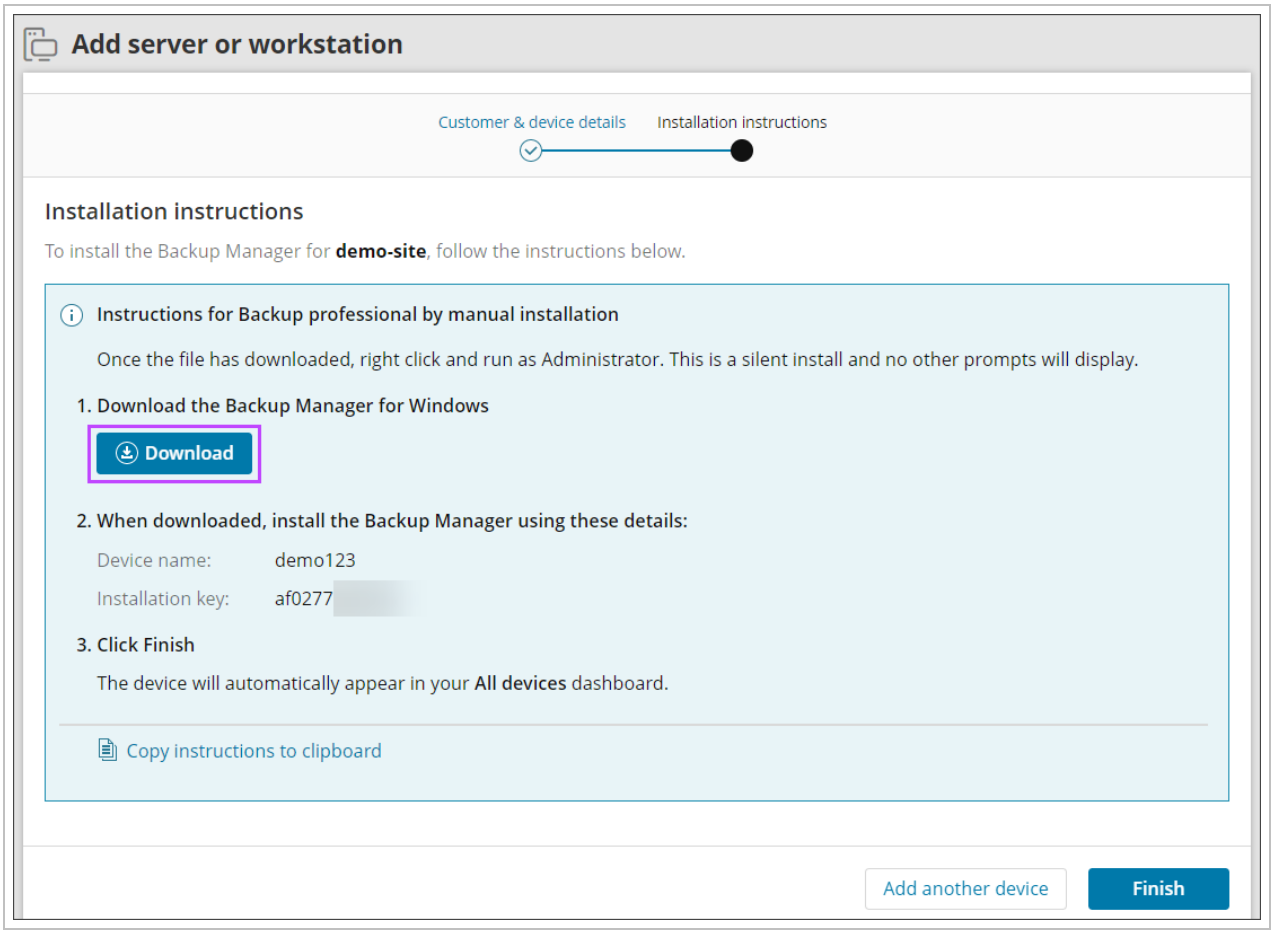
3. Using the toggle in the upper right-hand corner of the wizard, enable **Alternative install**



4. Select the **Customer** to install the device for from the dropdown
5. Choose the **Manual** Installation method



6. Give the device a memorable name
7. Select a product for the device (if applicable). The product determines the set of features and storage options allocated to the device (learn more).
8. Select the operating system
9. Click **next**
10. Download the Backup Manager installer



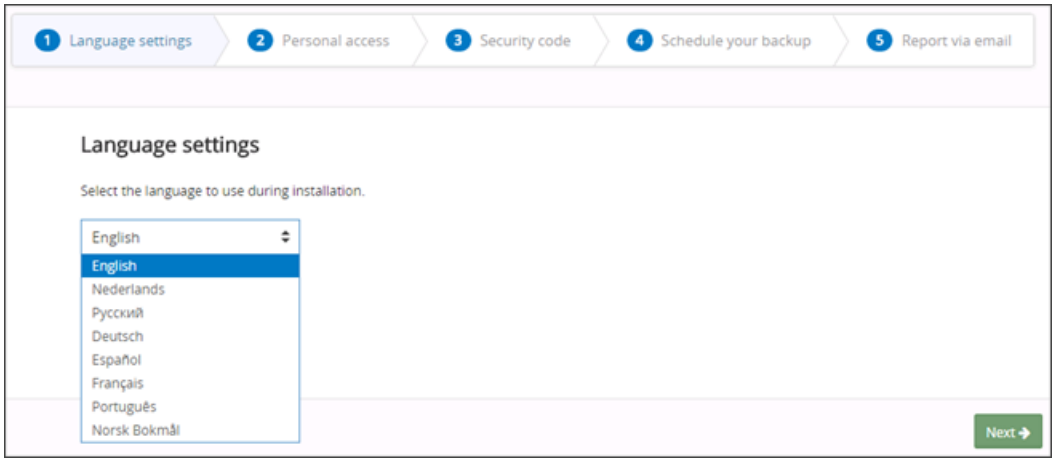
You will need the **Device name** and **Installation key** for installation, so it is recommended you take a copy here, though these can be found at a later date from the device properties Settings tab if this is closed before taking a note.

11. Run the installer and follow the instructions provided on screen

If the installer does not run after downloading and attempting to run, check the properties of the install file to ensure that it has not been blocked by your system upon download or attempt to run as the Administrator on the device.

Step 2: Language settings

The Backup Manager is available in many languages. Choose the language for the current installation.



Step 3: Personal access

Enter your access details for the Backup Manager. Your **device name** and **installation key** is required.

If you need access details, please contact your system administrator or service provider.

Step 4: Security code (Encryption key or Passphrase)

Set a **security code (Encryption key or Passphrase)** that will be used to encrypt your data.

It can be any word or sentence of your choice, but should be secure and not easily guessed. Using this secret code, you can encrypt your files with a strong encryption algorithm, thus keeping your private data protected from unauthorized access.

The most important challenge is finding the best code, the one that you can remember but that no one else knows or can guess. There is an encryption limit of 100 characters for the security code/encryption key.

> If you use the Security code/Encryption key method, you **MUST** remember this. We **do not** store this code anywhere for you, so please ensure you keep it safe, stored somewhere other than on this device. It will not be possible to restore your backed up data or re-install the current backup device without it.

Step 5: Schedule your backup (optional)

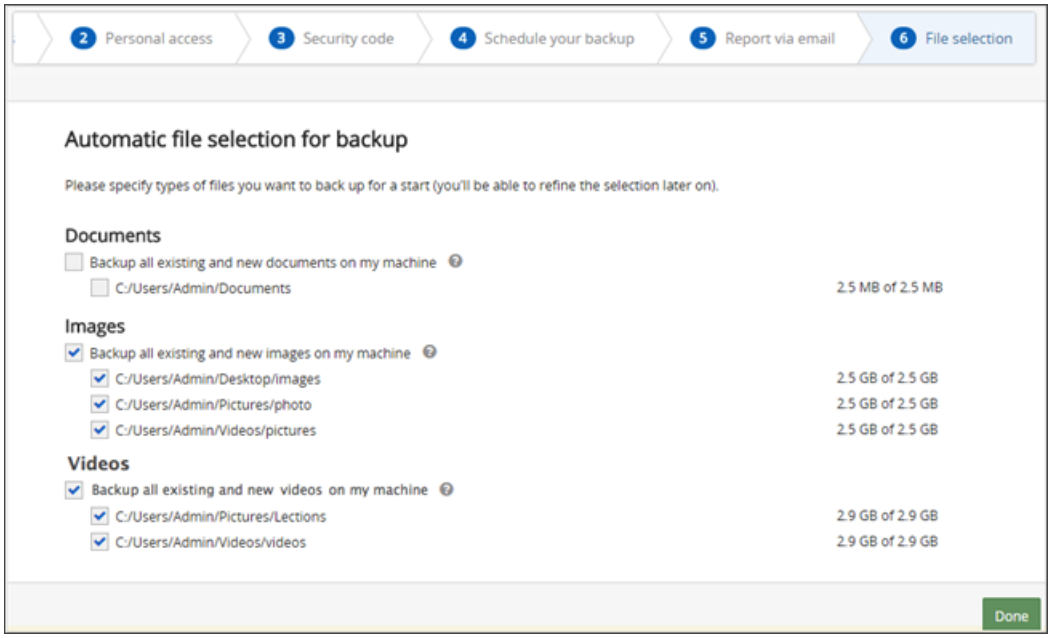
You can specify at what time to start regular backups and choose appropriate frequency.

Step 6: Report via email (optional)

Enter your email address to start receiving email reports on the statuses of recent backup activities. The frequency of report delivery is customizable.

Step 7: Automatic selection for backup (Windows workstations only)

You can quickly populate your backup selection with **documents, images and videos** detected on your computer.



You can change your initial choice of the file groups after the installation as well as refine your backup selection.

> Ensure you enable Full Disk Access for the Backup Manager *before* running backups on macOS 10.14 Mojave or later.

macOS Full Disk Access

With the release of macOS 10.14 Mojave, Apple introduced new privacy controls to prevent third-party applications from interacting with your private data without authorization.

> These privacy controls are present on **all macOS devices from 10.14 Mojave newer**. See Supported operating systems for a list of supported macOS operating systems.

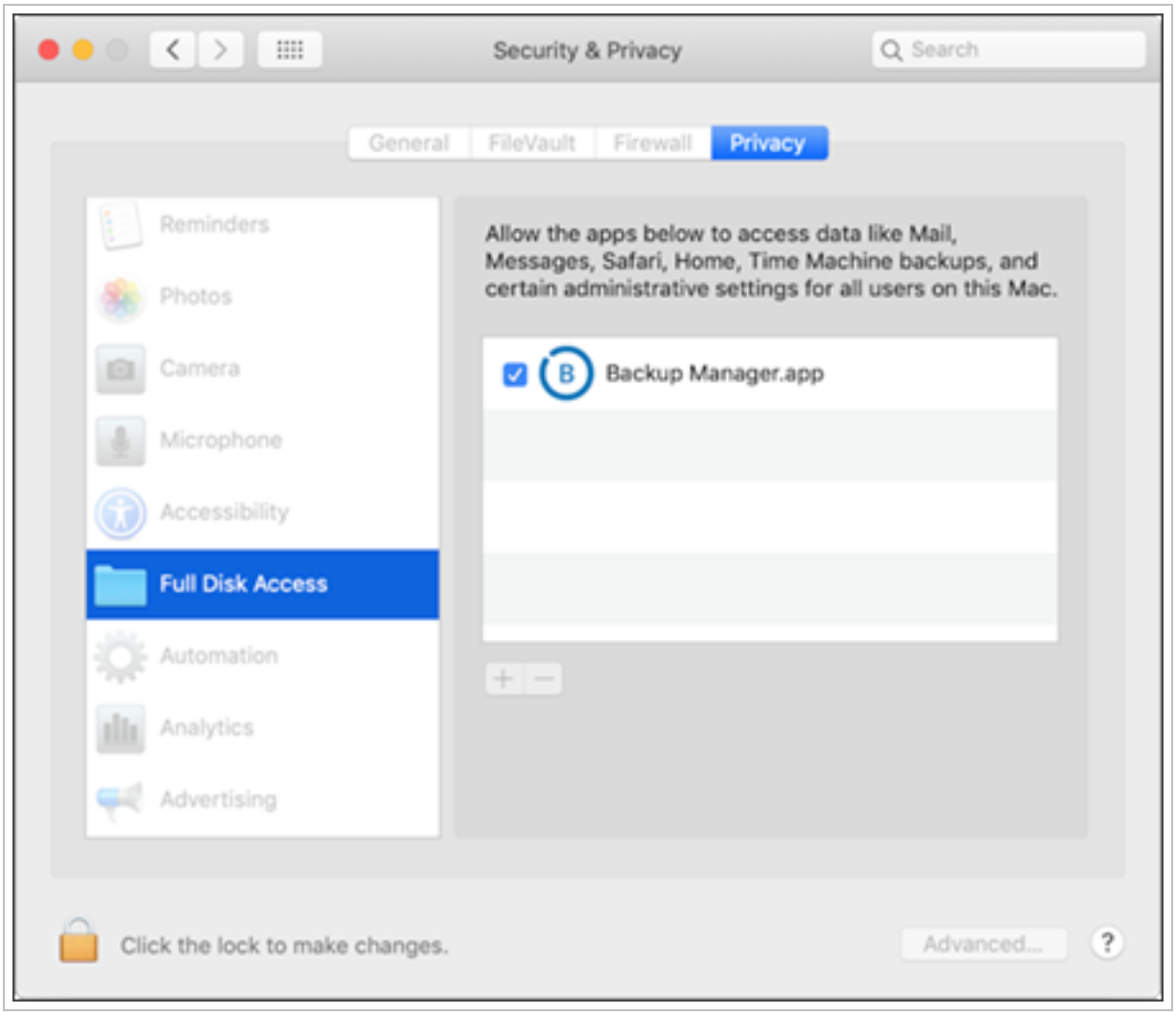
The privacy controls' default setting is block, and where an application requires access to protected private data (for example Backup Manager when backing up the computer) it must first be granted Full Disk Access.

Data classed as protected by Apple includes Mail, Messages, Safari, Home and Time Machine backups.

To enable Full Disk Access for Backup Manager:

1. Go to **System Preferences** and choose **Security & Privacy**
2. Select **Privacy** then **Full Disk Access**
3. Click on the padlock in the bottom left corner to unlock and allow changes
4. Enter the computer's administrative account credentials when prompted
5. Click the plus icon below the main window to add an application
6. Use **Finder** to navigate to the **Applications** folder and select **Backup Manager**
7. Click **Open**
8. Ensure the **Backup Manager** box is ticked in the main window

9. Close the **Security & Privacy** window



Silent installation of Backup Manager

> We strongly **do not** recommend downgrading Backup Manager to a lower version after installation is complete. In cases where the Backup Manager has been downgraded, we cannot guarantee the application will function correctly.

Silent Installation is a way to install Backup Manager on devices through the command line on Windows.

Quick Installation vs. Silent installation vs. Manual installation

Three installation methods available are:

1. **Quick Installation** - The Automatic Deployment feature lets you install Backup Manager on multiple devices simultaneously

2. **Silent Installation** - lets you install one device at a time using the command line on Windows
3. **Manual Installation** - lets you install one device at a time manually

Please see the table below for the differences between these options.

	Quick Installation	Silent installation	Manual Installation
Supported versions	All Windows, macOS and Linux on which Backup Manager works (full list)	All Windows, macOS and Linux on which Backup Manager works (full list)	All Windows, macOS and Linux on which Backup Manager works (full list)
Feature availability	Only resellers and end-customers	All types of customers	Only resellers and end-customers
Number of installations	Multiple devices simultaneously	One device at a time	One device at a time
Details required for installation	Installation command (generated automatically)	1. Device name 2. Device password/installation key 3. security code/encryption key	1. Device name 2. Device password/installation key 3. security code/encryption key

We **do not** store the Security Code/Encryption Key of a device, this must be kept by yourself as it **cannot** be retrieved in our system if lost.

Instructions

To perform the silent installation of the Backup Manager:

1. Download the Backup Manager for Windows from the Management Console's Downloads page
2. Run the command line on the device as an administrator
3. Run the installer using cmd and submit the appropriate parameters for the installation. For example:

```
mxb-windows-x86_x64.exe -user "support_win_jab67v" -password "ab0982b2bxgt" -
encryption-key "SECUR_ITY2016!"
```

Technically, you can submit the name of the installer file alone (`mxb-windows-x86-x64.exe` in the above example). In that case you will be offered to provide the remaining parameters when you start the Backup Manager software for the first time.

The installer file name may differ to the above example. The name used must be that of the file downloaded in step #1.

Installation parameters

All text values must be submitted in **straight double quotes**.

Recommended parameters

Parameter	Description	Supported values
`-user`	A device name for authentication (generated automatically when you add a device in the Console)	Text
`-password`	The installation key associated with the device name (generated automatically when you add a device in the Console)	Text
`-encryption-key`	Enter a security code/encryption key that will be used to encrypt your data. Please store the key in a secure location as it will not be possible to re-install the Backup Manager and recover your data without this key. If you are **re-installaing** an existing device that was installed by means of the automatic deployment, use the `-passphrase` parameter instead.	Text (6-100 symbols)
`-passphrase`	The passphrase generated through the Console (used instead of the security code/encryption key for **re-installing** existing devices installed by means of the Quick Installation)	Text

Proxy settings (optional)

Parameter	Description	Supported values
`-use-proxy`	This setting prompts the Backup Manager to connect to the Internet through a proxy server.	▪ `1` (use a proxy connection) ▪ `0` (do not use a proxy connection) - default
`-proxy-type`	The type of the proxy server	▪ `HTTP` ▪ `SOCKS4` ▪ `SOCKS5`
`-proxy-address`	The host name or IP address of the proxy server	IP address or host name, for example `192.188.33.55` or `some.server.com`
`-proxy-port`	The port number of the proxy server	Number (0 by default)
`-use-proxy-authorization`	Prompts the Backup Manager that the proxy requires authorization by username.	▪ `1` - the proxy requires authorization ▪ `0` - the proxy does not require authorization (default)
`-proxy-user-name`	A username for access to the proxy server	Text, for example `domain\username` or `username`
`-proxy-pass-word`	A password for access to the proxy server	Text

Misc. optional parameters

Parameter	Description	Supported values
`-encryption-method` (legacy)	Supported by the Backup Manager **17.4** and earlier versions. This setting lets you customize the data encryption method. Starting from the 17.5 release, **AES-256** has become the common encryption method for all installations. All previous installations retain their original encryption method selections.	▪ `AES-256` (default) ▪ `AES-128` ▪ `Blowfish-448`
`-restore-only`	This flag lets you install a backup device in the restore-only mode (for example, because it is already installed on another computer).	N/A (enter the parameter as is)
`-silent`	This flag prevents the installer from displaying warning and error messages. It also prevents the Backup Manager from starting automatically after the installation.	N/A (enter the parameter as is)
`-no-shortcuts`	This flag prevents the installer from creating a Backup Manager shortcut in the Windows Start menu. If the shortcut is missing, the only way to start the Backup Manager is by typing in its URL into a web browser or by launching a remote connection to the device from the Backup & Recovery Console.	N/A (enter the parameter as is).

Silent installation of Backup Manager - macOS

> We strongly **do not** recommend downgrading Backup Manager to a lower version after installation is complete. In cases where the Backup Manager has been downgraded, we cannot guarantee the application will function correctly.

Silent installation is a way to install backup devices through the Terminal on macOS devices.

For macOS devices, the silent installation option only installs the software, there is no way to pass the extra installation parameters to the installation package via the Terminal, so must be done manually.

Instructions

Here is how to perform the silent installation of the Backup Manager:

1. Run your terminal emulator as an administrator
2. Download the Backup Manager for macOS from the Management Console's Downloads page
3. Run the installer and submit appropriate parameters for the installation. Here is an example command:

```
sudo installer -pkg mxb-17.7.0.17249=macos-x86_64.pkg -target
```

It would be possible to create a script that references a configuration file (config.ini) with the device name, installation key and encryption key/security code to update the `config.ini` file after a successful installation and then have it restart the Backup Service Controller. This would reload the system with the new configuration updates, however a pre-existing script is not available so you would have to write this manually.

The config.ini file can be found in this location:

```
/Library/Application Support/MXB/Backup Manager/config.ini
```

Variables

You can update the following variables with the correct information:

- User=**X**
- EncryptionKey=**X**
- installation key=**X**

Once you have updated the config.ini file, you will need to restart the internal backup process for all changes to take effect.

Update Backup Manager

Methods of updating the Backup Manager differ depending on the operating system of the device in question. It is important to carry out the precursor checks for your OS before manually updating the Backup Manager version.

Precursor checks:

- **Windows** & **macOS** - Run a version check to confirm the version of Backup Manager used
- **Linux**:
  1. Confirm the bitness of your system
  2. Run a version check to confirm the version of Backup Manager used

Update to the newest version:

- Windows & macOS Via Installation File
- Linux:
  - Update the RUN package
  - Update and migrate the DEB package
  - Update and migrate the RPM package

> All devices using the latest version of Backup Manager will automatically update when newer versions are released.

Precursor checks

> Before updating the Backup Manager manually, there are checks that must be carried out.

Windows Version Check

Check which version of Backup Manager the device is using by viewing the Device Details.

If the device is using an older version of Backup Manager than **version 16.11**, you must first install version 16.11 before proceeding with updating to the latest version:

- **Windows** - version 16.11
- **macOS** - version 16.11

Linux Bitness Check

Before beginning, check the bitness of your system first by running the following command in the command line of the device:

```
# uname -m
```

The response will be one of two:

- `x86_64` - you have a **64-bit** system
- `i686` - you have a **32-bit** system

Linux Version Check

Check which version of Backup Manager the device is using by viewing the Device Details.

If the device is using an older version of Backup Manager than **version 16.11**, you must first install version 16.11 before proceeding with updating to the latest version:

- **RUN**:
  - i386 (32-bit) version 16.11
  - amd64 (64-bit) version 16.11
- **RPM**:
  - i386 (32-bit) version 16.11
  - amd64 (64-bit) version 16.11
- **DEB**:
  - i386 (32-bit) version 16.11
  - amd64 (64-bit) version 16.11

Instructions

Windows & macOS Via Installation File

1. Download the latest version of the Backup Manager from the Downloads page
2. Run the installation file on the device you wish to update

   > This will overwrite the existing installation, but preserve selections and preferences.

Linux

Update the RUN package

1. Log in to the device as a root user:

```
sudo -i
```

2. Download the latest RUN package from the Downloads page **Or** by using the following command:
   a. 64-bit

```
wget -O ./mxb-linux-x86_64.run
https://cdn.cloudbackup.management/maxdownloads/mxb-linux-x86_64.run
```

   b. 32-bit

```
wget -O ./mxb-linux-i686.run
https://cdn.cloudbackup.management/maxdownloads/mxb-linux-i686.run
```

3. Install the package:
   a. 64-bit

```
chmod +x ./mxb-linux-x86_64.run
./mxb-linux-x86_64.run
```

   b. 32-bit

```
chmod +x ./mxb-linux-i686.run
./mxb-linux-i686.run
```

Update and migrate the DEB package

1. Log in to the device as a root user:

```
sudo -i
```

2. Make a reserve copy of Backup Agent configuration:

```
cp -f /opt/MXB/etc/config.ini ~/config.ini.save
```

3. Uninstall the current Backup Agent DEB package:

```
apt-get -y remove mxb
```

4. Restore Backup Agent configuration by copying the `config.ini` file saved in step #2 to the `/opt/MXB/etc` folder:

```
mkdir -p /opt/MXB/etc
cp -f ~/config.ini.save /opt/MXB/etc/config.ini
```

5. Download the latest RUN package from the Downloads page **Or** by using the following command:
   - 64-bit

     ```
     wget -O ./mxb-linux-x86_64.run
     https://cdn.cloudbackup.management/maxdownloads/mxb-linux-x86_64.run
     ```

   - 32-bit

     ```
     wget -O ./mxb-linux-i686.run
     https://cdn.cloudbackup.management/maxdownloads/mxb-linux-i686.run
     ```

6. Install the package:
   - 64-bit

     ```
     chmod +x ./mxb-linux-x86_64.run
     ./mxb-linux-x86_64.run
     ```

   - 32-bit

     ```
     chmod +x ./mxb-linux-i686.run
     ./mxb-linux-i686.run
     ```

Update and migrate the RPM package

1. Log in to the device as a root user:

```
sudo -i
```

2. Make a reserve copy of Backup Agent configuration:

```
cp -f /opt/MXB/etc/config.ini ~/config.ini.save
```

3. Uninstall the current Backup Agent RPM package:

```
rpm -e mxb
```

4. Restore Backup Agent configuration by copying the `config.ini` file saved in step #2 to the `/opt/MXB/etc` folder:

```
mkdir -p /opt/MXB/etc
cp -f ~/config.ini.save /opt/MXB/etc/config.ini
```

5. Download the latest RUN package from the Downloads page **Or** by using the following command:
   - 64-bit

   ```
   wget -O ./mxb-linux-x86_64.run
   https://cdn.cloudbackup.management/maxdownloads/mxb-linux-x86_64.run
   ```

   - 32-bit

   ```
   wget -O ./mxb-linux-i686.run
   https://cdn.cloudbackup.management/maxdownloads/mxb-linux-i686.run
   ```

6. Install the package:
   - 64-bit

   ```
   chmod +x ./mxb-linux-x86_64.run
   ./mxb-linux-x86_64.run
   ```

   - 32-bit

   ```
   chmod +x ./mxb-linux-i686.run
   ./mxb-linux-i686.run
   ```

Re-installation

If you have a Backup Manager device configured and need to re-install the backup software but wish to keep the old configuration settings such as the device name, installation key, security code/encryption key and the previously stored backup data, this can be done on **Windows**, **Linux** or **macOS** devices by:

1. Navigate to the configuration file, the Config.ini location will differ depending on the operating system
2. Take a copy of the `config.ini` file and paste it to the desktop
3. Uninstall the Backup Manager
4. Download the newest version of the Backup Manager that is compatible with your device from the Downloads page of the Management Console or Cove Data Protection downloads page on the N-able website
5. Double click the file to run the installer

6. Once installed and the installation page will open in the browser, from here you can either:
   a. Enter the credentials for the original device i.e. device name, installation key, security code/encryption key and complete the wizard via the browser

      Or

   b. Stop the processes and service
   c. Delete the new `config.ini` file which has been created at the Config.ini location
   d. Copy the original file from the desktop
   e. Paste it into this location
   f. Start the processes and service
7. Refresh the browser page to ensure the Backup Manager loads or close the page and run the Backup Manager app from your device

   > It may take some time for the Backup Manager to download all data relating to the device from the cloud

Replaced end-user device

When installing the Backup Manager on a new device, the current history will transfer over as long as the old credentials are used (as found on the **Settings** tab for the original device in the Management Console).

1. Run the downloaded installer from the Downloads page on the new device
2. Enter the credentials from the original account i.e. device name, installation key, security code/encryption key
3. Select **Yes** when asked if this is the correct device
4. Complete installation through the browser

Reinstall old device for recovery only

In the case where you have an old (inactive) backup device which has not been deleted from the Management Console, it is possible to install Backup Manager on a device using these details to recover existing data.

Install on a device where Backup Manager is currently installed

> If you cannot remember your security code/encryption key for the old device, we cannot help you as this is not stored anywhere within the system

1. Stop the internal backup process
2. Navigate to the configuration file, the Config.ini location will differ depending on the operating system
3. Rename the `config.ini` file to something like "Devicename_config.ini"

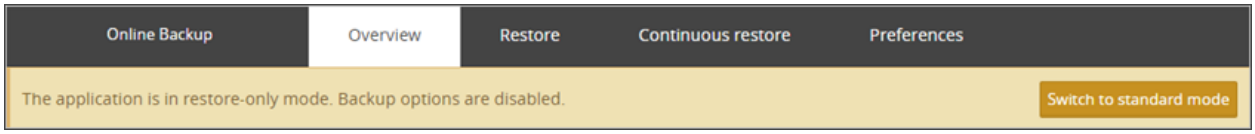
   > This allows you to keep track of which configuration file relates to which device name and allows you to revert the file names back easily

4. Launch the Backup Manager for the device
5. Configure the backup using the old (inactive) backup devices details

6. When configuring the device, you will be prompted on how you want to configure the Backup Manager, select **Restore-Only** mode
   - If this does not pop up, manually put the device into Restore-Only mode:
     a. Stop the internal backup process
     b. Open the `config.ini` file in notepad as administrator
     c. Under the `[General]` section, add `ReadOnlyMode=1`
     d. **Save** the file

     > This is case sensitive so please type carefully or copy from here and paste

     e. Start the internal backup process
7. Confirm the device is in Restore-Only mode when a banner will be displayed to advise as such



> Do **not** click **Switch to standard mode** as this will take the device out of Restore-Only mode and may (depending on configuration) cause a backup to run on the new device

8. Once configured, you can now run the restore
9. When your recovery is complete:
   a. Stop the internal backup process
   b. Navigate to the configuration file, the Config.ini location
   c. Rename the `config.ini` file to "Devicename_config.ini" for the recovered device details
   d. Rename the original configuration file back to `config.ini`
   e. Start the Backup Service Controller again

Install on a device where Backup Manager is not installed

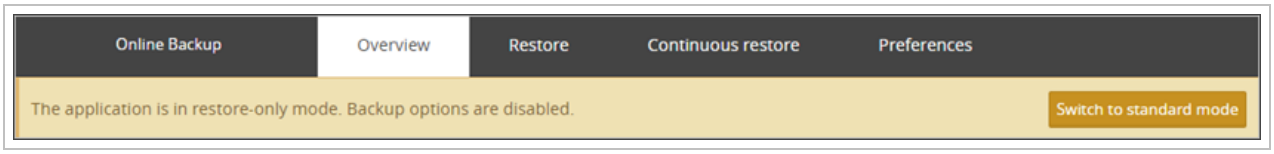
> If you cannot remember your security code/encryption key, unfortunately we cannot help you as this is not stored anywhere within the system

1. Download and install the Backup Manager from the downloads page of the Management Console or Cove Data Protection downloads page on the N-able website
2. Once installed and the installation page appears in the browser, configure the backup using the old (inactive) backup devices details i.e. device name, installation key, security code/encryption key

3. When configuring the device, you will be prompted on how you want to configure the Backup Manager, select **Restore-Only** mode
   - If this does not pop up, manually put the device into Restore-Only mode:
     a. Stop the internal backup process
     b. Open the `config.ini` file in notepad as administrator
     c. Under the `[General]` section, add `ReadOnlyMode=1`
     d. **Save** the file

     > This is case sensitive so please type carefully or copy from here and paste

     e. Start the internal backup process
4. Confirm the device is in Restore-Only mode when a banner will be displayed to advise as such



5. Once configured, you can now run the restore. When you are done uninstall the Backup Manager or disable restore-only mode to allow the device to backup as per the schedule of the original device

Backup Manager Restore-Only Mode

The **restore-only mode** is a way to have the Backup Manager installed on a device without backing up the device's data, either temporarily or perminantly. This is done to prevent unwanted backups in cases such as:

- When your computer has failed and it is necessary to recover data from it to a new location
- When you want an up-to-date copy of all necessary data available straight away on another computer

> During the restore-only mode the **Backup** tab is absent from the Backup Manager. The options on the **Restore** tab are updated automatically after each new backup session on the source computer.

While you are in the restore-only mode, you can restore data in either of the following ways:

- On Demand - These are one-off restores, configured and triggered manually on the device
- Continuous Restore - This function enables automatic, continuous recovery of the source computer

Preconditions

Restore-Only mode is available on all the supported operating systems. It requires 2 computers:

1. A **source computer** (the one that the data has been backed up)
2. A **target computer** (where you want to recover the data to)

Enabling the restore-only mode

A device can be put into restore-only mode at one of two times:

1. Option 1: During installation
   a. On Linux devices

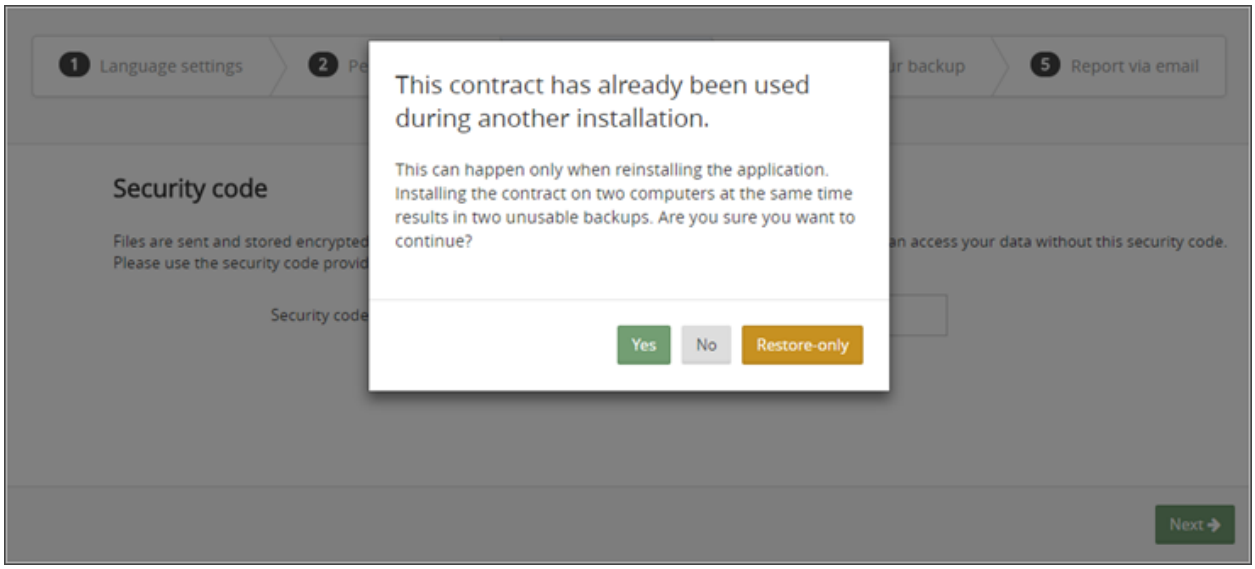
2. Option 2: After installation
    a. On Linux Devices

Option 1: During installation

1. Install the Backup Manager on the target computer using the same **device name**, **installation key** (previously known as the Password) and **security code/encryption key/passphrase** that are used on the source computer using the Manual Installation mode

    > Do **not** use the **Automatic Deployment** method of installation, as you cannot specify device credentials using this method.

2. When the Backup Manager recognizes the device credentials, you will receive a message offering to enable the restore-only mode, click **Restore-only** to complete the installation



Option 2: After installation

1. Click on **Start** and type **services.msc**
2. Locate the **Backup Service Controller** and right click to open the action menu
3. Select **Properties**
4. **Stop** the service
5. Open a text editor on the device as an **Administrator**
6. Confirm **User Access Control** to permit changes
7. Open the Backup Manager configuration file (config.ini)

8. Under the `[General]` section, enter `ReadOnlyMode=1`

```
[General]
User=XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Password=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
EncryptionKey=XXXXXXXXXXXXXXXXXXXXXXXX
ReadOnlyMode=1
```

9. Return to **services.msc**
10. Locate the **Backup Service Controller** and right click to open the action menu
11. Select **Properties**
12. **Start** the service

Disabling the restore-only mode

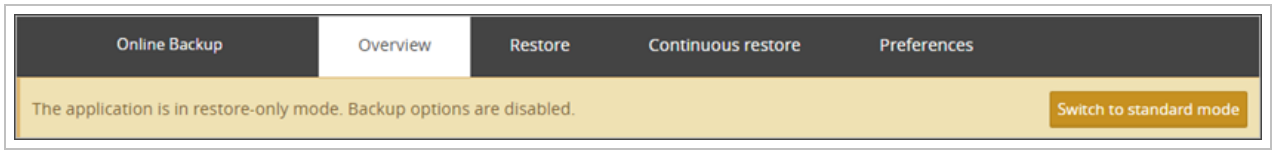
A device can be taken out of restore-only mode and placed back into standard mode in one of three ways:

1. Option 1: Using the notification ribbon
2. Option 2: Through config.ini
3. Option 3: By reinstalling the device
4. On Linux Devices

Option 1: Using the notification ribbon

As soon as Backup Manager recognizes the device is in restore-only mode, you will be given a notification banner on every page while viewing the Backup Manager.

To disable the restore-only mode, click the **Switch to standard mode** button on the notification:



Option 2: Through config.ini

1. Click on **Start** and type **services.msc**
2. Locate the **Backup Service Controller** and right click to open the action menu
3. Select **Properties**
4. **Stop** the service
5. Open a text editor on the device as an **Administrator**
6. Confirm **User Access Control** to permit changes
7. Open the Backup Manager configuration file (config.ini)

8. Under the `[General]` section, change the `ReadOnlyMode` value to `=0` or remove it

```
[General]
User=XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Password=XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
EncryptionKey=XXXXXXXXXXXXXXXXXXXXXXXX
ReadOnlyMode=0
```

9. Return to **services.msc**
10. Locate the **Backup Service Controller** and right click to open the action menu
11. Select **Properties**
12. **Start** the service

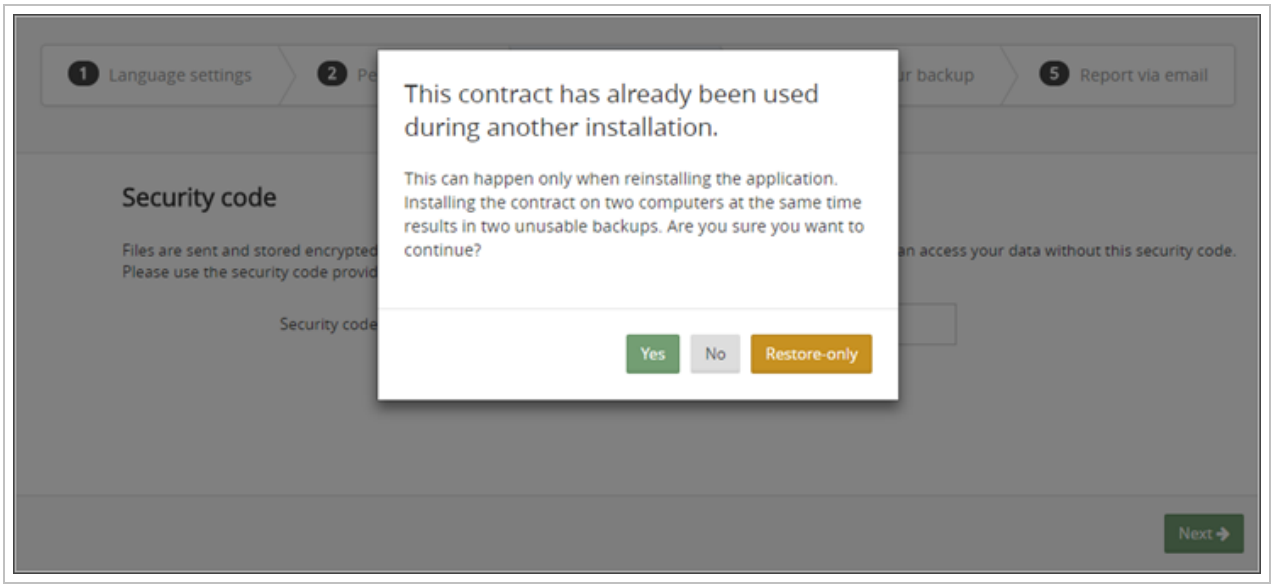
Option 3: By reinstalling the device

Re-install the Backup Manager on the device.

1. Install the Backup Manager on the target computer using the same **device name**, **installation key** (previously known as the Password) and **security code/encryption key/passphrase** that are used on the source computer using the Manual Installation mode

   > Do **not** use the **Automatic Deployment** method of installation, as you cannot specify device credentials using this method.

2. When the Backup Manager recognizes the device credentials, you will receive a message offering to enable the restore-only mode, click **Yes** to complete the installation



Backup Manager Restore-Only Mode - Linux

Restore-only installation steps

If you want to install the device in restore-only mode, installation is done through an interactive installation process.

1. Log in to the system as a root:

```
% sudo -i
```

2. Download the RUN installer suitable for your distribution from the Management Console's Downloads page:

```
# wget https://cdn.cloudbackup.management/maxdownloads/mxb-linux-i686.run
```

3. Grant the installer execute permissions:

```
# chmod +x mxb-linux-i686.run
```

4. If required, you may change the predefined installation folder:

> By default, the Backup Manager is installed to `/opt/MXB`. If you wish to install the software to the `/usr` mount (for example because it has more free space), you should create symlinks for it. For example:

```
# ln -s /usr/local/MXB /opt/MXB
```

5. Start the installer *without* additional installation parameters:

```
# ./mxb-linux-i686.run
```

6. You will be asked to provide parameters for the installation including device name, installation key (previously known as password) and security code/encryption key/passphrase

> The device name and installation key can both be found in the Settings tab of the device in the Management Console.

7. If a previous installation is detected for the device details given, you will receive a message stating:

```
This contract is already in use
You can either use this contract, abort configuration or install application
in restore only mode [u/a/R]:
```

   - **u**: use contract for normal backup install
   - **a**: abort the configuration
   - **R**: install device using restore-only mode

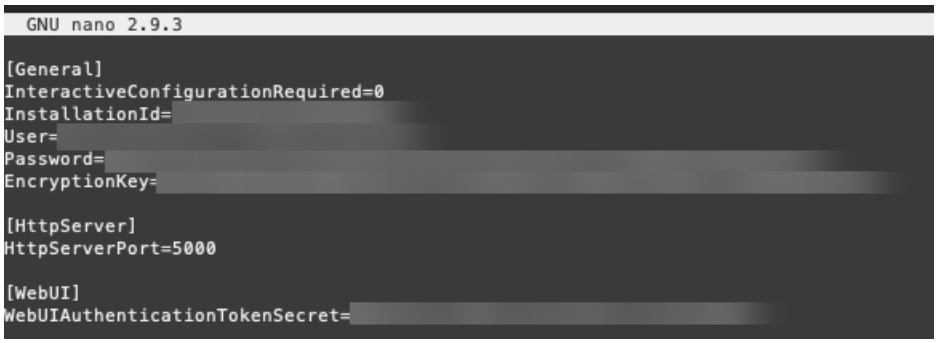
8. Select **R** here for **Restore-Only mode** installation
9. Allow the installation to complete, this will display **-- Done** once finished

Enable Restore-Only Mode

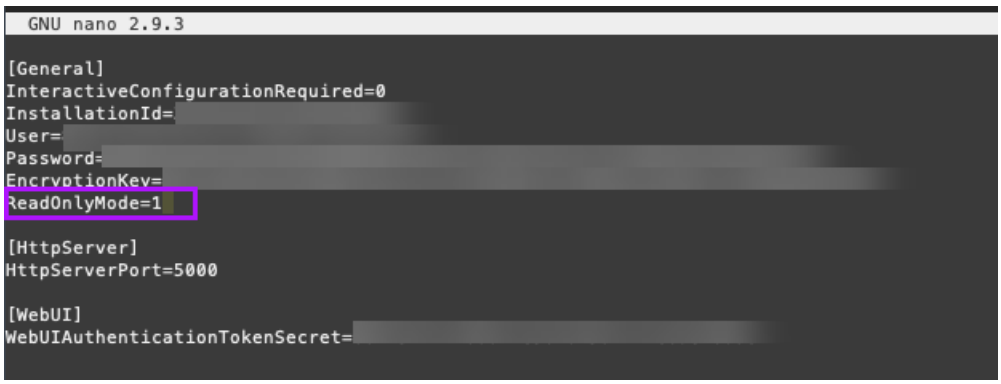
If you have installed Backup Manager on the device using the normal Backup Manager Restore-Only Mode - Linux above and wish to convert this normal version of backup to use restore-only mode, you can do this by following the below steps:

1. Open the the config.ini file. The following example command with Nano installed will open the config.ini file for editing:

```
sudo nano -w /opt/MXB/etc/config.ini
```



2. Under the **[General]** section check for an instance of `RestoreOnlyMode=0`
3. If this exists change `=0` to `=1`

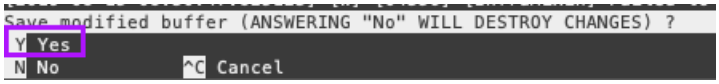


4. If this does not exist, add it as above to the **[General]** section

> This is case sensitive so please ensure it is added correctly and *without* spaces.

5. Close the file by using **Ctrl+X**
6. Save the changes to the file

```
Y
```



7. Restart the service

```
$  sudo service ProcessController restart
```

OR

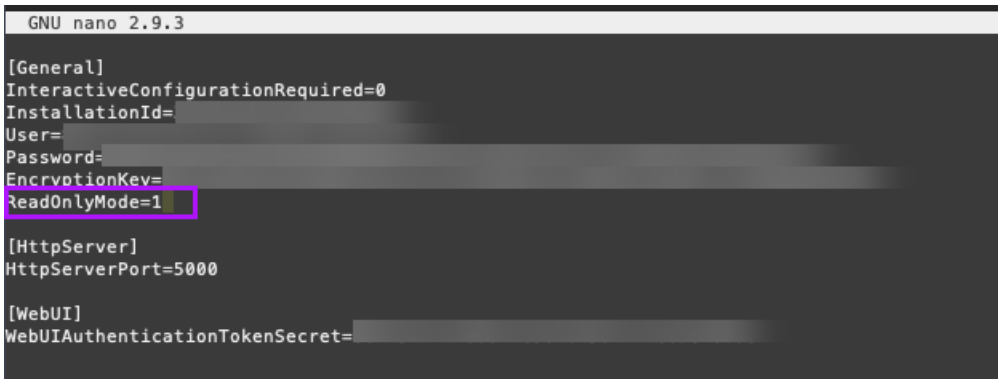
```
$  sudo /etc/init.d/ProcessController restart
```

Disable Restore-Only Mode

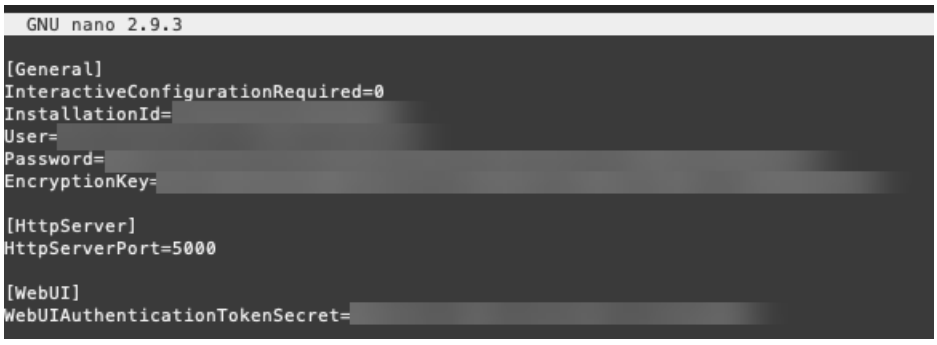
If you have a device which has had Backup Manager installed in restore-only mode and you wish to convert this to a normal version of backup, this can be done by following these steps:

1. Open the the config.ini file. The following example command with Nano installed will open the config.ini file for editing:

```
sudo nano -w /opt/MXB/etc/config.ini
```

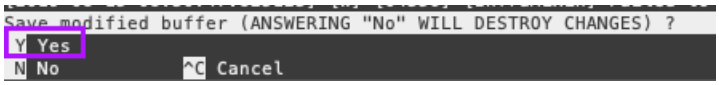


2. Under the **[General]** section check for an instance of `RestoreOnlyMode=1`
3. If this exists change `=1` to `=0` or remove the line entirely



4. Close the file by using **Ctrl+X**
5. Save the changes to the file

```
Y
```



6. Restart the service

```
$  sudo service ProcessController restart
```

OR

```
$  sudo /etc/init.d/ProcessController restart
```

Uninstalling Backup Manager

To uninstall the Backup Manager, follow instructions for your operating system:

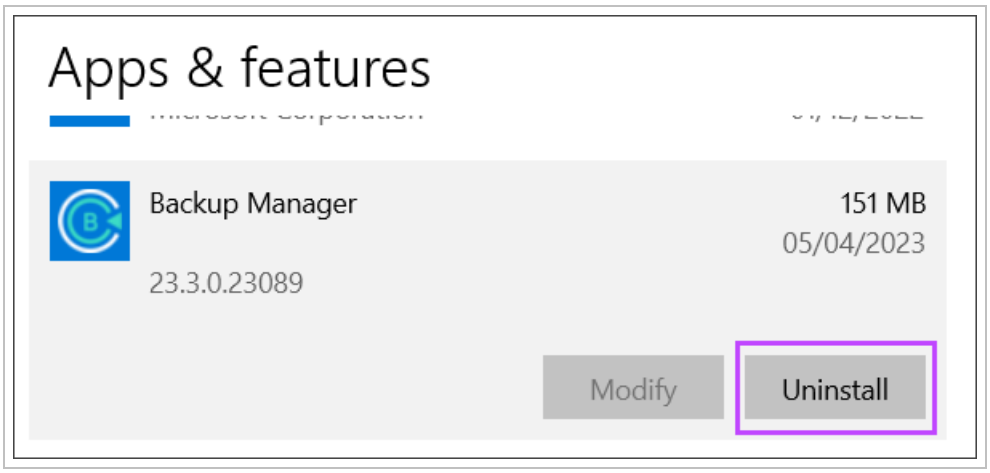
- Uninstalling Backup Manager - Windows
- Silent uninstallation of Backup Manager (Windows Only)
- Uninstalling Backup Manager - macOS
- Uninstalling Backup Manager (GNU/Linux)

Uninstalling Backup Manager - Windows

> These instructions pertain to the standalone version of Backup from Cove Data Protection (Cove) **only**, and are not relevant to any integrated version via N-Sight RMM or N-central.

You can uninstall the Backup Manager from your Windows computer through the Control Panel.

1. Open the **Start** menu and type **Add or Remove Programs**
2. In the Apps & Features window, browse to **Backup Manager**
3. Select **Uninstall**



4. Wait for the program to complete uninstallation
5. Restart your workstation

> This will uninstall the application and clear its installation folder from your computer

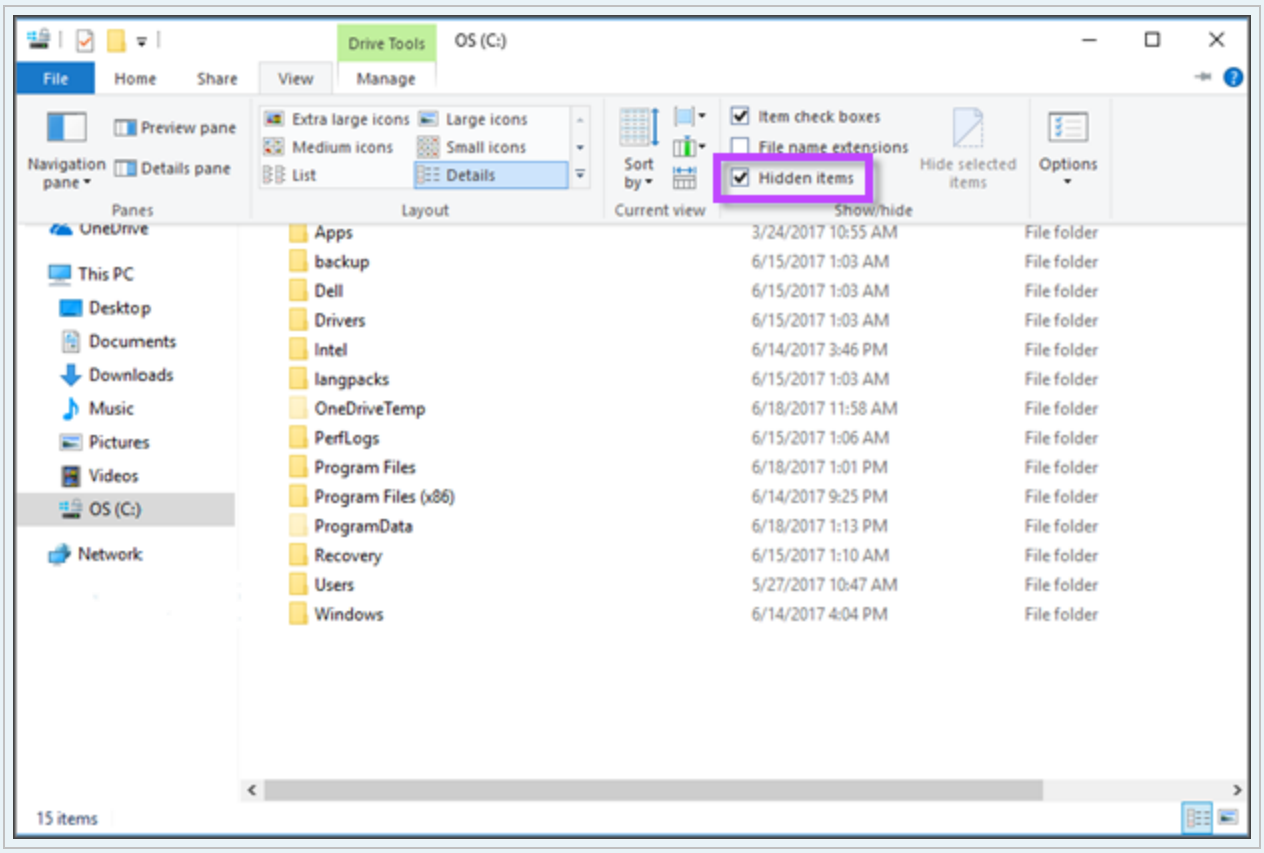
Additionally, you can **delete all related files and settings** manually:

Their location varies slightly depending on your Windows version.

- Pre Windows Server 2003: `C:\Documents and Settings\All Users\Application Data\MXB`
- Post Windows Vista: `C:\ProgramData\MXB`

> If you are **reinstalling** Backup Manager using the same storage account, we recommend renaming the **\MXB** folder instead of deleting it as data loss could occur if deleted

On **Windows 10**, the `ProgramData` folder is hidden by default. To unhide it, open File Explorer, go to the `C:\` drive and then click **View > Show hidden items**.

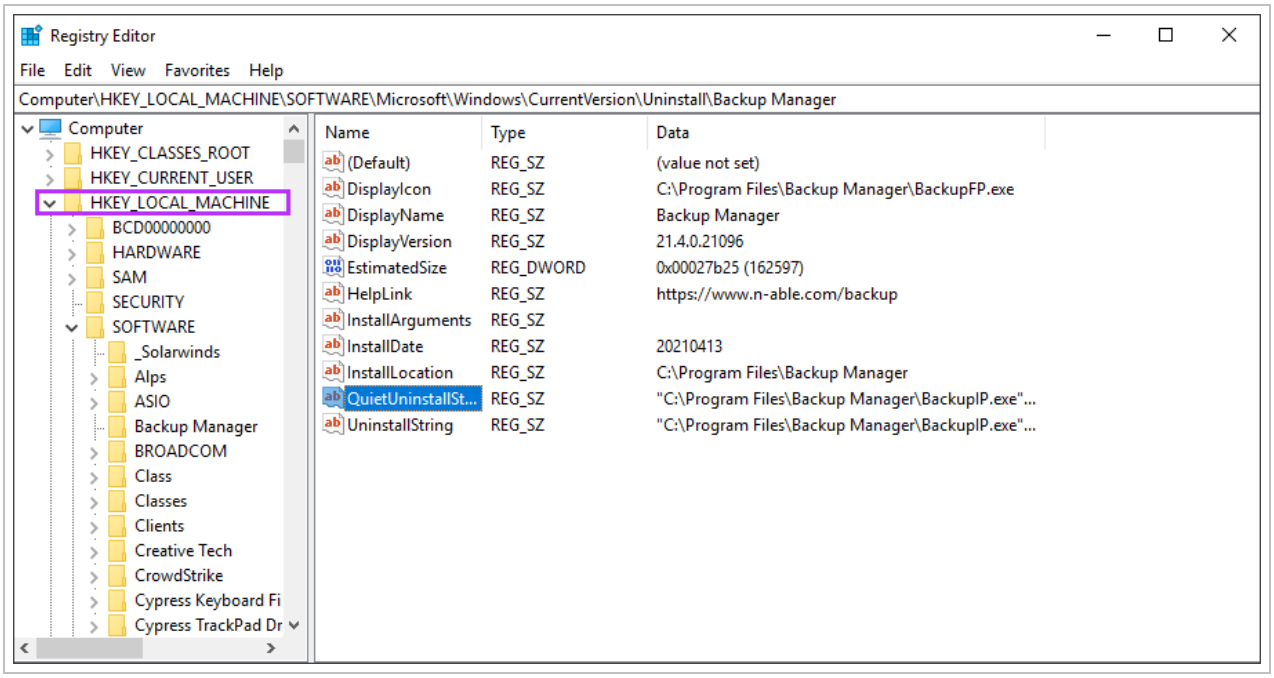


If your Backup Manager files are stored in a different location, it is likely you are not running the Cove Data Protection (Cove) standalone version of Backup Manager and are instead using one of the integrated versions of Backup from N-Sight RMM or N-central.

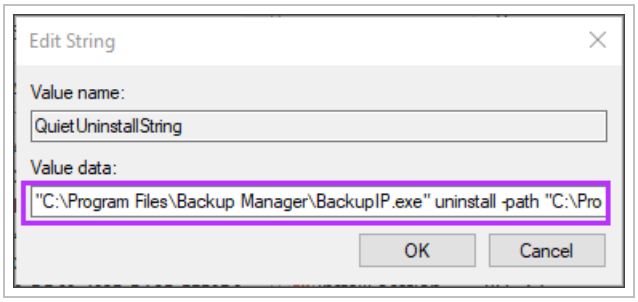
Silent uninstallation of Backup Manager (Windows Only)

You can uninstall the Backup Manager through the command line on Windows. The feature has been available starting from version **16.10** released in October 2016.

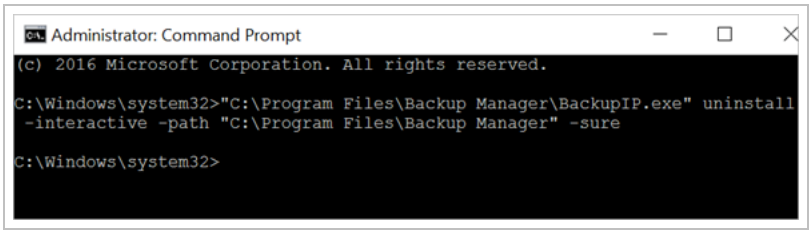
1. Open the Windows Registry Editor (**Regedit**). You can quickly locate the app by typing in its name to the Windows Start menu
2. Go to `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\Backup Manager`



3. Double-click `QuietUninstallString`
4. Copy the value



5. Start the Command Prompt as an administrator and submit the command you have copied



6. Restart the device

To confirm that Backup Manager has uninstalled check the following locations:

- File explorer navigate to:

```
C:\Program Files\
```

The folder named **Backup Manager** that used to belong in here will have been deleted.

- Services.msc, check that **Backup Service Controller** has been deleted

Uninstalling Backup Manager - macOS

On macOS, the Backup Manager is uninstalled using a hidden helper application. Here are steps to follow:

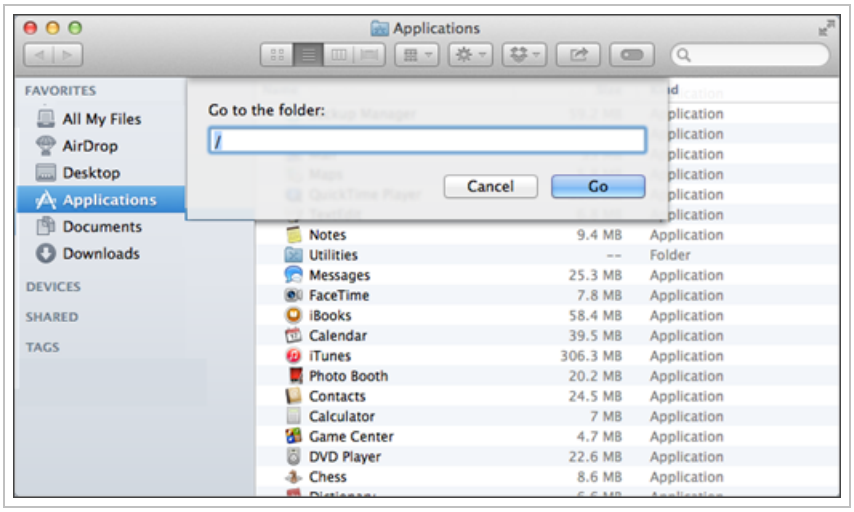
1. Open the Finder
2. From the Sidebar, choose **Applications**
3. Right-click (or control-click) the Backup Manager icon
4. Choose **Show package contents**

5. Click **Contents > Resources**
6. Double-click the **Uninstall** file
7. Confirm your intention to uninstall the Backup Manager.

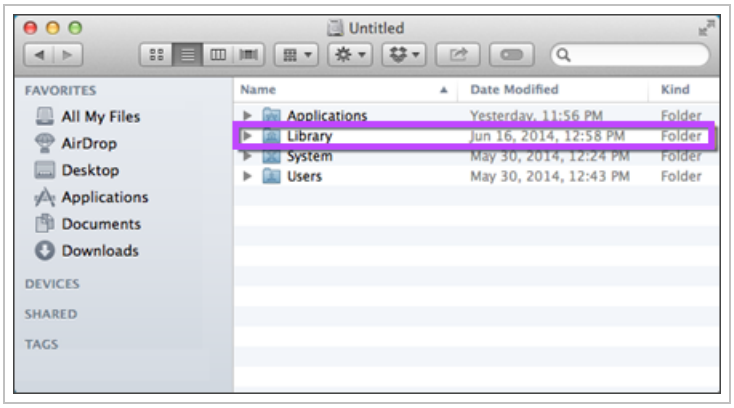
If you want to **clear all remaining files** associated with the Backup Manager (settings, local cache and the like), you can find them in the Library folder: `/Library/Application Support/MXB/Backup Manager`.

You can access the Library folder through the root folder of your Mac.

1. Open the Finder
2. From the macOS menu bar, choose **Go > Go to folder** or use the **Command+Shift+G** keyboard shortcut
3. Enter a slash to the address field
4. Click **Go**



5. Find the Library folder inside



Uninstalling Backup Manager (GNU/Linux)

The way to uninstall the Backup Manager on Linux is determined by the **file format of the installer** you used. There are three of them altogether:

- **RUN** - this is the recommended format (suits all Linux distributions and requires minimum settings)
- **DEB** - for Debian and Ubuntu
- **RPM** - for CentOS, RHEL, and SUSE

Step 1. Uninstall Backup Manager

To uninstall the Backup Manager from your Linux machine, run the command suitable for your installation package.

1. Log in to the device as a root user:

```
% sudo -i
```

2. Run the ininstall command:
   - **RUN**: `# /opt/MXB/sbin/uninstall-fp.sh`
   - **DEB**: `# apt-get -y remove --purge mxb`
   - **RPM**: `# rpm -e mxb`

Step 2 (optional). Remove related files

You can clear all files created by the Backup Manager using the following command (suits all the Linux distributions):

1. Confirm you are still logged in as the root user:

```
% sudo -i
```

2. Run the remove command:

```
# rm -rf /opt/MXB
```

Launch the Backup Manager

After the installation, the Backup Manager opens as a **web application**. A command-line interface is also available.

In-Agent Authentication

In order to enhance access security in update 22.2, opening the Backup Manager client on the device is now done via in-agent authentication.

> This means that you can no longer browse directly to http://localhost:5000 (or alternate port number if this was changed) on the devices web browser.

The following message will be displayed when trying:

For the following older Windows operating systems, this new feature required you to install Microsoft fix #3024777:

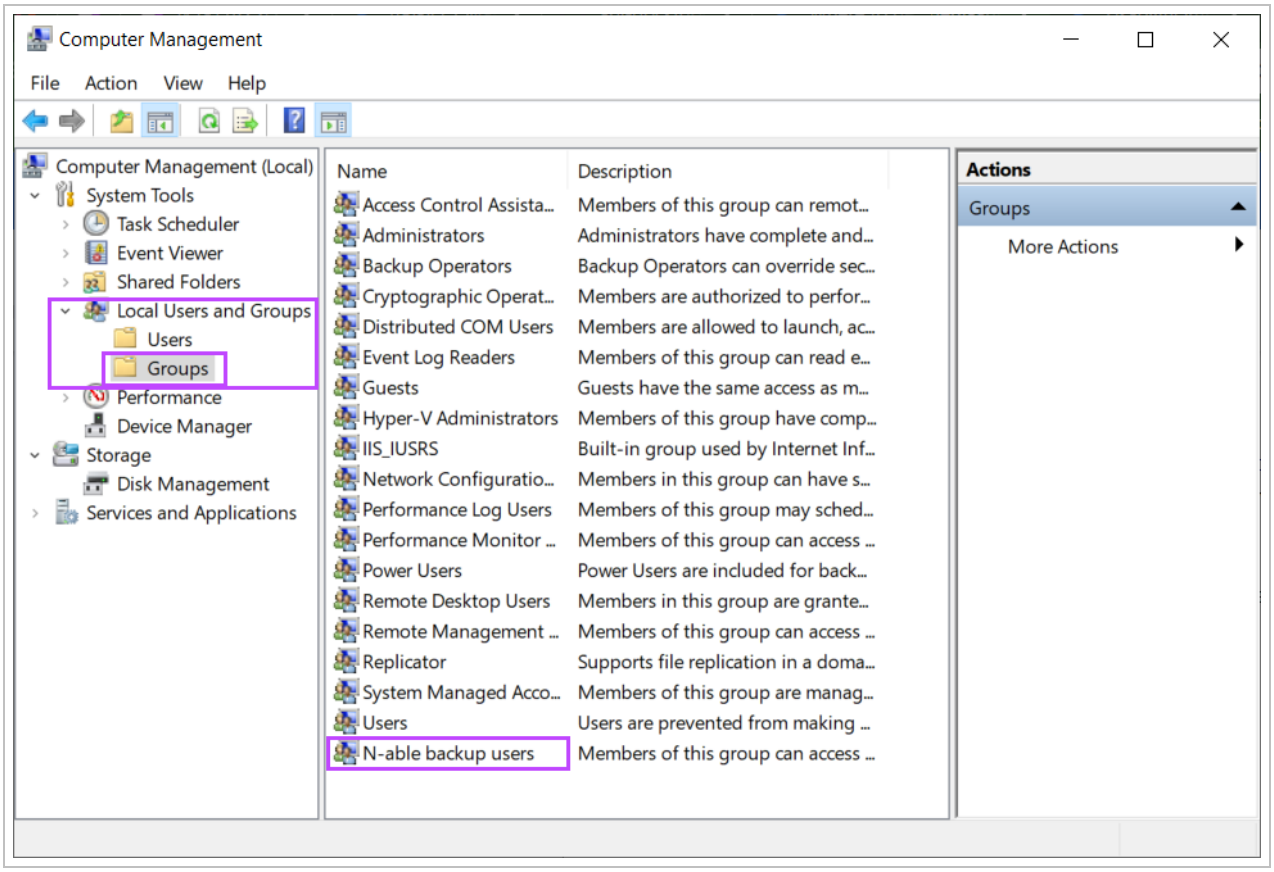
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2008 &R2
- Windows Server 2012 & R2

This security enhancement also means that the Backup Manager client can only be opened on the device by a local administrator or a member of the automatically created "N-able Backup Users" group.

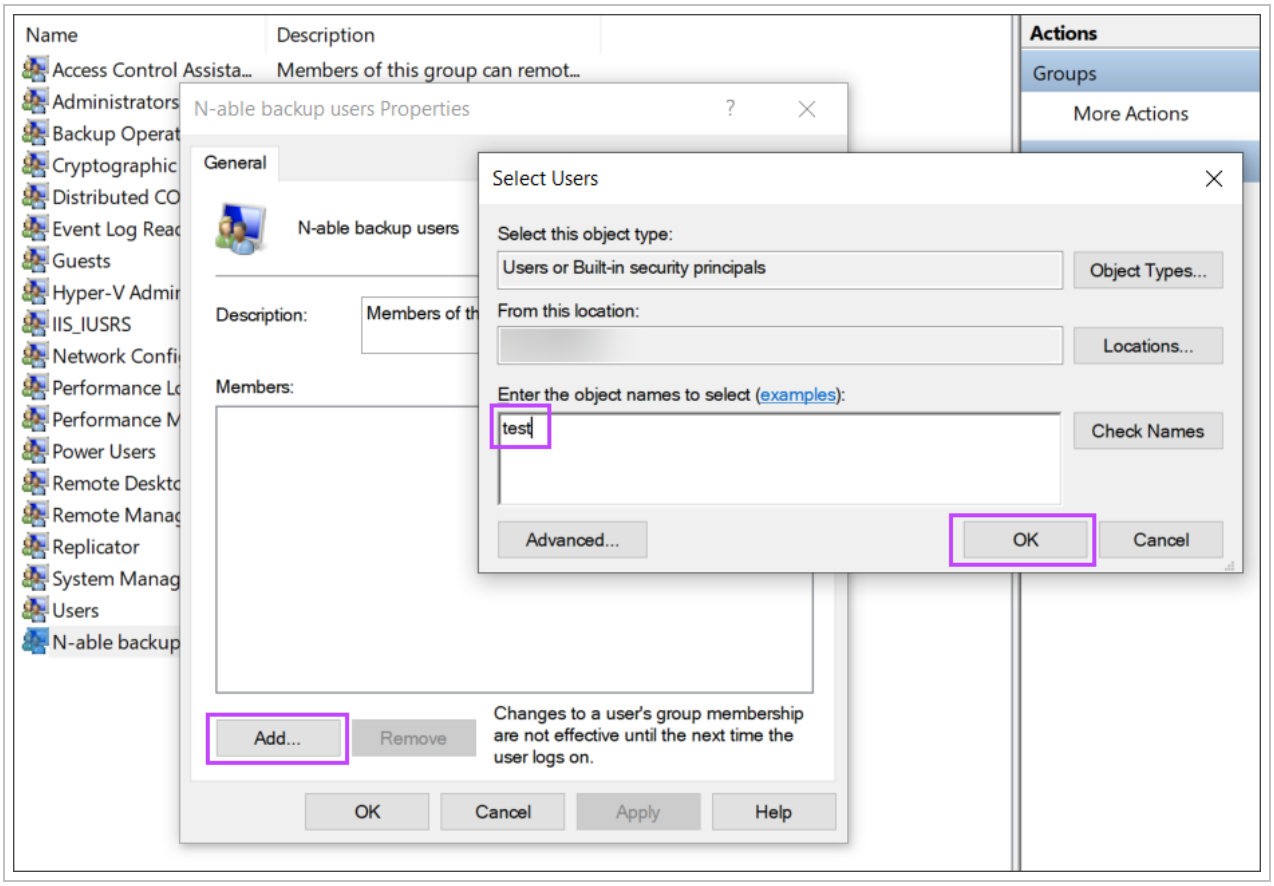
Add users to the "N-able Backup Users" Group **(Windows Only)**

To add users to this group:

1. Open the **Start** menu
2. Type **Computer Management**, then hit **Enter**
3. In the Computer Management window, expand **Local Users and Groups** and open the **Groups** view



4. Right click the **N-able Backup Users** group and select **Properties**
5. Under the Members section, select **Add**
6. Enter the User in the Select Users window and click **OK**



7. Click **Apply**, then **OK** in the N-able Backup Users Properties window

> Once complete, user will be able to start the Backup Manager client and work within this to perform manual backups and restores.

Launch Backup Manager on Windows

From Start

To start the Backup Manager on Windows devices:

1. Open the Start menu
2. View the list of installed applications
3. Click **Backup Manager**
4. Approve permissions for this application to make changes

From Command-Line interface

It is possible to open Backup Manager via the command line interface:

1. Open the Command-line interface for Backup Manager
2. Run the following command:

```
ClientTool.exe bm-ui.open
```

Launch Backup Manager on macOS

To start the Backup Manager on macOS devices:

1. Open the Finder
2. From the Sidebar, choose **Applications**
3. Click the Backup Manager icon

> Ensure you enable Full Disk Access for the Backup Manager *before* running backups on macOS 10.14 Mojave or later.

Launch Backup Manager on Linux

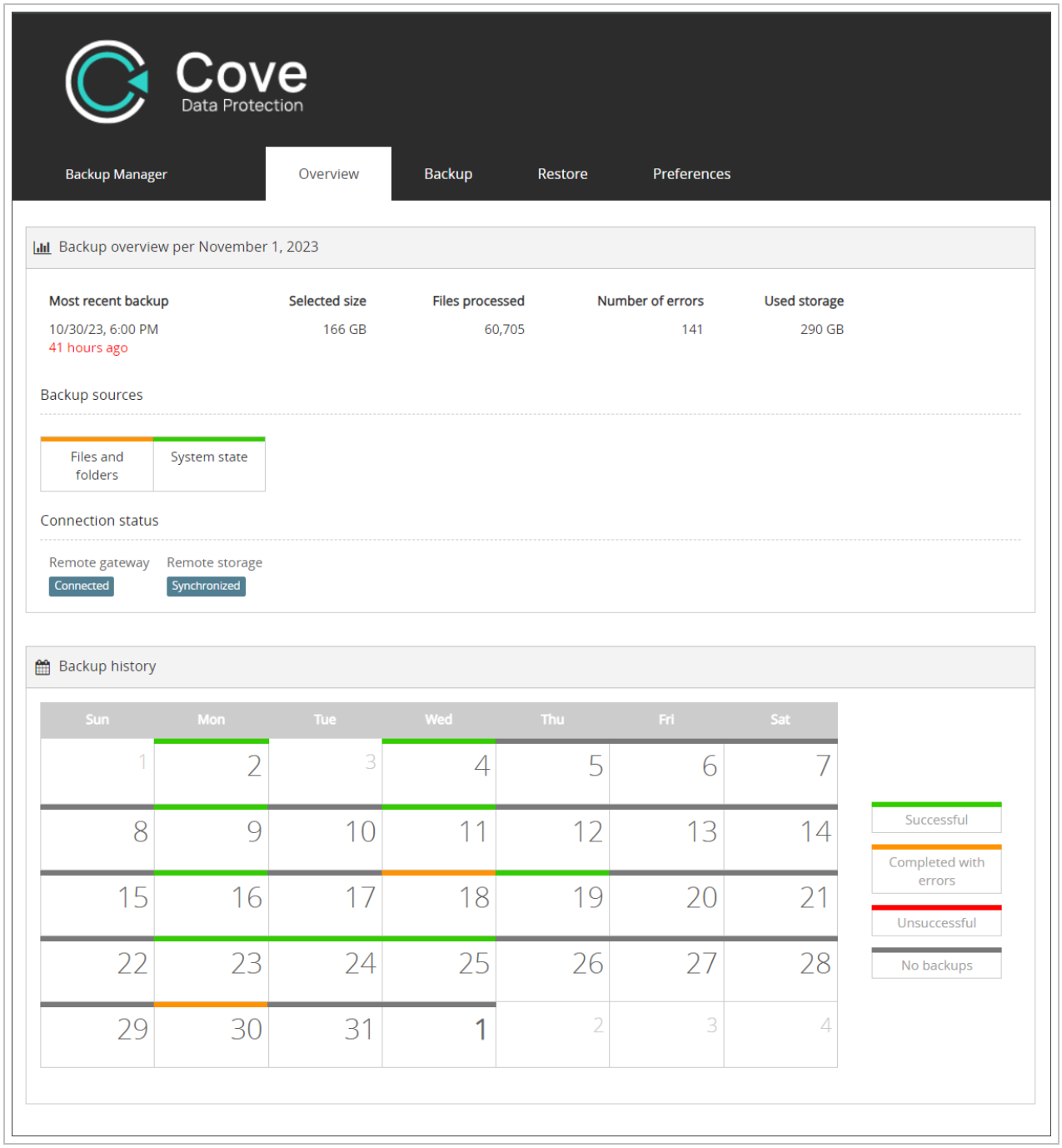
To start the Backup Manager on Linux devices:

1. On the host machine, open the **Terminal**
2. Execute the `ClientTool` command as the **root** user by using the following command:

```
sudo ./ClientTool bm-ui.open
```

Backup Manager guide

The Backup Manager is your primary tool for backup and recovery. It specializes in enterprise-level data that cannot be handled with the help of mass-market solutions: databases, virtual machines and content management systems.



What's inside:

Backup Manager Interface

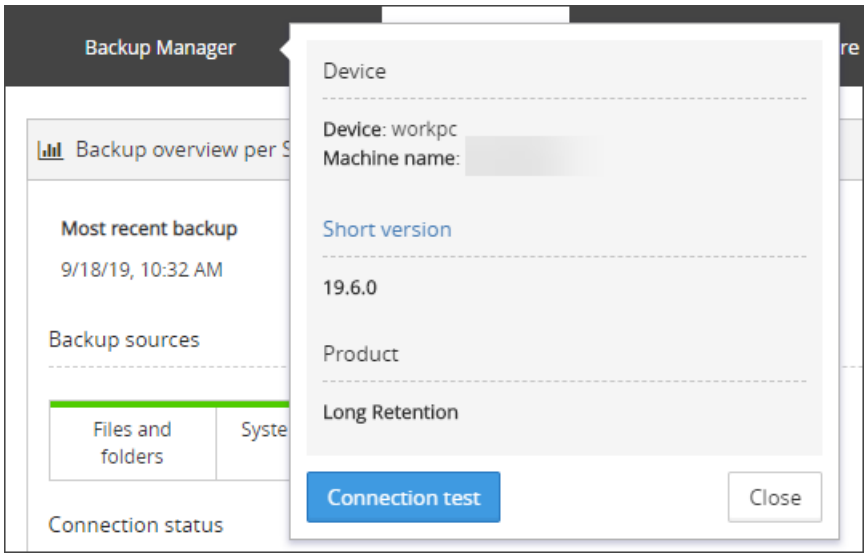
The interface of the Backup Manager consists of four main pages:

- Overview
- Backup
- Restore
- Preferences - This page contains the following sections which are useful for additional configuration
  - General
  - Schedule
  - Scripts
  - Proxy
  - Performance
  - LocalSpeedVault
  - Archiving
  - Backup Filters
  - Advanced
  - Seeding

> If using a backup profile, several of the preference tabs and configuration settings will become locked and cannot be edited. These pages are identified by a banner at the top of the page and the individual settings will be locked with a padlock icon.

Device Details

The graphical user interface (or GUI) also provides details of the device you are currently viewing which can be found by clicking **Backup Manager** on the menu bar.



On this popup you will see the **device name** as it was given during the install, the physical **machine name** as determined on the computer itself, the **version** of Backup Manager installed on the device and the name of the **Product** the device is using (if one is assigned to it).

Overview

The **Overview** page is split into two sections:

- Backup Overview per date
- Backup History

Backup Overview per date

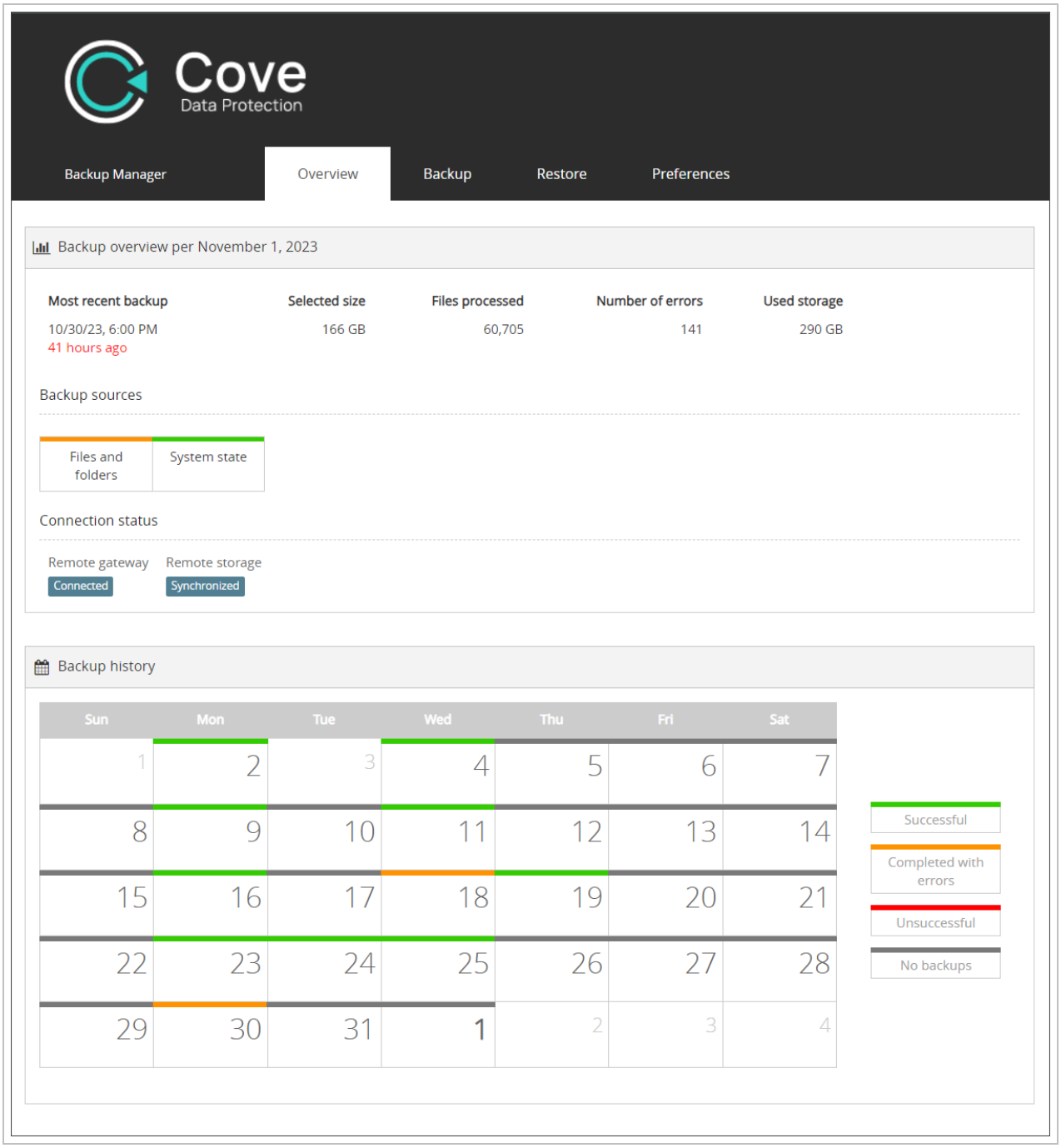
In the Backup overview per date section, information will be provided on the:

- Date and time of the most recent backup and how long ago this was
- Selected size
- Number of files processed
- Number of errors encountered
- Amount of Used Storage
- Which data sources are configured for backup

  > The colour of the bar at the top of each data source denotes the status of the most recent backup of this source, i.e.
  >
  > - **Green** - Successful
  > - **Orange** - Completed with errors
  > - **Red** - Unsuccessful

- Connection status of the remote gateway and remote storage

  > If these say anything other than **Connected** and **Synchronized**, you may encounter problems with your backups



Backup History

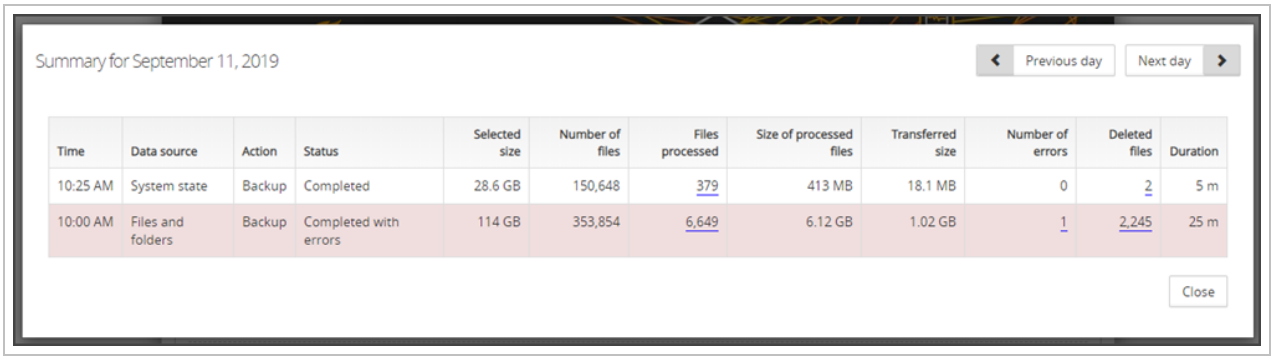
The Backup History section provides a calendar layout of the last 28 days of backups for the device.

The colour of the bar at the top of each day denotes the status of the last backup session of the day. This means that if the device is scheduled to run multiple backup sessions in a day, the colour relates *only* to the last one and cannot show the status of multiple sessions.

The colours relate to the following statuses:

- **Green** - Successful
- **Orange** - Completed with errors
- **Red** - Unsuccessful
- **Grey** - No Backups

To see the details (number of sessions, details on each session, status of the backup and restore sessions carried out) for a given day, select the day to view from the calendar.

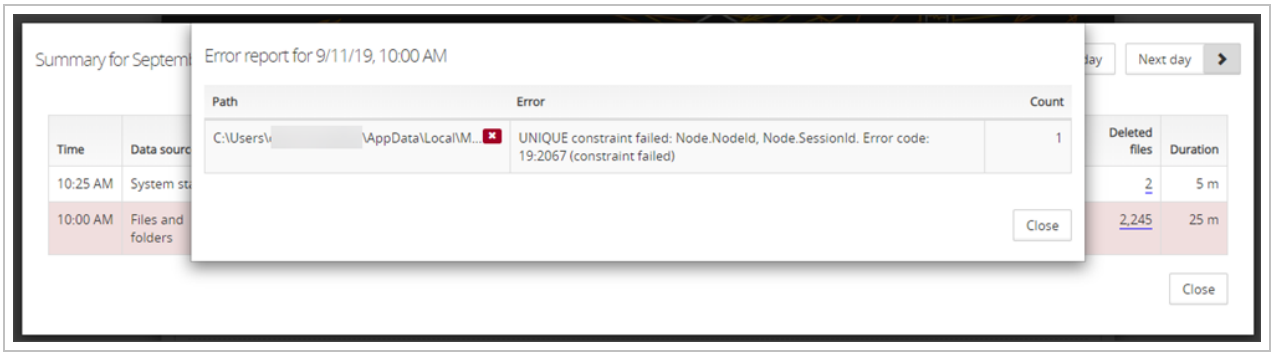


Time	Data source	Action	Status	Selected size	Number of files	Files processed	Size of processed files	Transferred size	Number of errors	Deleted files	Duration
10:25 AM	System state	Backup	Completed	28.6 GB	150,648	379	413 MB	18.1 MB	0	2	5 m
10:00 AM	Files and folders	Backup	Completed with errors	114 GB	353,854	6,649	6.12 GB	1.02 GB	1	2,245	25 m

On this popup, the following details will be provided for each backup or restore session and data source carried out:

- **Time** - Time of the session
- **Data source** - The name of the data source the session relates to
- **Action**
  - Backup
  - Restore
- **Status** - The status of the session
  - Successful
  - Completed with errors
  - Unsuccessful
- **Selected size** - The total size of the selected data source
- **Number of files** - The number of files in the data source checked by the session
- **Files processed** - The number of files (new or changed) actually processed by the backup or restore session
- **Size of the processed files** - The size of the files that were processed by the backup or restore session
- **Transferred size** - The size of the files transferred to storage after compaction or restored
- **Number of errors** - If the session encountered errors during the backup or restore session, the number of errors encountered will be displayed
- **Deleted files** - The number of files deleted from the device
- **Duration** - The total length of the backup or restore session

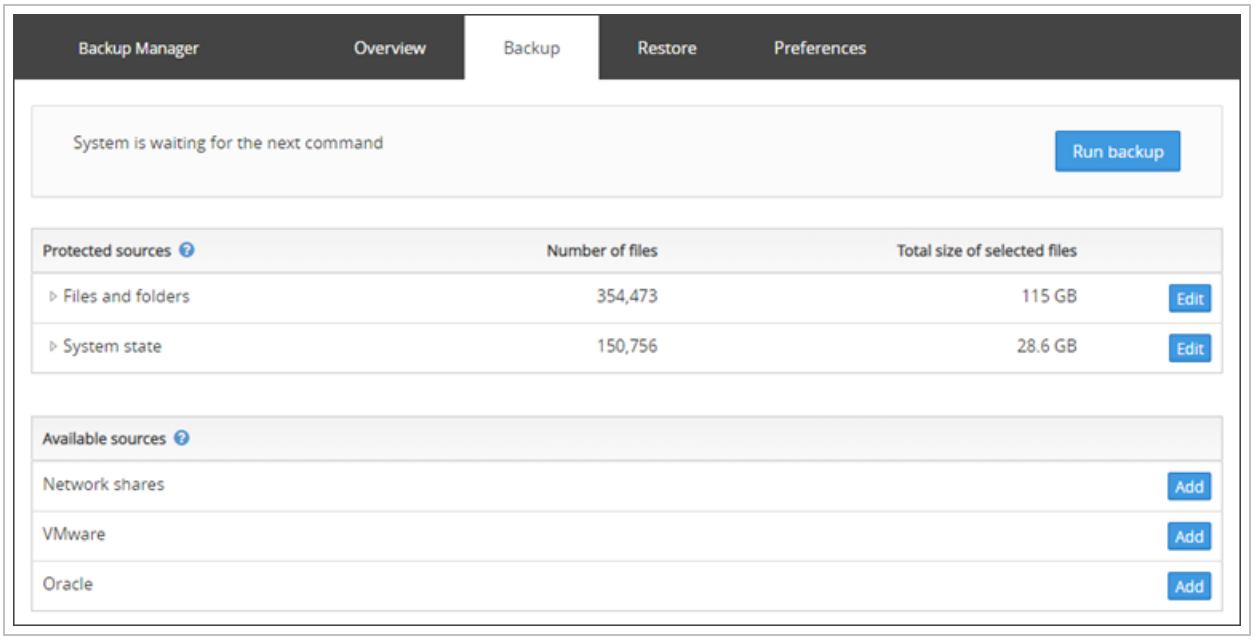
If this session encountered errors, you can click the number of errors, which will provide further details of the error encountered:



If you require assistance with any errors, you can access N-AbleMe here where you can find articles on how to fix issues yourself, or you can click **Contact Support** in the top right corner of N-AbleMe to log a ticket with our support team for further help.

Backup

The **Backup** page allows you to configure your backup selections. This is where you add data source selections to determine what information we will store during the backup.



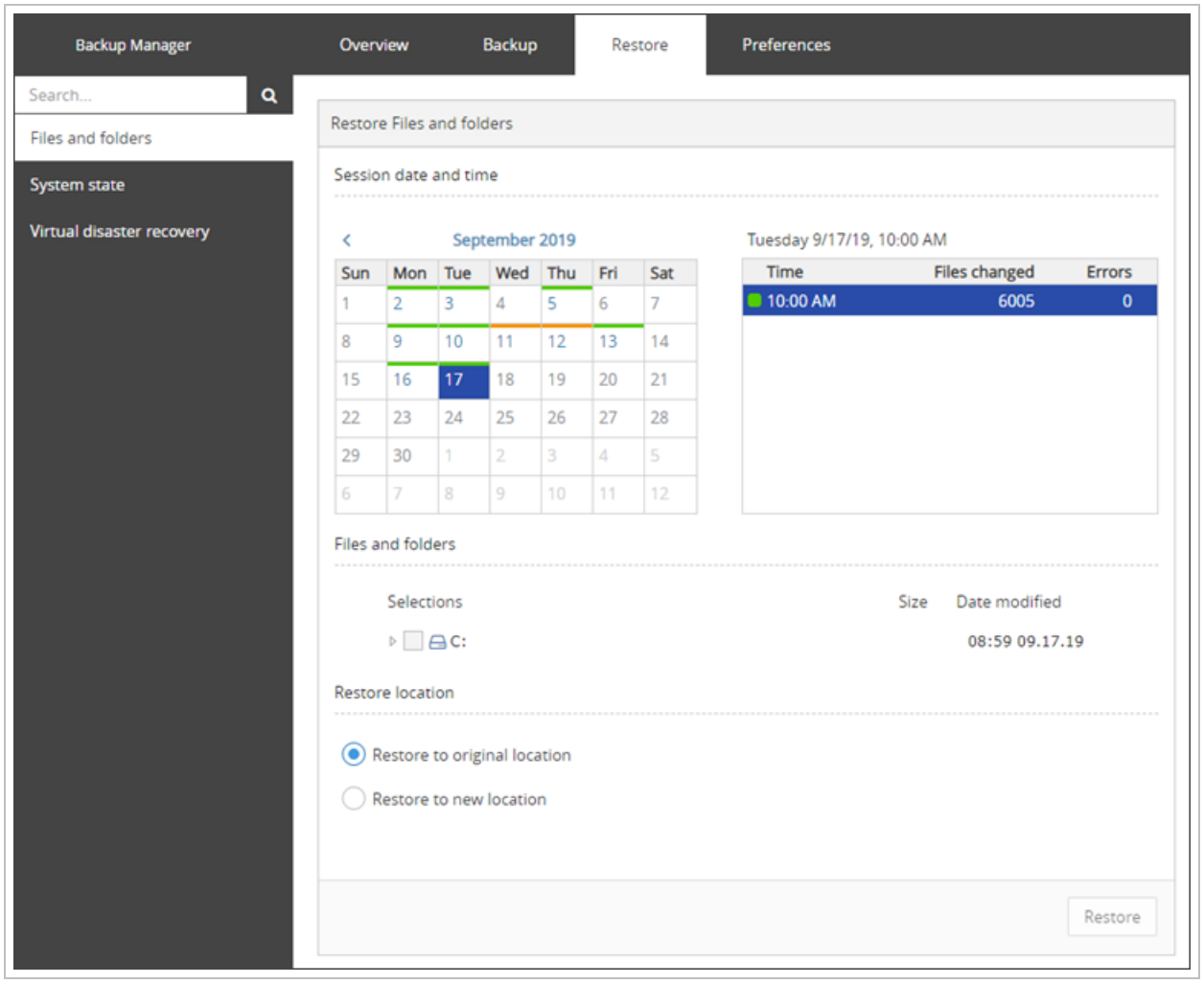
Any information you wish to back up **must** be selected in here. If it is not, it will not be included in the backup.

> Please note: adding a selection in here does not enable a backup schedule, this must be done either using a backup profile or in the Preferences page.

For full details on enabling backups, see Enabling backups in Backup Manager page.

Restore

The **Restore** page allows you to see the data sources, days and sessions available for recovery.



For detailed steps using the Backup Manager to restore data to the same device, see the Recovering data in Backup Managerpage.

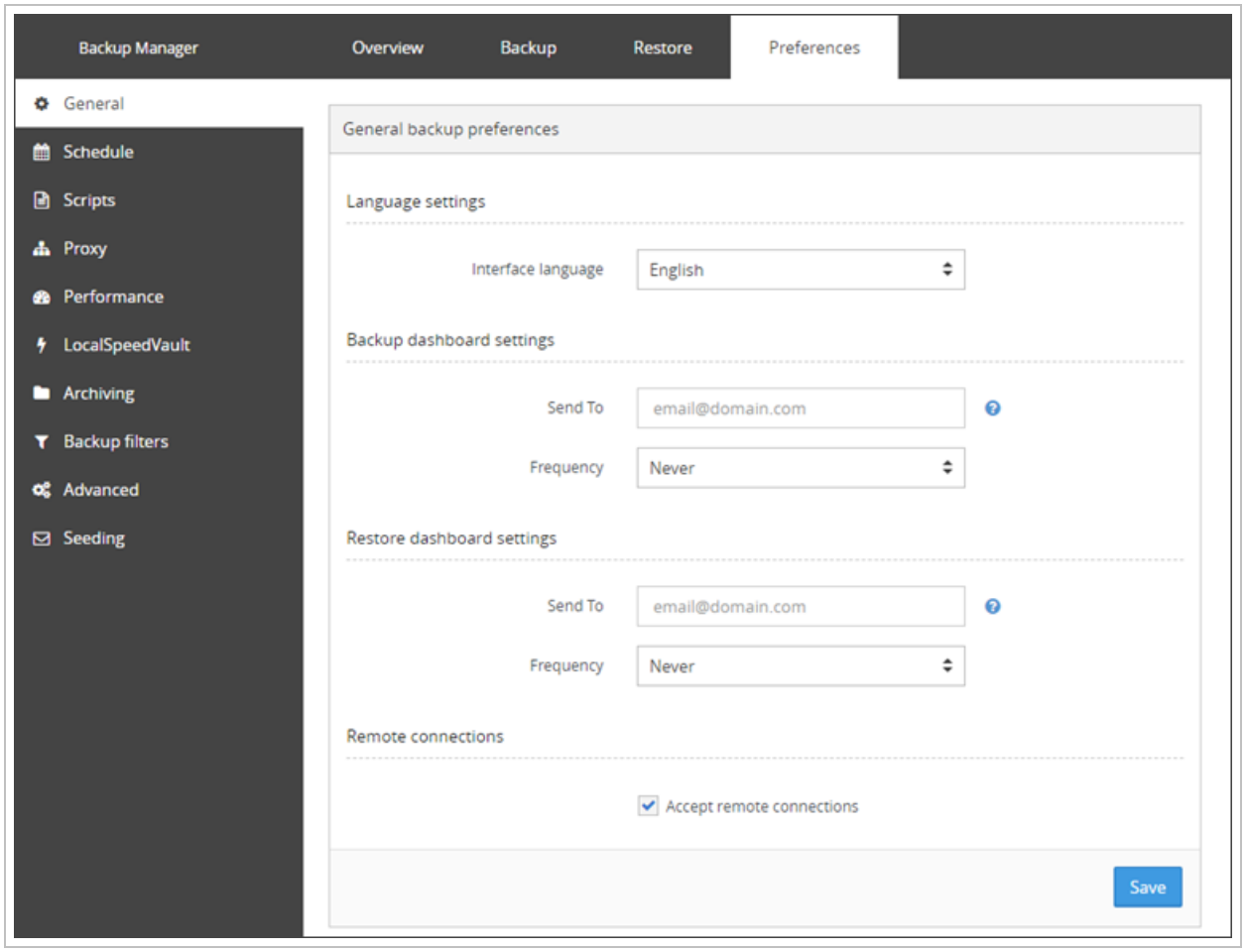
Preferences

The **Preferences** page contains several further tabs which may be useful in configuring the backup device, but may not be necessary during an emergency.

General

In here you can:

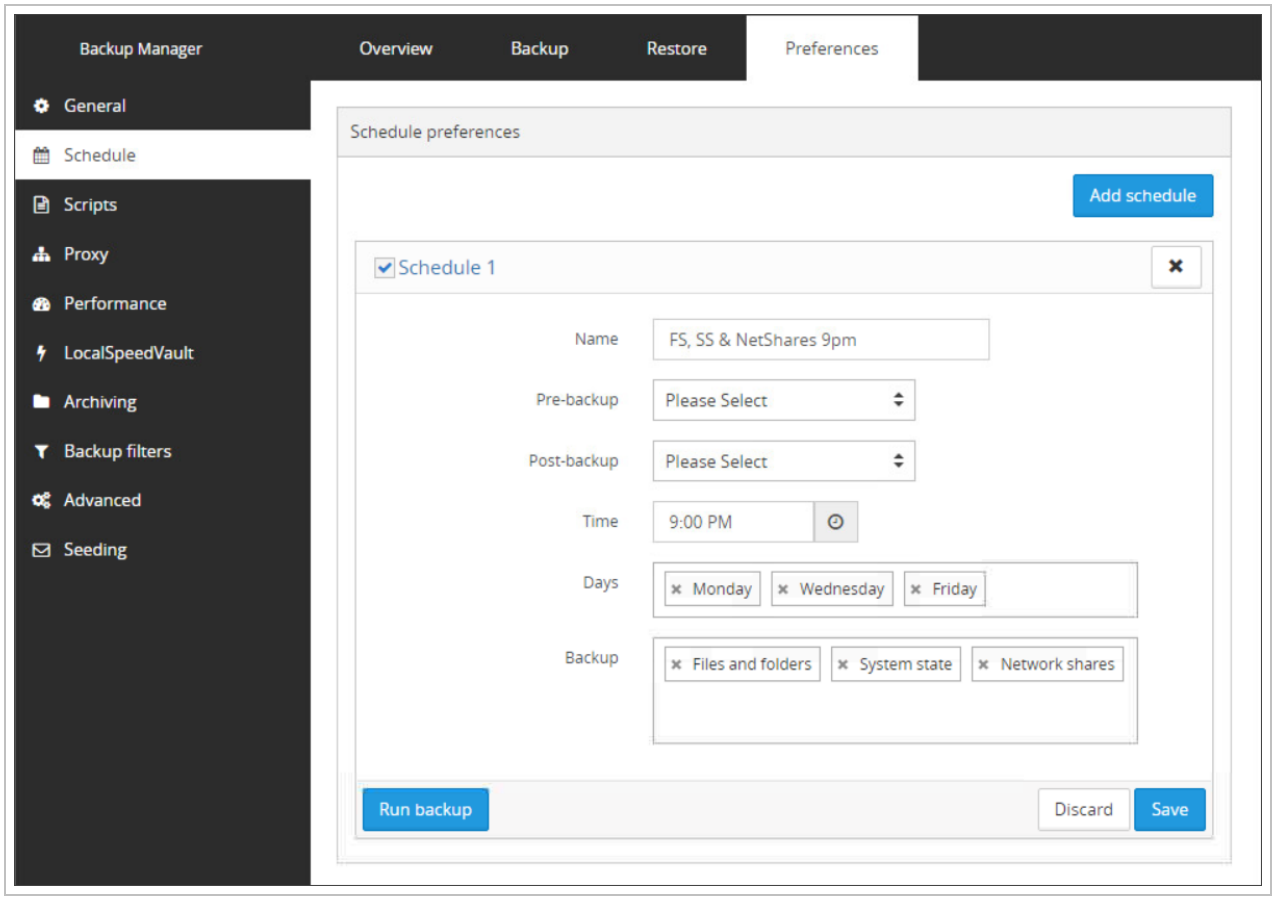
- Set the language the page should be displayed in (this can be set using a profile)
- Set an email address to send emails to regarding the success of backup jobs (this can be set to send **daily**, **every Wednesday and Saturday**, **every Saturday** or **never**)
- Set an email address to send emails to regarding the success of restore jobs (this can be set to send **daily**, **every Wednesday and Saturday**, **every Saturday** or **never**)
- Allow or disallow remote connections to the device's Backup Manager GUI.



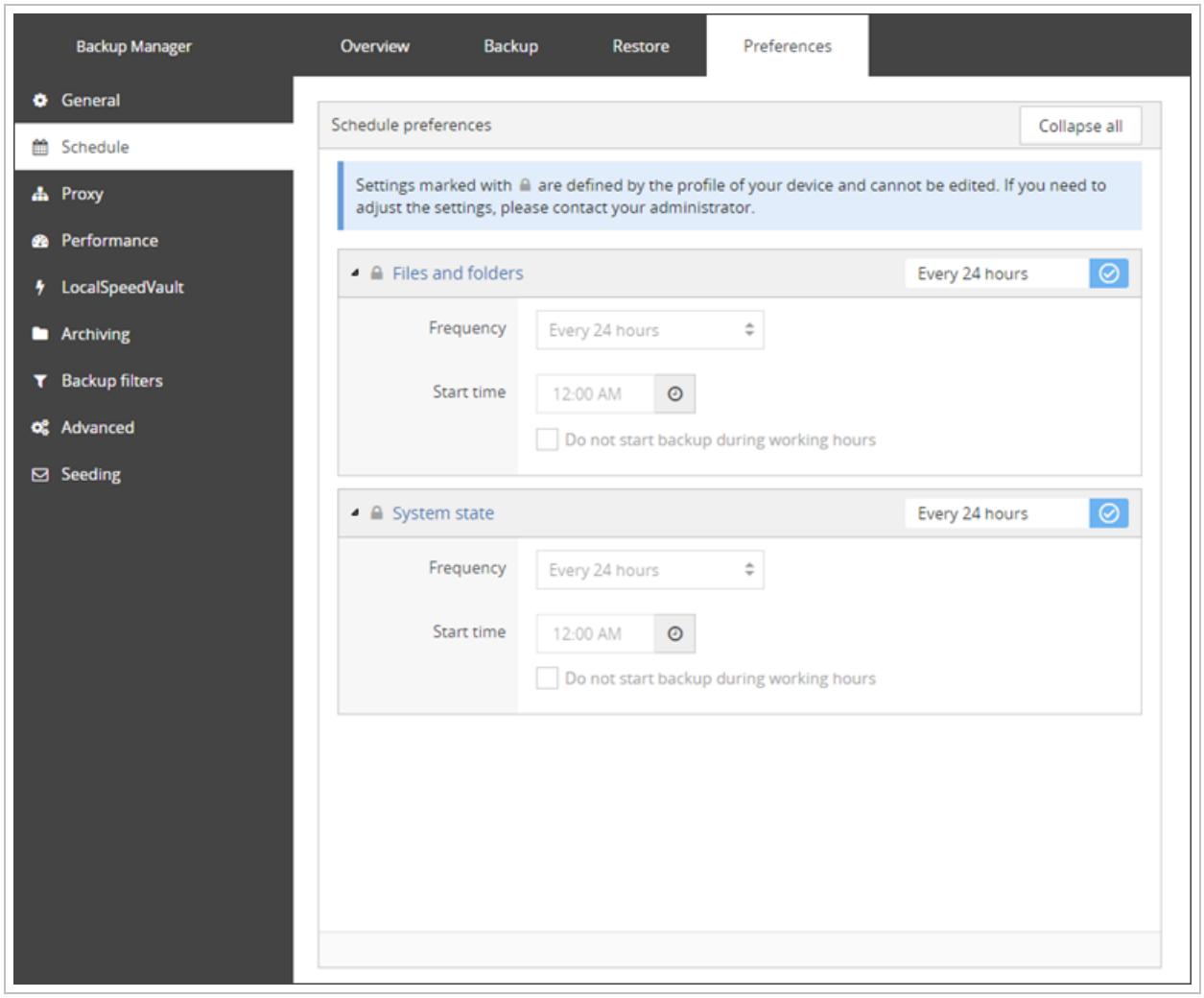
Schedule

If you are not using a backup profile, the **Schedule** tab will look as below and will allow you to set multiple timings for backing up data sources whenever and however frequently you need.

You can create separate schedules per data source if this is most convenient for you. However, during an emergency, it is unlikely that this would be necessary.

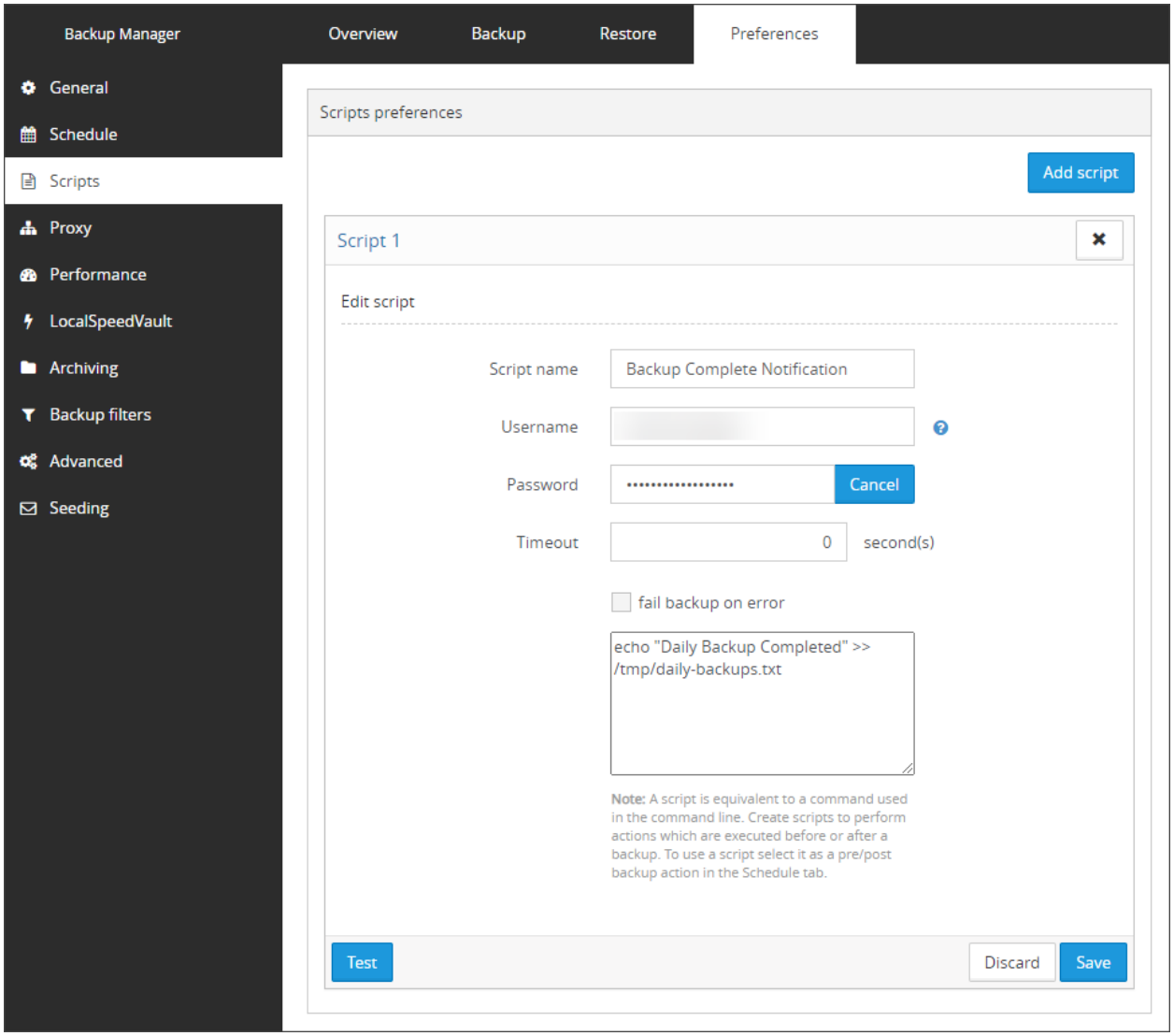


If you have a profile configured and assigned, the **Schedule** tab will look as below, and will show you the configuration previously configured on the Management Console.



Scripts

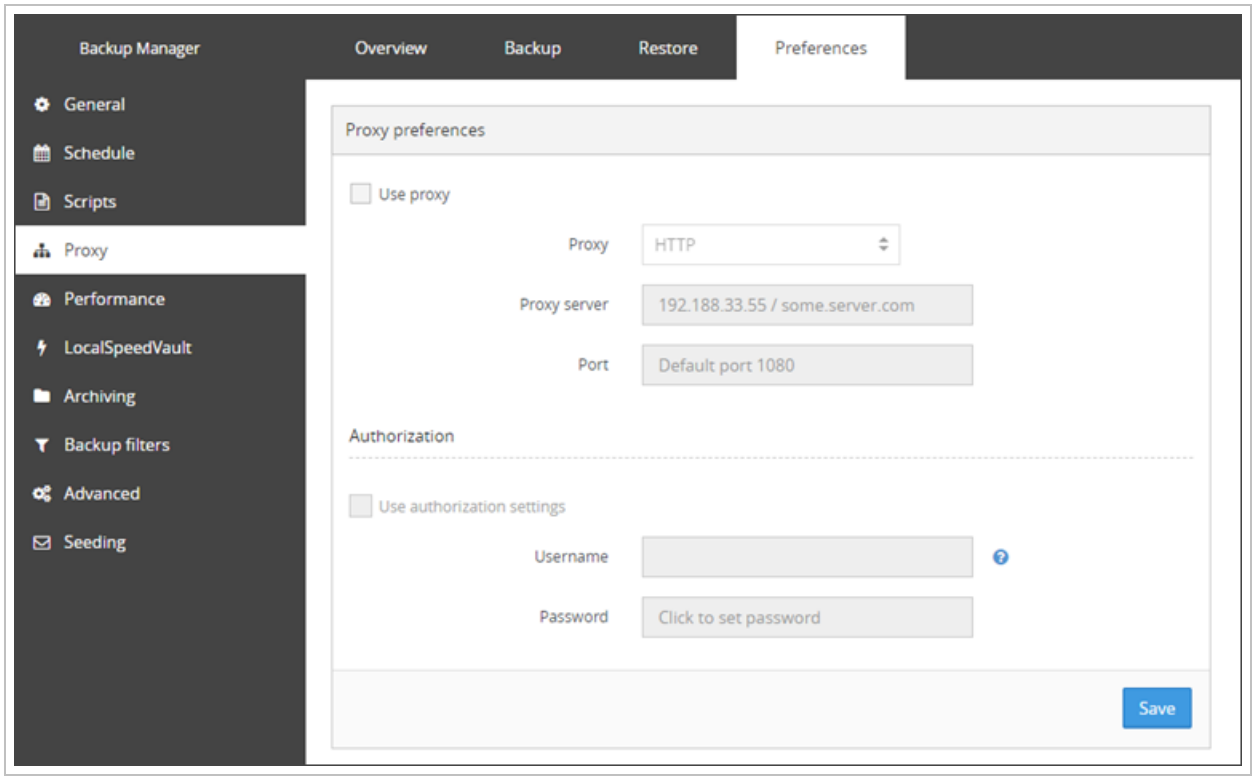
If you have a profile assigned to the device, this tab will not be displayed.



For full details on configuring Scripts, see the for details.

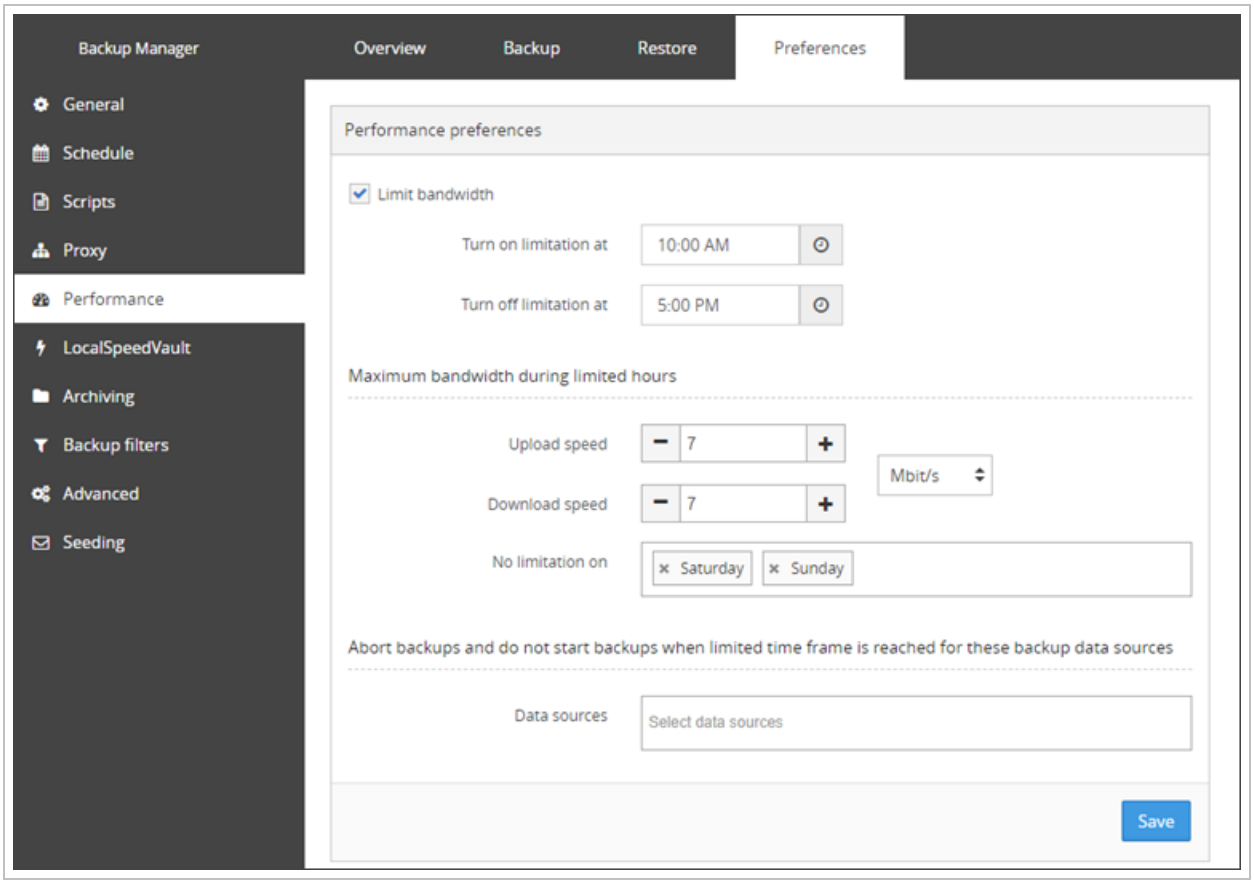
Proxy

f you would like to configure the use of a proxy, you can do so in here by ticking 'Use proxy' and supplying the details for this and saving.



Performance

The **Performance** tab allows you to enable bandwidth limitations for the device.

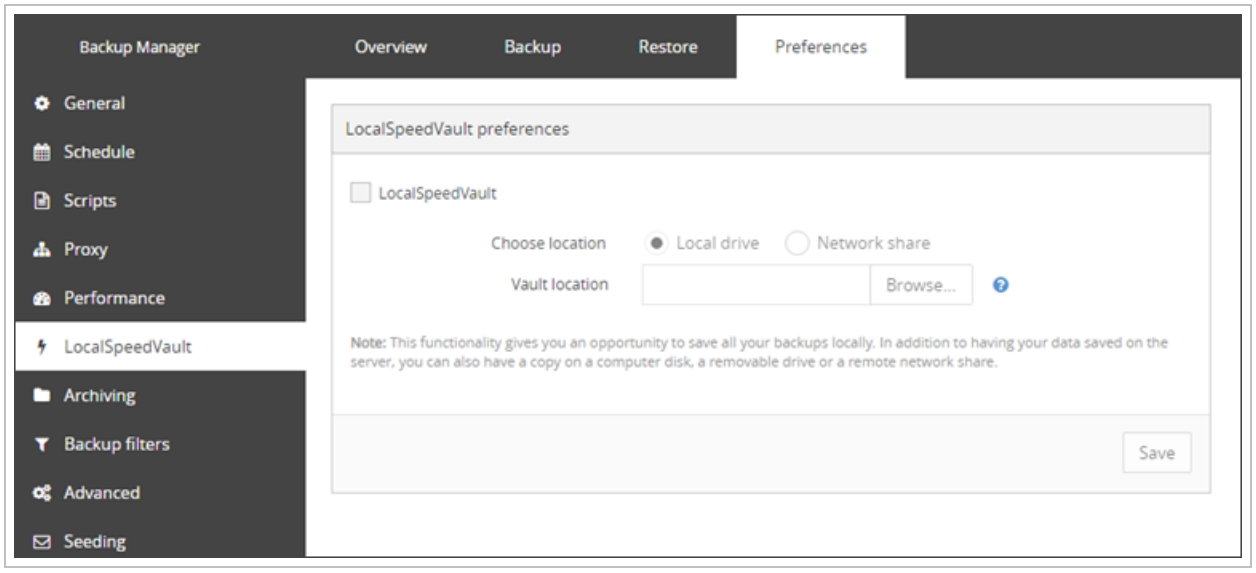


Further information on bandwidth limiting can be found here.

LocalSpeedVault

If you are using a backup profile, this can be set outwith this page, however can be set in here instead if it is missed during the profile configuration.

A LocalSpeedVault is an additional storage directory for the backup data which is automatically synchronized with the cloud where your backup data is stored. Having an LSV configured speeds up backup and restore sessions, but is not mandatory.

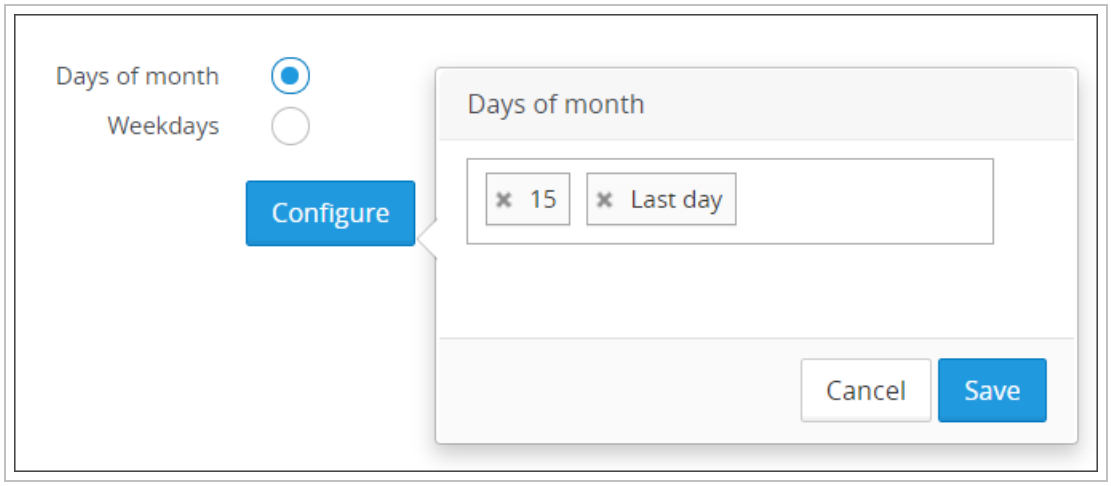


If you would like information on configuring a LocalSpeedVault, please see.

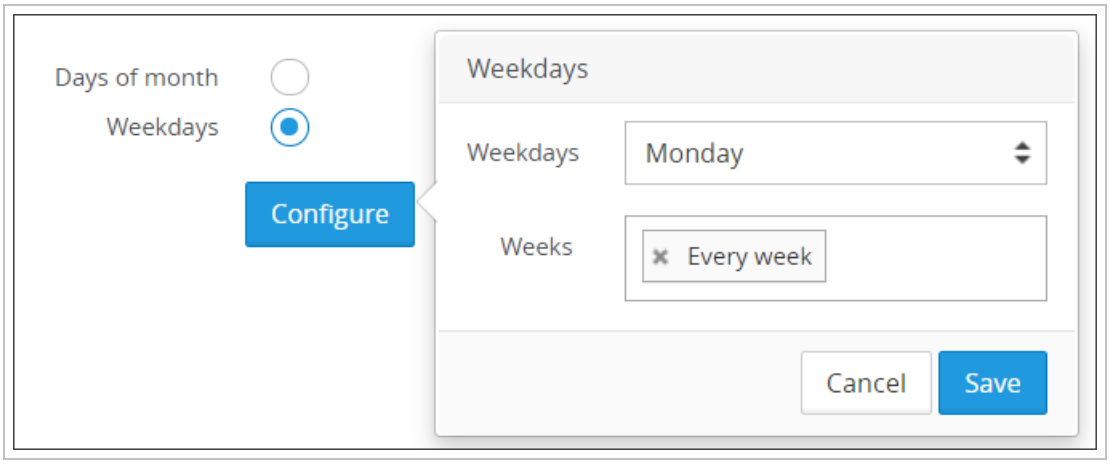
Archiving

Using the **Archiving** tab, you can set the system to store the backup session immediately following the archiving time to be stored indefinitely. If no archive is configured, data will be cleared when the retention period is reached.

The default retention period from the date that the backup was completed is 28 days and 3 file versions.



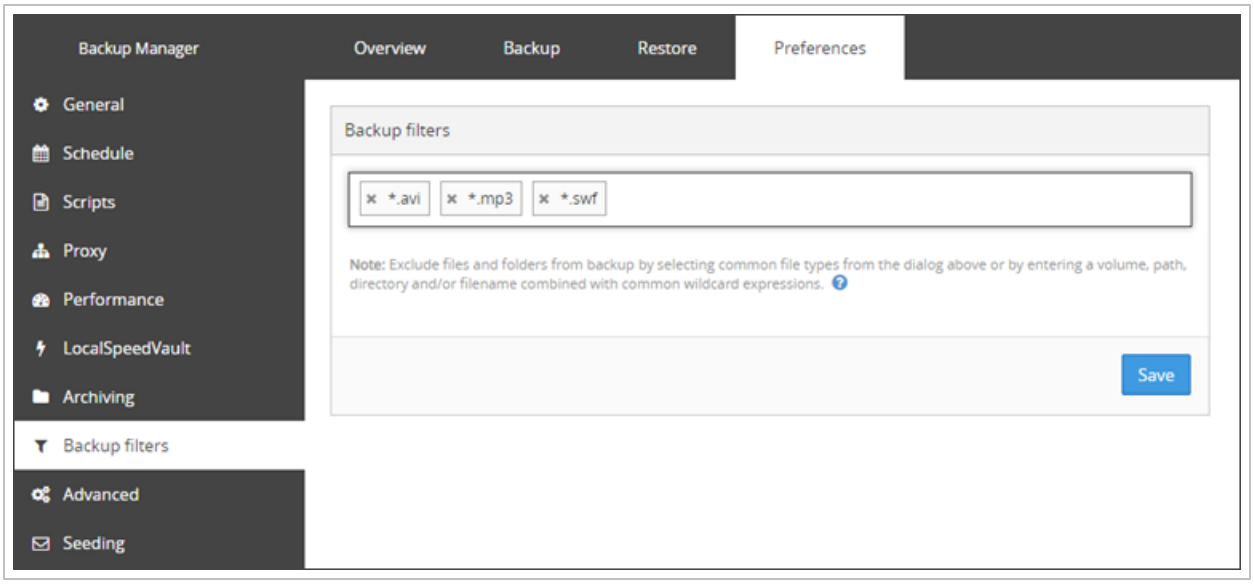
You may choose to archive sessions by dates in the month - for example the first day of the month and the 15th day of the month - as above, or you can choose by days of the week - such as every Sunday - as below.



For further details on archiving backup sessions, see the Archiving backup sessions in Backup Manager page .

Backup Filters

Backup filters are used to exclude certain file types or file directories from being backups.

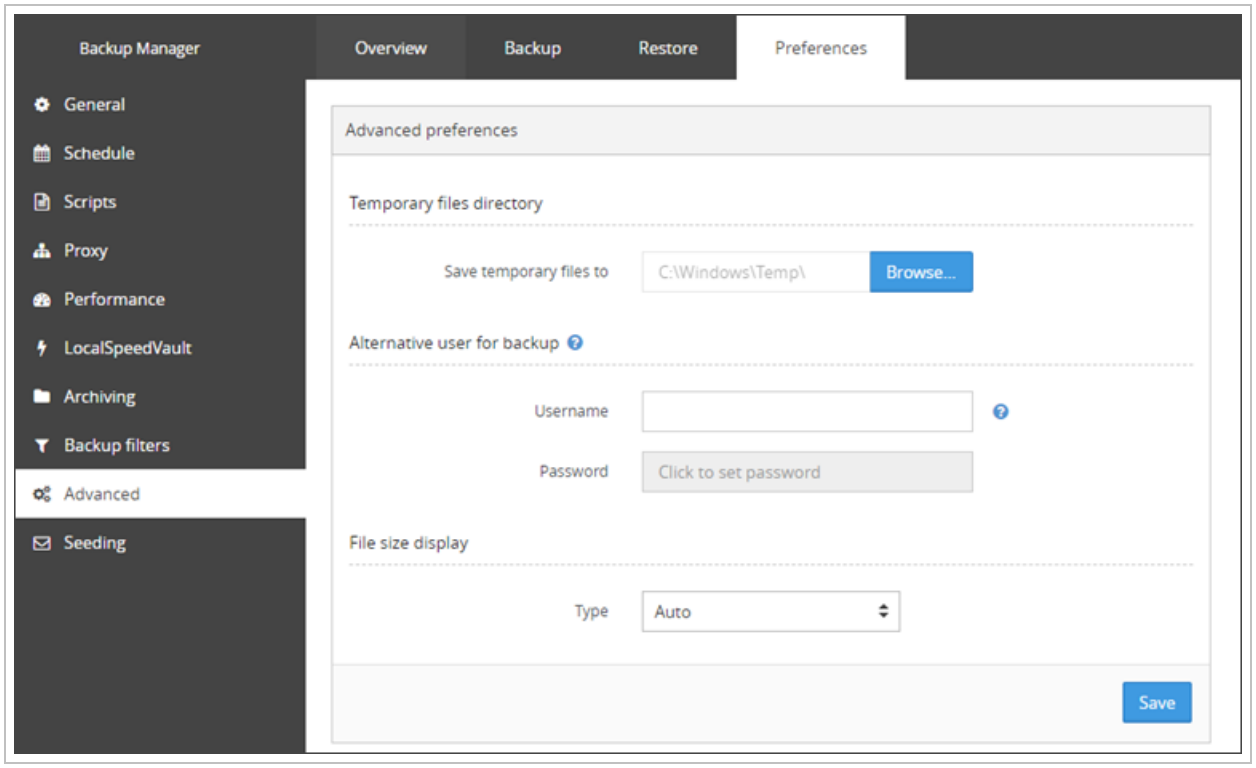


This can also be set in a backup profile, but as the page does not become locked, you can amend this as needed.

You can find full details on backup filters here.

Advanced

In the **advanced** tab, there is functionality to change the temporary file directory, add a second user for backup access and the file size display format.



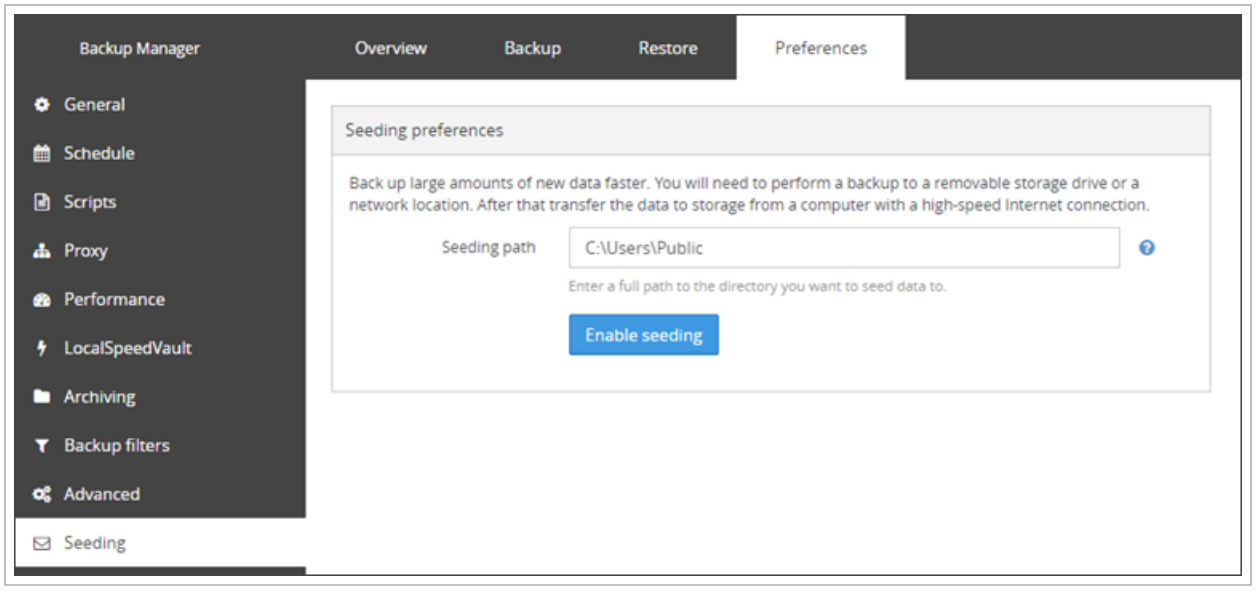
If a temporary file directory has been provided in the backup profile, this section will be locked.

To see full details on configuring the settings on this tab, see the Advanced page .

Seeding

Please see the Seed backup in Backup Manager page for details on enabling and configuring seeding mode.

This page cannot be configured outside of the GUI and is not included in any profile settings.



Preferences for Backup Manager

The **Preferences** page in Backup Manager contains several tabs which are used in configuring the backup device.

What's inside:

General

Language

The Backup Manager can be used in any of these 9 languages:

- English
- Dutch
- Russian
- German
- Spanish
- French
- Portuguese
- Norwegian
- Italian

Backup Dashboard Settings

Send a report regarding the status of the **backup** to the email address(es) entered into the **Send To** field.

> Separate multiple recipient email addresses with a semicolon, e.g. `user1@company1.com;admin@company1.com`

Using the **Frequency** dropdown, set how often to send the report to the provided addresses:

- Daily
- Every Wednesday and Saturday
- Saturday
- Never

Restore Dashboard Settings

Send a report regarding the status of the **restore** to the email address(es) entered into the **Send To** field.

> Separate multiple recipient email addresses with a semicolon, e.g. `user1@company1.com;admin@company1.com`

Using the **Frequency** dropdown, set how often to send the report to the provided addresses:

- Daily
- Every Wednesday and Saturday

- Saturday
- Never

Remote Connections

Enable or disable remote connections to the device by either selecting or deselecting this setting.

Save

You must make sure to save any changes you make before moving away from this page.

Schedule

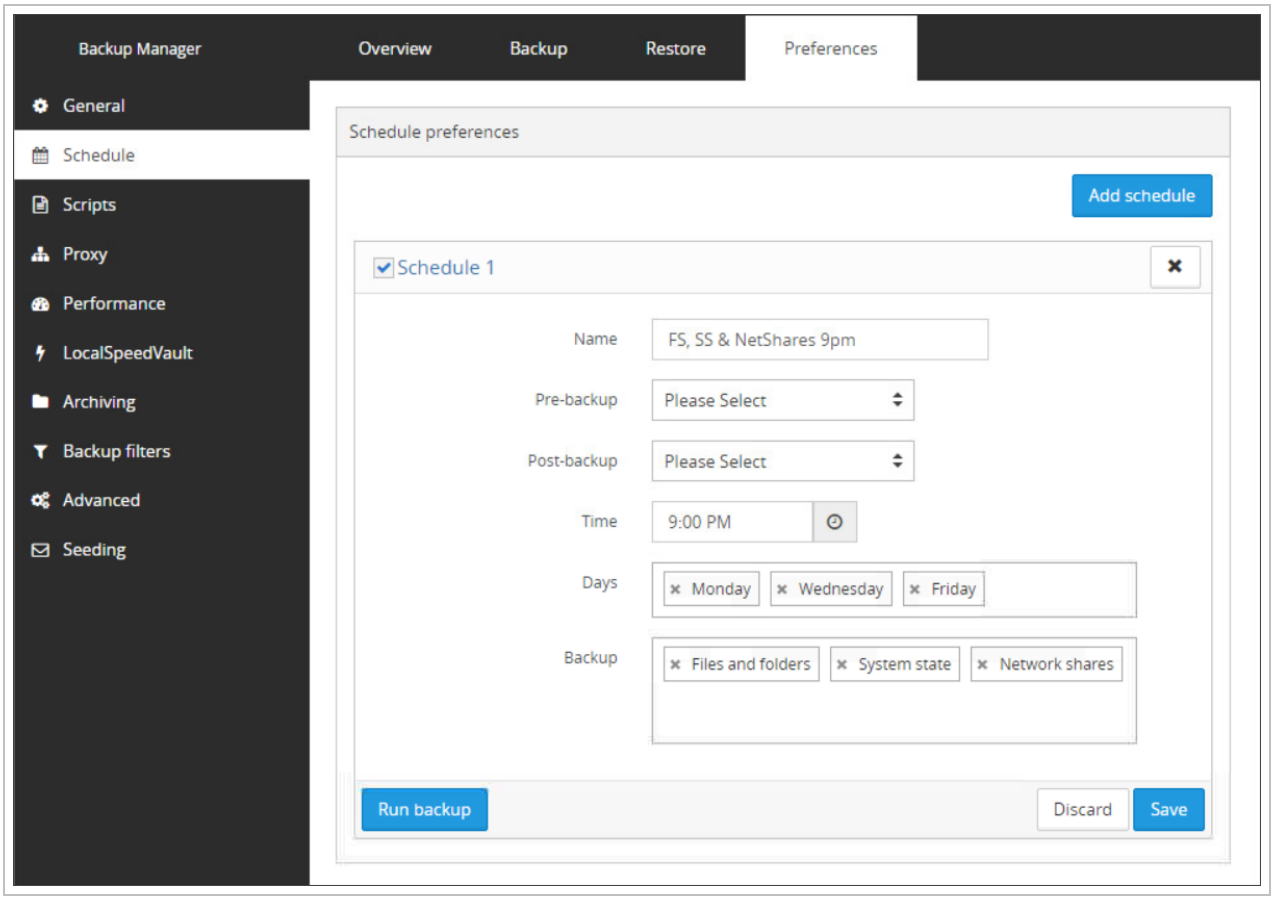
The most convenient method of configuring backups is to set up a **backup schedule** which will automatically run the backups without requiring you to intervene.

You can create multiple schedules for each device, for example if you want Files and Folders to run at 9am but you want Files and Folders, System State and MySQL to run at 9pm.

Create Schedule

To create a backup schedule:

1. Launch the Backup Manager for the device
2. Open the **Preferences** tab
3. Click **Schedule**
4. Select **Add Schedule**



5. Give the schedule a name - make this something relevant to the backup configured such as "FS, SS & MyS 9pm"
6. Optional - If you have created any scripts, these can be selected to run before the backup (Pre-backup) or after the backup (Post-backup) by selecting them from the given dropdowns.
7. Set the time for the backup to run
8. Choose the days on which you want the backup to run
9. Select the data sources to backup
10. Click **Save**

> If you want to back up a data source regularly, it **must** be configured for backup as well as selected in a schedule or a profile. This can be done by following the Schedule steps above.

> If you have not configured the backup selection, the schedule will run, but as no data source configuration exists, nothing will be backed up.

Disable Schedule

If you have multiple schedules listed in this page, you can enable or disable them by ticking the check box beside the name of the schedule. Disabling a schedule does not delete it, but will stop it from running until you manually enable it again.

Edit Schedule

To edit a schedule, you just need to expand the schedule in question, make the necessary changes and click **Save**.

Delete Schedule

To delete a schedule, simply click the **X** to the right of the schedule name, you will be prompted to confirm deletion of the schedule - click **Yes**.

> Please note, once a schedule has been deleted, it cannot be undeleted and would have to be recreated manually.

Save

You must make sure to save any changes you make before moving away from this page.

Scripts in Backup Manager

You can set up Backup Manager client to perform certain actions before or after backups. This is done with the help of scripts. You can use any command line commands as scripts in Backup Manager.

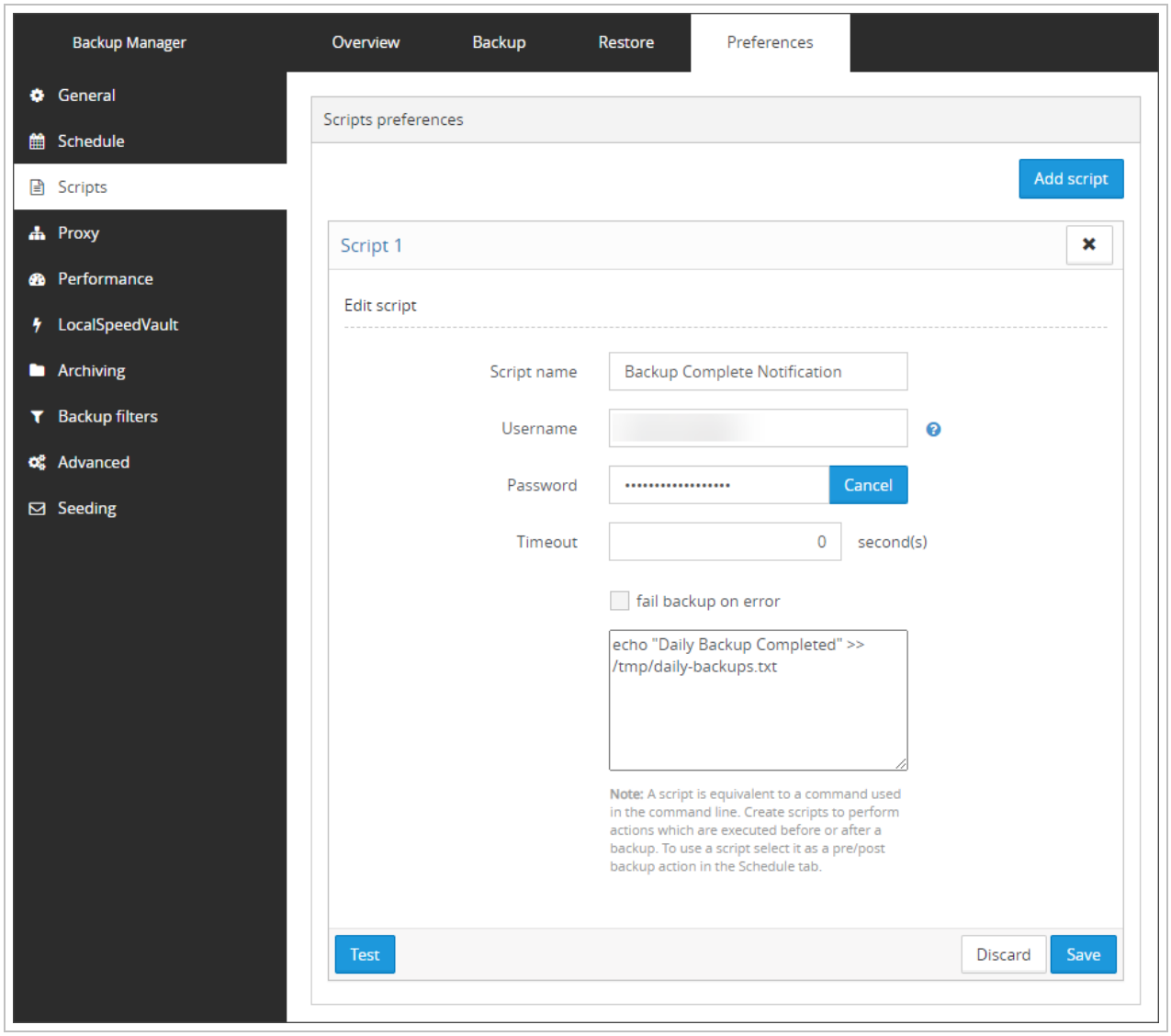
> The scripts tab is only available when opening the backup manager locally on the device.

Adding scripts

Before you can add the script to run as part of the schedule, you must first create the script in the Backup Manager client.

1. Launch the Backup Manager for the device
2. Click **Preferences > Scripts**

3. Click **Add script**



4. Configure the settings:
   - **Script name** - Name the script something that will be recognizable when adding the script to the schedule, e.g. Backup Completed Notification
   - **Username** - The username for a user with sufficient permissions to run scripts on the local system
   - **Password** - The password for the username with sufficient permissions to run scripts on the local system
   - **Timeout** - enter a time limit (in seconds) after which the script will be stopped
   - **Fail backup on error** - Check this box to fail the backup, or stop the backup from running if the script returns an error

     > If a **pre-backup script** is important, enabling the **fail backup on error** setting will stop the following backup from running

   - **Script body** - In the remaining text box, provide the script content
5. *(optional)* Click **Test** to make sure the script has been entered correctly
6. Click **Save**

Available settings for scripts

- Scripts run under the **LocalSystem** account that Backup Manager normally operates under. If your script requires some special permissions, you should provide an alternative username and password. The account you specify must be from the **administrative group**. Different username formats are supported: `username`, `username@domain` and `domain\username`
- The **Group** field on Linux and macOS devices requires the name of the group

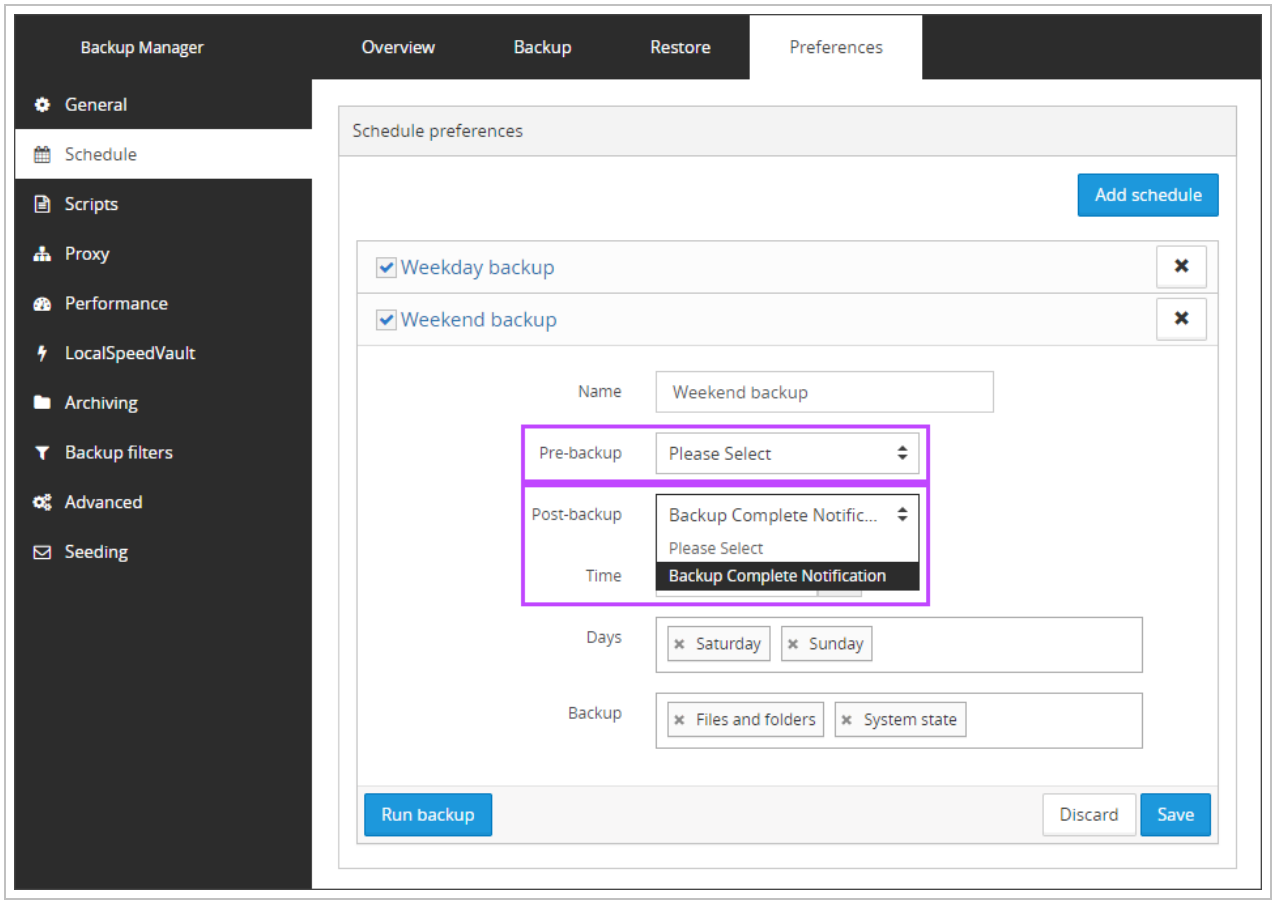
Applying scripts

The scripts you have added become available for selection in the backup schedule settings **(Preferences > Schedule)**. You can add a script to an existing backup schedule or create a new schedule for this purpose.

Once added to the schedule, these scripts run once per backup source. For example, where a schedule contains both *Files & Folders* and *System State* backup sources, a schedule's pre-backup script runs before each backup takes place.

1. Launch the Backup Manager for the device
2. Click **Preferences > Schedule**
3. Expand an existing schedule, or click **Add Schedule** to create a new one

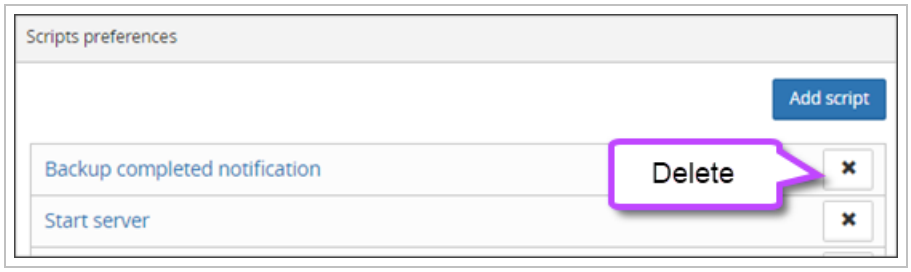
4. If adding a script to an existing schedule, select the script from the **Pre-backup** or **Post-backup** dropdown boxes. If creating a new schedule, follow these instructions to create a new schedule



5. Click **Save**

Removing scripts

To remove a script that you no longer need, remove it from any schedules, then navigate to the Scripts tab and delete it using the cross icon next to its name.



Note for Linux users

The syntax for Linux machines is the same as for usual bash scripts. Here is an example:

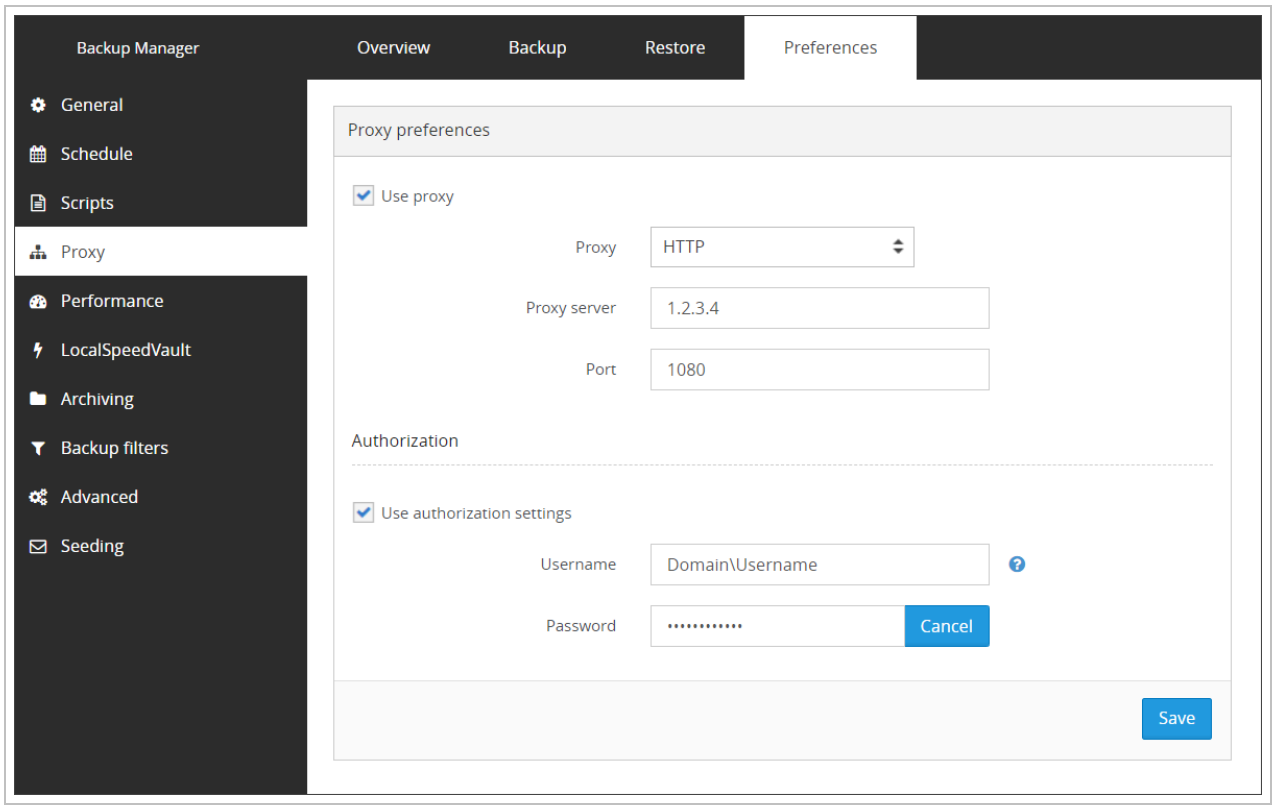
```
#!/bin/sh
echo "Daily backup completed" >> /tmp/daily-backups.txt
exit 0
```

Save

You must make sure to save any changes you make before moving away from this page.

Proxy

You may configure the Backup Manager to use a **Proxy** from this tab.



Enable Proxy

1. Enable **Use Proxy** by placing a check in the box
2. Provide the proxy details:
    - **Proxy** - select from one of the following proxy types:
        - HTTP
        - SOCKS4
        - SOCKS5
    - **Proxy Server** - provide the proxy address
    - **Port** - Enter the port to use, the default is 1080
3. **Save** the changes

Authorization

Once the proxy is enabled, the **Authorization** section becomes available. To use these:

1. Enable **Use authorization settings** by placing a check in the box
2. Provide authorization details:
    - **Username** - Enter a username with sufficient credentials to access the proxy server e.g. `domain\username` or `username`
    - **Password** - Enter the password for the user
3. **Save** the changes

Save

You must make sure to save any changes you make before moving away from this page.

Performance

By default, Backup Manager does not use any kind of bandwidth throttling or restriction, meaning that if a backup is set to run during regular working hours, or begins over night and continues into normal working hours, Cove Data Protection (Cove) will not throttle bandwidth by default. This can, however, be set manually by enabling bandwidth limiting and restricting the maximum upload and download speed during backups and the times in which backups are permitted to start.

Reasons to enable Bandwidth Limiting

This can be useful if the device:

- Is used heavily during certain hours
- Has other programs installed which require exclusive access to databases or files
- Has a slow internet connection

Feature availability

The bandwidth throttling feature is supported on Windows, macOS and Linux devices.

Set Bandwidth Limiting

There are two ways to configure bandwidth limitation, one through the Backup Manager client as detailed below and the other by using the **set bandwidth** remote command.

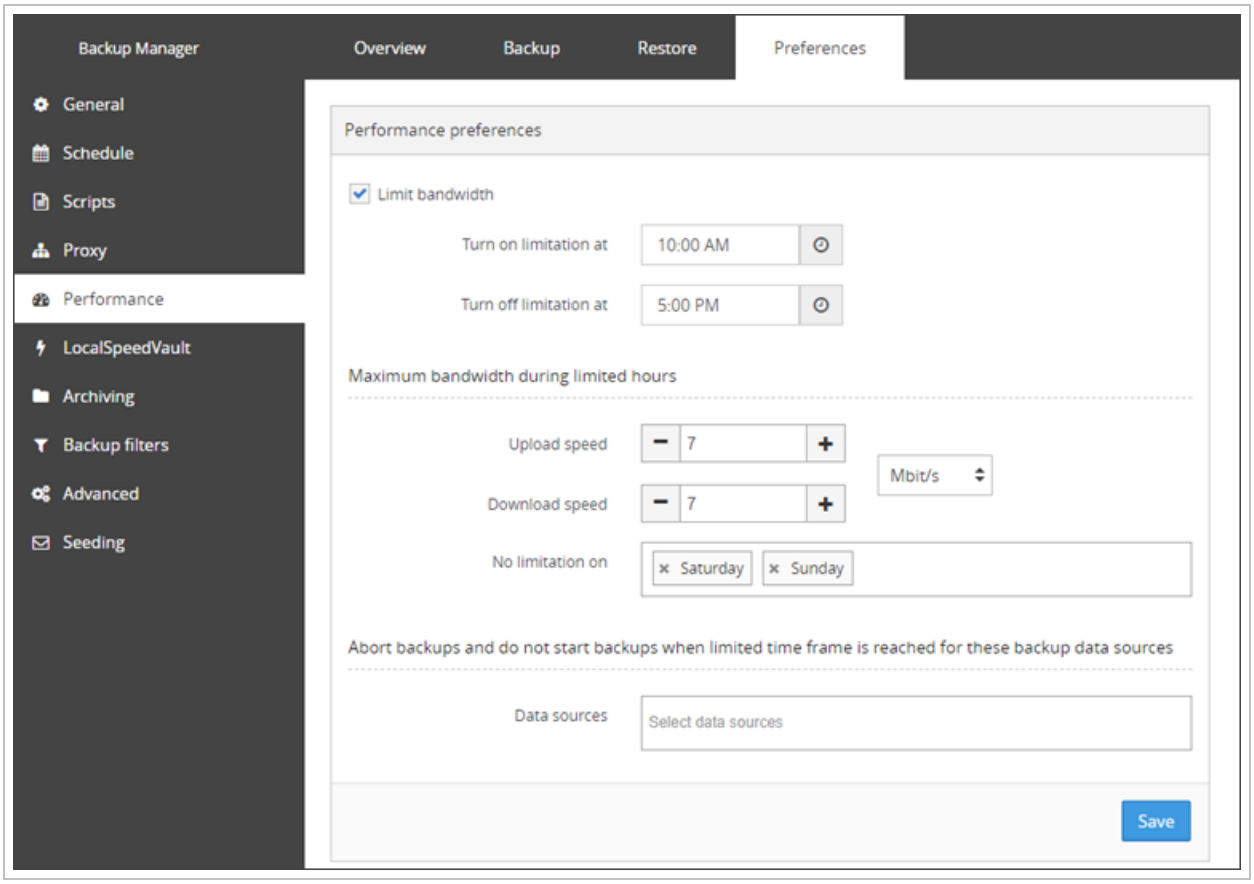
1. Launch the Backup Manager for the device
2. Go to **Preferences > Performance**
3. Select **Limit bandwidth** checkbox
4. Specify times for the limitation to start and end
5. Specify the maximum bandwidth during the specified times

   These can be in Kbit/s or Mbit/s.

6. Add the days in which you *do not* want any limitation
7. Specify any data sources you wish to abort or not start a backup for when the time frame provided above is reached

   This feature is not available if the device is using a profile.

8. **Save** the changes you have made



Save

You must make sure to save any changes you make before moving away from this page.

LocalSpeedVault (a local storage directory in Backup Manager)

By default, the Backup Manager saves your backups remotely in the cloud or at a private data center (depending on your terms of service). You can enable the LocalSpeedVault (a local storage directory) to have an **additional copy** on your own computer or in your local network. Doing this helps speed up the backup process.

Overview

Reasons to enable the LocalSpeedVault

When the LocalSpeedVault is on, scheduled backups **run** secondary to the cloud backup, thus speeding up the backup process. Also restoring data to a local folder becomes faster and does not depend on your Internet connection.

How it works

When a LocalSpeedVault is enabled on a device and a backup runs, the data is sent to both the LocalSpeedVault and the cloud or private storage location. As the LSV is on the local network, this part of the backup completes faster. Once this has completed and synchronized, the LSV begins pushing the backup data to the cloud or private storage as well.

This effectively means that the backup to the cloud or private storage is being sent twice at the same time and so completes faster.

During a restore, data is automatically downloaded from the LocalSpeedVault first to the local device. If the LocalSpeedVault is not available or not synchronized, the restore data will be pulled from the cloud or private storage location. This takes place automatically and cannot be reconfigured.

> If the LocalSpeedVault becomes full, backups will still continue to the cloud, or your private storage nodes.

Feature availability

The feature is supported on Windows, macOS and Linux devices.

What can be used as the LocalSpeedVault

You can create a LocalSpeedVault directory on a local disk, a removable disk or in a local network. All kinds of network resources are suitable: workstations, file servers or network-attached storage (NAS) devices.

Network Shares can be used as a storage location for Linux and macOS devices by mounting them, then browsing to the Network Share location.

Requirements

Size Requirements

Whether you are using a local drive or a network resource, there must be a **sufficient amount** of **free space**.

Your backup data will take up the same amount of disk space as on the remote server, so we recommend that the LocalSpeedVault should be two or three times that of the **used storage**, e.g.:

Initial Backup	Incremental Backup	Total Used Storage	LocalSpeedVault size
200GB data backed up initially	50GB worth of changes backed up incrementally throughout the day	450GB of data stored	1TB - 1.5TB recommended

For Local Drives

If the LocalSpeedVault directory is on a local drive, it must meet the following requirements:

1. It must be **open to the LocalSystem account** (this is the account that the Backup Manager usually performs backups under)

   > Read and write permissions are required

For Network Resources

If the LocalSpeedVault directory is in your local network, it must meet the following requirements:

1. The local network must use the **SMB protocol** for file sharing
2. The network resource must be **accessible** during backups (it must not go into the sleep mode or get disconnected from the network)
3. The network resource must be **open** (available without authorization), which is not recommended due to security reasons, or – preferably – it must have an account that **coincides with the account** on the client machine where the Backup Manager is installed (the same username and password). This can be an Active Directory account
4. If the computers in your local network are united into domains, the network resource must belong to the **same domain** as the client machine (otherwise there may be cross-domain authentication issues on Windows)

The network resource can be integrated with **Active Directory** or **connected to a workgroup**.

Security recommendations for network resources

Recommendations for network resources integrated with Active Directory

If you manage the local network using Active Directory, the accounts from the client machines are suitable for access to the network resource (**pass-through authentication**). You can differentiate access to the network resource with the help of **groups**.

Recommendations for network resources connected to a workgroup

If the network resource is connected to a workgroup, we recommend creating a **separate user account** for backup purposes on each client machine where the Backup Manager is installed. The same account must be created on the network resource (this is necessary for access to the network resource).

- Use a **unique** username and password for each client machine
- Do not use administrative logins/passwords
- Limit access to the defined LocalSpeedVault share for all other users and groups

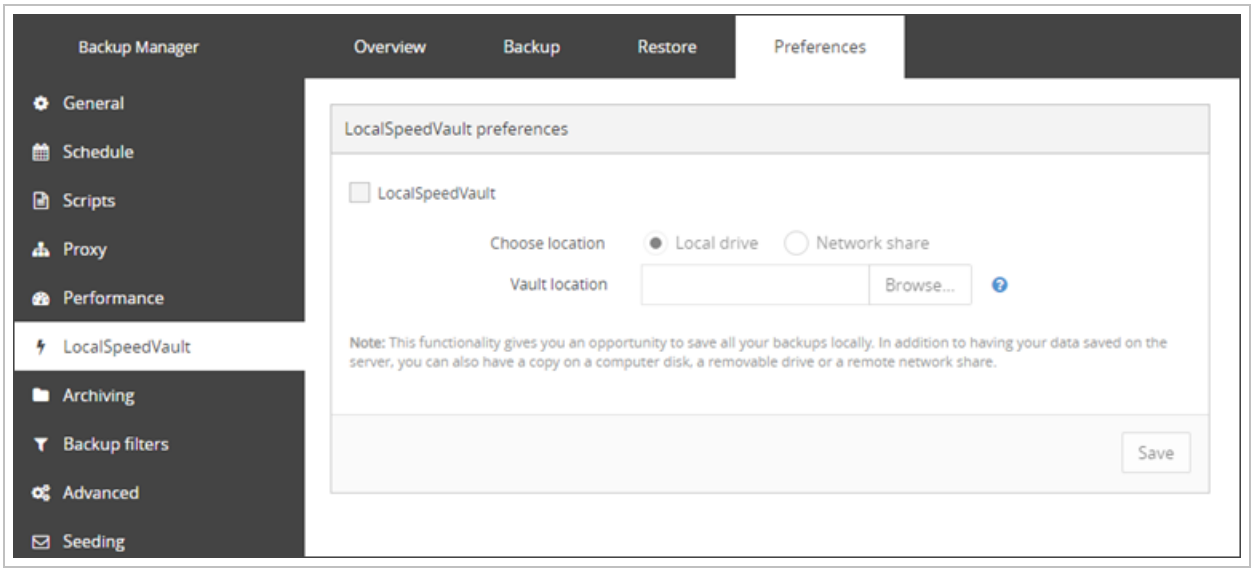
Enabling the LocalSpeedVault

Windows

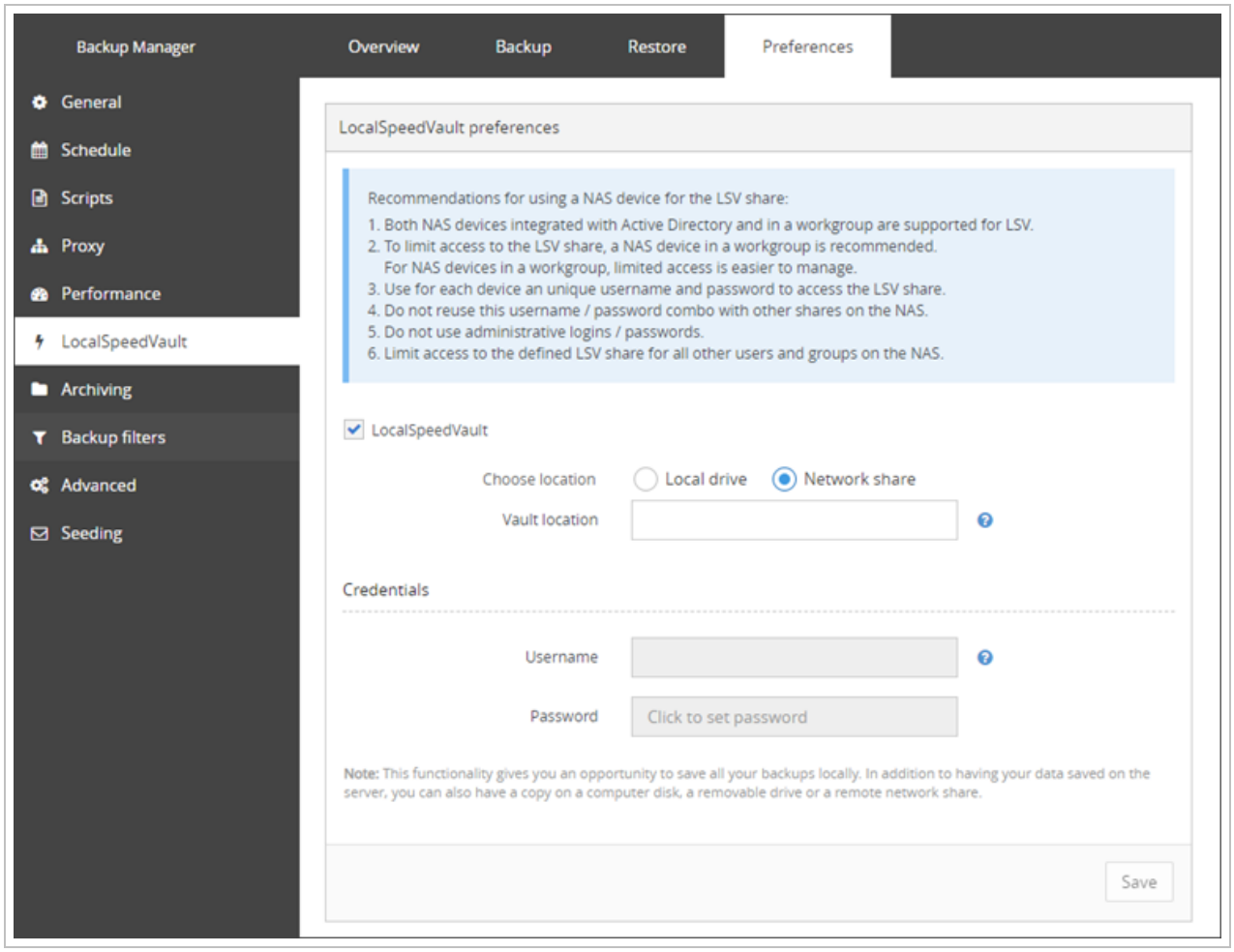
To enable the LocalSpeedVault, do the following:

Go to **Preferences > LocalSpeedVault**

1. Select the **LocalSpeedVault** checkbox
2. Specify the location of the directory allocated for the LocalSpeedVault. This can be an existing or a new directory (the Backup Manager will create it for you automatically if it is not there yet)



3. If the directory is on a network share, enter your access credentials for that network share



4. Save the changes you have made

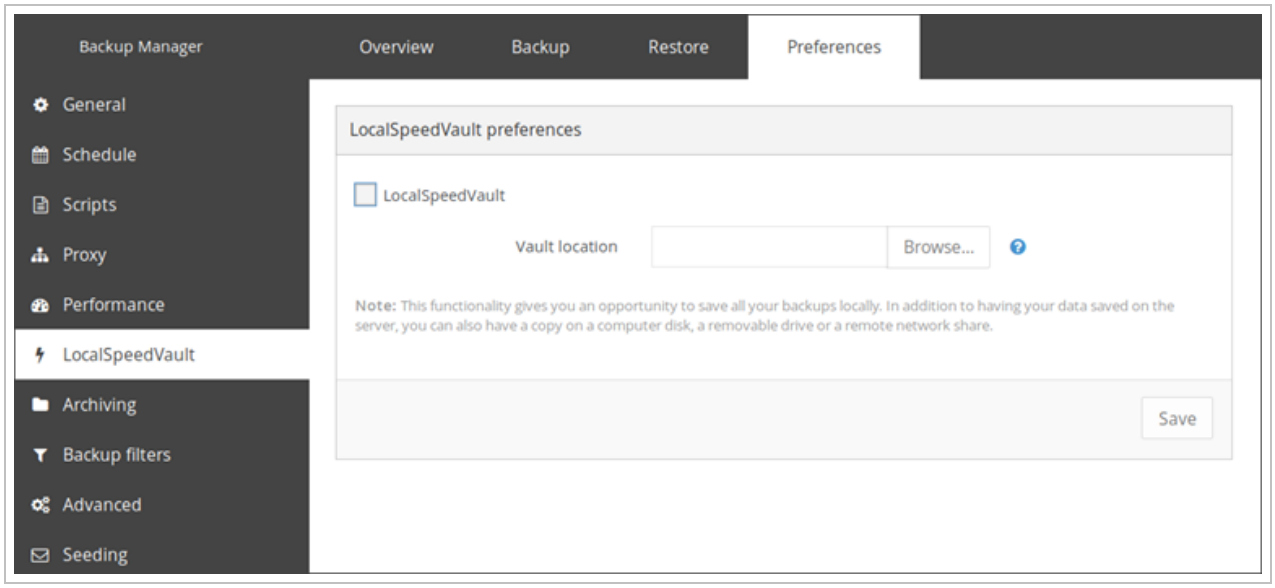
macOS & Linux

To enable the LocalSpeedVault, do the following:

1. Go to **Preferences > LocalSpeedVault**
2. Select the **LocalSpeedVault** checkbox
3. Specify the location of the directory allocated for the LocalSpeedVault

> If the directory is on a network share, you must mount it on the device then select the network share location using the browse option for Vault Location.

4. Save the changes you have made



Monitoring LocalSpeedVault

See the Synchronized page for full details.

Save

You must make sure to save any changes you make before moving away from this page.

Monitoring the LocalSpeedVault

During a backup process, data is sent to the cloud and the LocalSpeedVault. If either of the two storage locations is temporary unavailable, it is updated later when the connection is re-established.

Synchronization statuses

To check whether the local and remote storage locations have all necessary data, open the **Overview** tab in the Backup Manager or go to **Preferences > LocalSpeedVault**.

LocalSpeedVault statuses can also be included in Management Console dashboards by adding the **LSV Status** column.

- Scheduled reports can be generated based on a view that contains the **LSV Status** column (Scheduled Reports in Management Console)

You can also enable **custom notifications** to receive emails regarding LSV status:

- Information on one-time notifications based on a certain LocalSpeedVault status can be found here.

There are three statuses altogether:

- Synchronized
- Synchronizing
- Failed

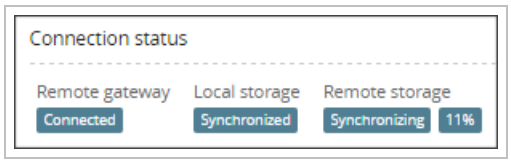
Synchronized

The **Synchronized** status means that both the LocalSpeedVault storage location and the Remote storage location (Cloud storage) have the same backed up data, and so, are both up-to-date.

Synchronizing

The **Synchronizing** status will be followed by a percentage (%), and means that either the LocalSpeedVault storage location or the Remote storage location (Cloud storage) are currently in the process of getting the backed up data from the other storage location.

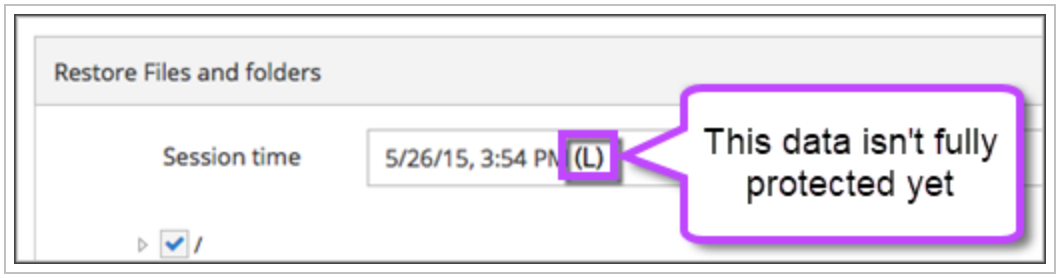
E.g. In the below image, you can see that the Local Storage (LocalSpeedVault) shows as Synchronized, while the Remote Storage is Synchronizing with a percentage of 11%.



This means that your recent backup(s) has been saved locally and is being copied to the remote server at that time. The data is not fully protected until the synchronization is completed for both Local and Remote storage locations.

> While the synchronization is in progress, it is **crucial** to keep the LocalSpeedVault working and to avoid making changes to its settings. Otherwise the sessions that have been backed up to the LocalSpeedVault can be lost.

> You can identify backup sessions which have not been successfully synchronized to the Remote storage location by viewing the Backup Session in the session list. If a session is marked with "L", this means it is available on the Local storage **only**.



Failed

The **Failed** status means that synchronization to one or both of the storage locations has failed and there is a risk of data loss.

Synchronization is automatically **disabled** after the LocalSpeedVault has stayed in the "Failed" state for 14 days (learn more). The Backup Manager invalidates the data that has not fully synchronized with the cloud and tries to back it up again during the next session.

> A notification will appear in the Backup Manager interface and an email alert is sent out in that case.

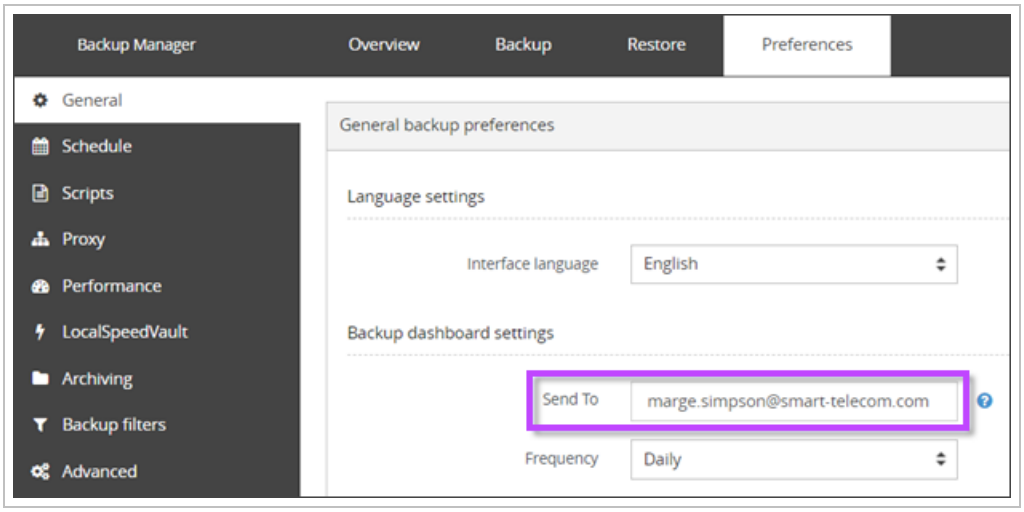
The default 14-day period can be customized for each backup device through the Backup Manager configuration file by adding the following parameter to the `[General]` section:

- `LocalSpeedVaultUnavailabilityTimeoutInDays = NN`
  - Where `NN` is replaced with the number of days

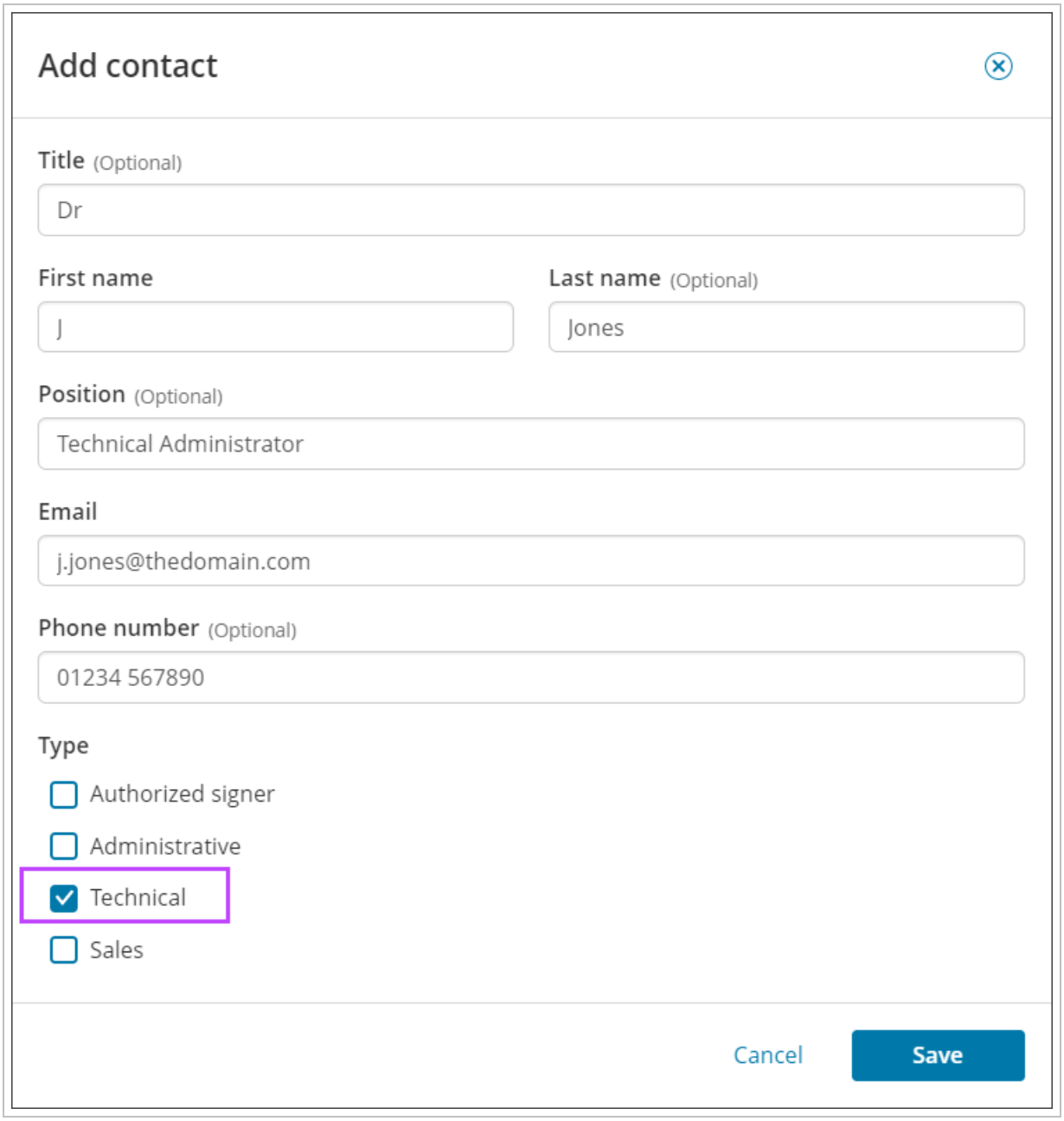
Email alerts on LocalSpeedVault synchronization statuses

Alerts on LocalSpeedVault failures are sent to the following emails:

- The email address specified for backup Dashboards. In the Backup Manager, this can be found under **Preferences > General > Backup Dashboard Settings**



- The technical contact person from the company the device belongs to. You can add such a contact person through the Management Console by navigating to **Management > Customers**, edit the company, open the **Contacts** tab and click **Add Contact**



Synchronizations errors

There are a number of reasons the Synchronization may have issues. Below are some common issues and how to resolve these:

Access is denied

If you have received an **Access Is Denied** error, check the following:

1. Check your local access credentials for the LocalSpeedVault storage location
2. Make sure the Backup Manager client has **read and write** access to the LocalSpeedVault directory
   - If the LocalSpeedVault is on a local drive, check the LocalSystem user account
   - If the LocalSpeedVault is on a shared network resource, check the specified network user account

Path is invalid

If the error received states that the **path is invalid**, check the specified LocalSpeedVault storage path and make sure the LocalSpeedVault directory is correct and available.

It might have been moved or deleted.

Not enough space

If the LocalSpeedVault directory is full and cannot receive any new data, the notification will state **Not Enough Space**.

To fix this you can:

1. Add more space to the directory (if your infrastructure allows it) by following local workstation instructions
2. Copy the previously stored files to another directory with a sufficient amount of space, then update the LocalSpeedVault path in the Backup Manager to the new, larger storage location
3. Disable the LocalSpeedVault and continue with the cloud storage only

   > If you choose this option, make sure the remote storage is synchronized with the LocalSpeedVault **before** disabling it, or you may risk loss of data.

4. Clean up unneeded Archive sessions from the LocalSpeedVault. This can be done in the same way as removing Archiving sessions from the Remote location, following the steps found here

Archiving backup sessions in Backup Manager

As you regularly back up your data using the Backup Manager, a series of backup sessions accumulate in the Cloud (your remote storage location), and on the LocalSpeedVault if this is used. After a certain period, older sessions are cleaned to free up storage space on both the remote and local storage locations. The duration of this retention period is measured in number of days to keep backup sessions for (depending on your Product settings).

If needed, you can keep selected backup sessions in the storage after their retention period expires using the **Archiving** feature. Such sessions will not be deleted (unless you choose to do so manually).

> Using Archiving will *increase* the storage space used.

If data is removed from the backup selection, any future backups will not include this information, but all versions of this data stored in an **Archive** session will not be affected and so will be kept until a clean is done of the archive sessions.

If LocalSpeedVault is used while Archiving is enabled, the used storage of both the Remote storage location (the Cloud) and the Local storage location (LocalSpeedVault) will increase.

Enable Archiving

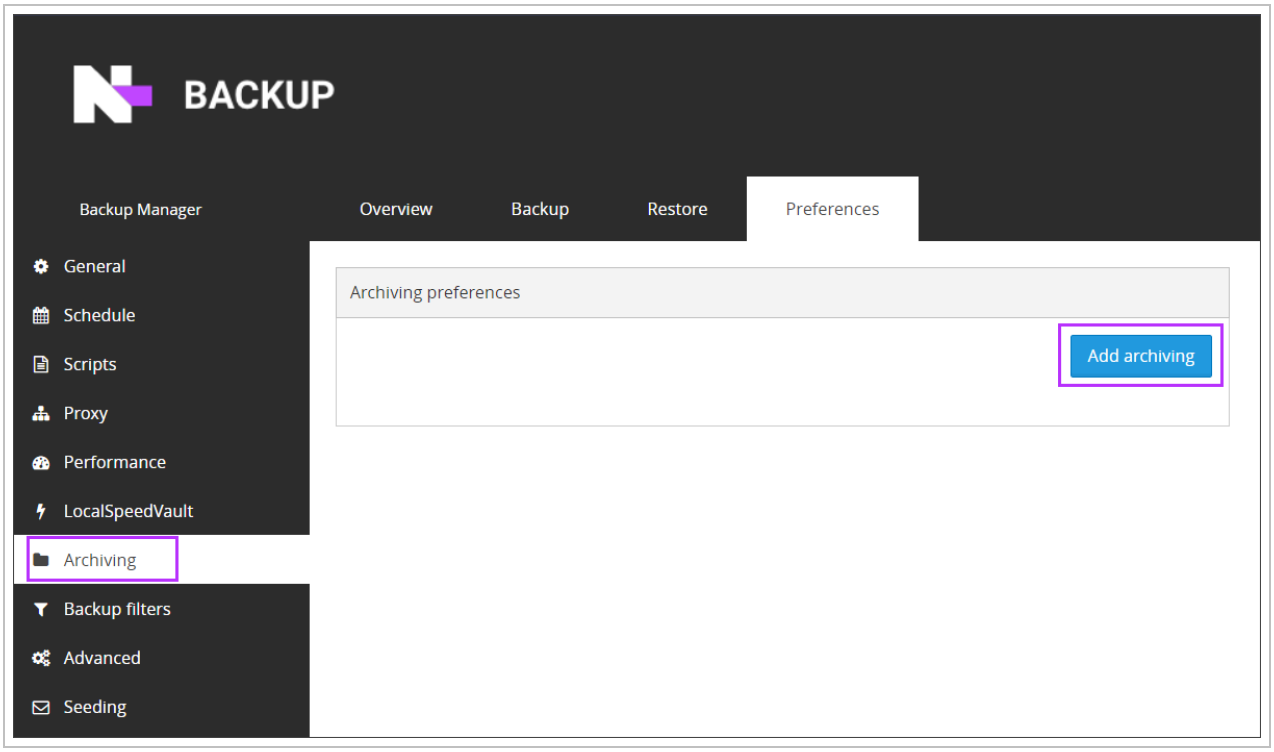
To archive a backup session, you need to enable archiving on the devices Backup Manager client. The task will apply to the next backup session to start after the archive time.

> Previously completed backup sessions cannot be archived.

- The archive task can be an individual or repetitive task
- There can be only one archiving task for each data source per day

  > It is not possible to archive data belonging to the same data source several times a day

1. Open the Backup Manager client for the device you wish to configure archiving on
2. Navigate to the **Preferences**tab
3. Go to **Archiving** on the left hand menu
4. Click **Add Archiving**

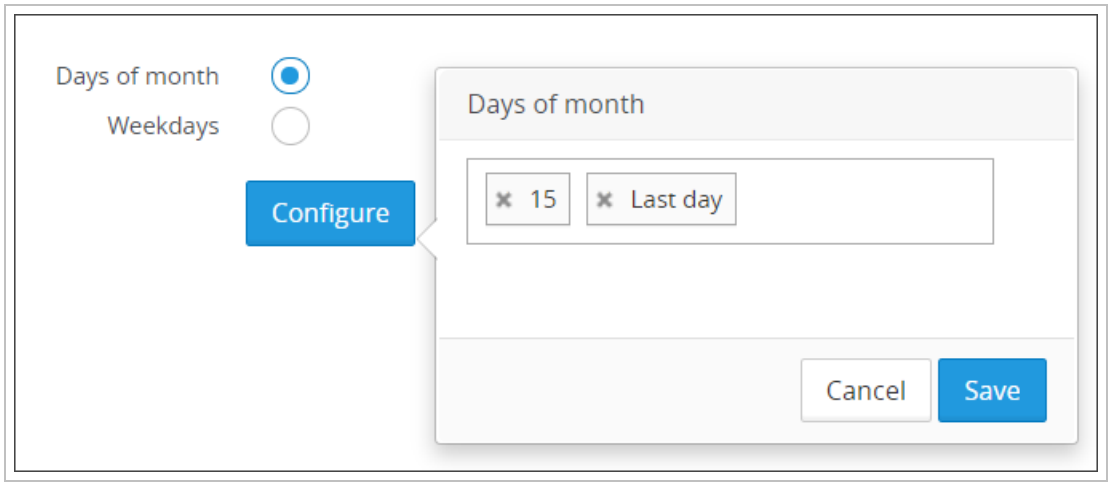


5. Give your archive a name relevant to the frequency of the archive such as "End-of-month archiving" or "Bi-Weekly archiving"
6. Set a time for the archive

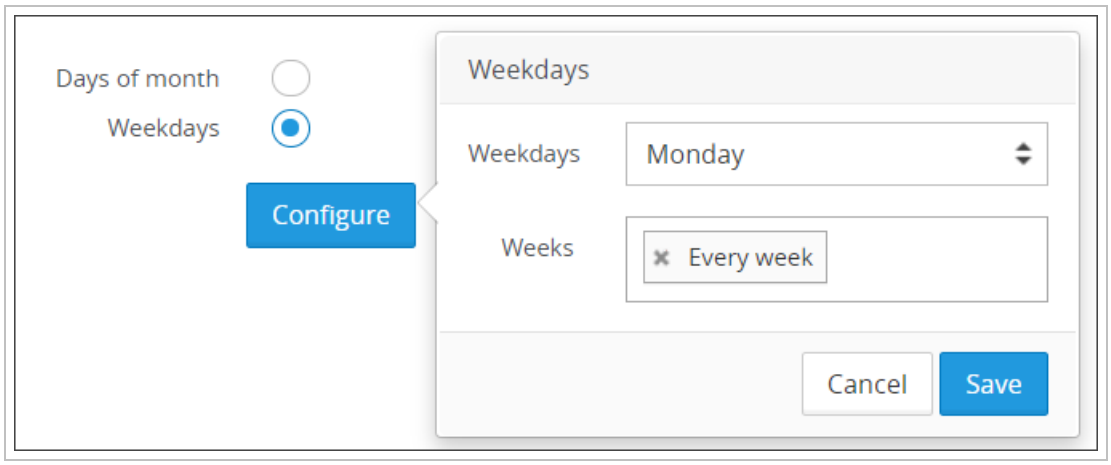
   > This **does not** mean the archive will run at the exact time, but that the archive session will apply to the nearest backup that runs *after* this time.

7. Select the data source(s) to apply the archive to
8. Select the months you wish the archive to be applied to

9. Now select either
   - **Days of month**: This will allow you to set the dates of days in the month you wish the archive to be set, for example the 15th of the month and the last day of the month:



   - **Weekdays**: This will allow you to set the day of the week and which week of the month(s) selected in step #8 you wish the archive to be set, for example every Monday:



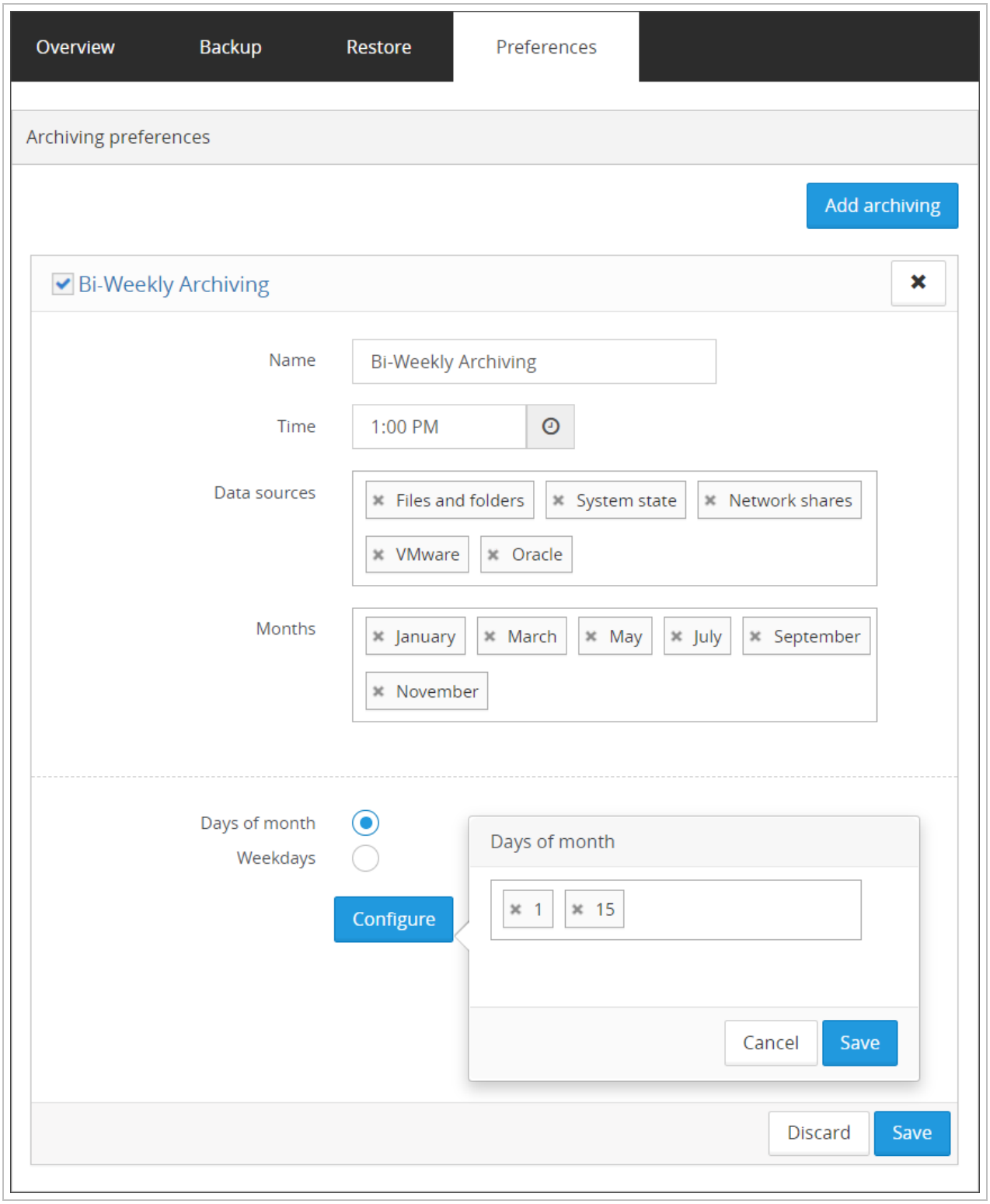
> If you want to run an archive more frequently than the **Weekdays** selection but you do not wish to use the **Days of month** selection (for example you wish it to be set for every Monday, Wednesday and Friday) you must create multiple archives and select each day per Archive.

Edit Archive tasks

You can easily change the task after it has been created.

1. Open the Backup Manager client for the device you wish to edit archiving on
2. Navigate to the **Preferences**tab
3. Go to **Archiving** on the left hand menu

4. Click the Archive task you wish to edit to expand the current settings



5. Make all changes you need

6. Click **Save**

Delete Archive tasks

When an archiving task is not needed anymore, you can delete it.

> This will not make any difference to the backup sessions that have been archived through this task.

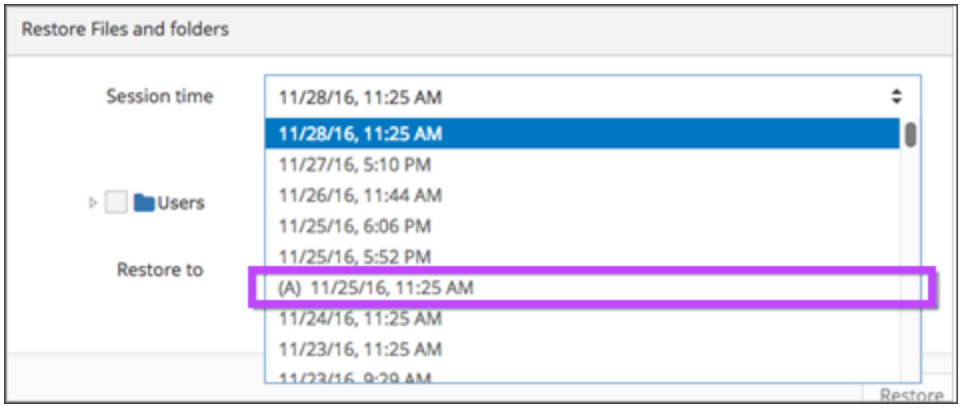
To delete an archive task:

1. Open the Backup Manager client for the device you wish to delete the archive task on
2. Navigate to the **Preferences**tab
3. Go to **Archiving** on the left hand menu
4. Click the Delete button to the right of the Archiving task

5. Confirm deletion by clicking **Yes** on the confirmation box

Recovering backup sessions from Archive

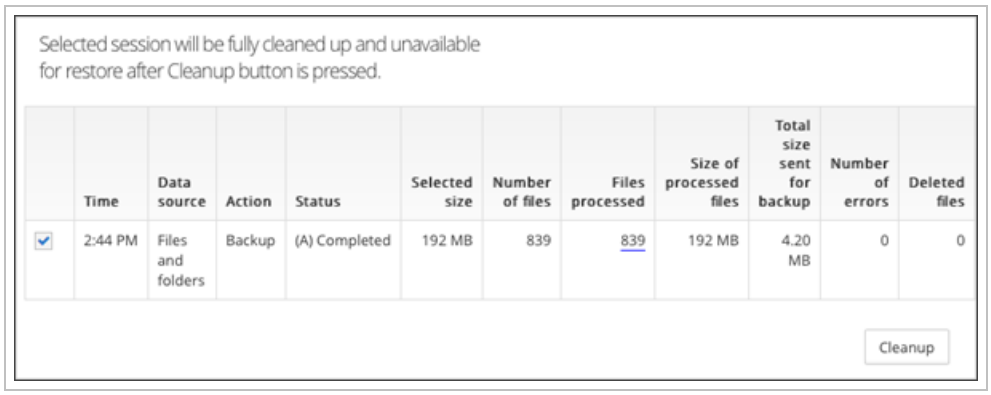
Data from archived sessions is recovered is the same way as from regular backup sessions. You will only notice that archived sessions have a special mark (A) in the **Session time** list which is intended to make it clear that the session is archived.



Clean up unneeded archiving sessions

If you no longer want to keep an archived session in the storage, you can clean it up. The (A) mark gets removed from the session. Then the session is cleared from the storage and is no longer available for recovery.

1. Go to **Preferences > Archiving**
2. Click **Cleanup** (You will see the list of all archived sessions that have passed their retention periods)
3. Select the sessions to clean up
4. Click the **Cleanup** button at the bottom
5. Confirm your intention to clean up the selected sessions



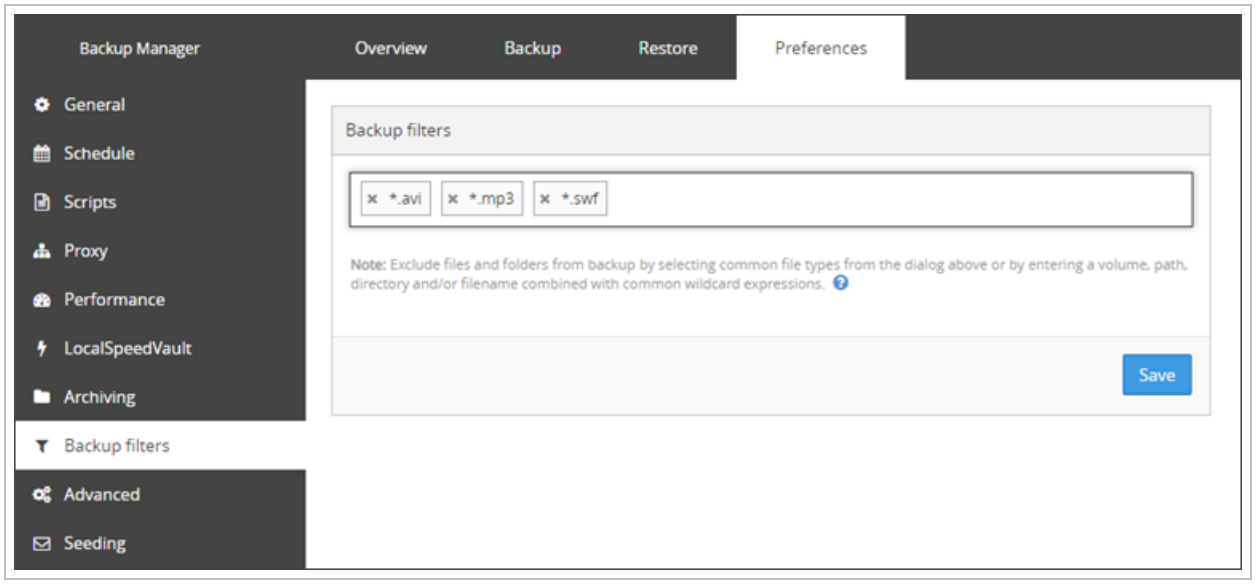
> The action **cannot be undone**. Once a session has been cleaned up, there is no way to get its contents back.

Save

You must make sure to save any changes you make before moving away from this page.

Backup Filters in Backup Manager

You can automatically exclude certain directories or types of files from backup. This is done using exclusion filters on the devices Backup Manager, by going to **Preferences > Backup filters**.



Predefined filters

Some files are automatically **excluded from backup** on Windows devices **only**, except when using certain security features of Products.

> These predefined filters only work on Windows devices by the use of a standard 'files not to backup' entry in the **Windows Registry**, meaning there is no alternative for Linux or macOS devices.

What files are automatically excluded from backup:

1. All files indicated in the registry subkey:

   ```
   HKEY_LOCAL_
   MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup
   ```

   Typical examples:

   - `\Pagefile.sys`
   - `\hiberfil.sys`
   - `%TEMP%\* /s`

2. All files from the Backup Manager installation folder

3. Temporary files of no importance:
   - ```
     C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer\IconCacheToDelete
     ```

     > There is such a file for every user account registered in the system
   - ```
     C:\Users\<username>\AppData\Local\Microsoft\Internet Explorer\DomainSuggestions
     ```

     > There is such a file for every user account registered in the system
   - ```
     C:\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit
     ```
   - Files from the **Print Spooler** folder
4. Files/folders matching the following masks:
   - `*\Local Settings\Temporary Internet Files\*`
   - `?:\RECYCLER`
   - `?:\System Volume Information`
   - `%systemdrive%\$WINDOWS.~??` (for example `C:\$WINDOWS.~BT` or `C:\$WINDOWS.~WS`
   - `%SYSTEM_ROOT%/Windows/*.config.cch`
   - `?:\swapfile.sys`
   - `?:\pagefile.sys`
   - `?:\hiberfil.sys`
   - `*\AppData\Local\Temp\*` (on Windows Vista and Windows 7)
   - `*\Local Settings\Temp\*` (on Windows XP)

File Type Examples

Filters based on file type are the same across all Operating Systems.

Here are some example filters you can add:

- **a*** - excludes all files starting with the letter "a"
- ***.mp3** - excludes all files with the .mp3 extension
- `C:\Data\*.*` - excludes all files in the `C:\Data\..` path and underlying folders
- `C:\Data\*.mp3` - excludes all files in the `C:\Data\..` path, with the .mp3 extension
- `C:\Data\*.m??` - excludes all files in the `C:\Data\..` path, with a three-character extension starting with .m and ending with any two other characters, such as .mob, .mp3, .mov or .mpg
     ```

> The filters are applied to **upcoming backup sessions**. Older backups stay as they are.

Suggested Additional Filters

We would strongly advise to add the following additional exclusions to your filters:

Windows temp locations

- `*\Microsoft\Windows Defender\Scans\mpcache*`
- `*\AppData\Local\Microsoft\Outlook\*.ost`

Chrome/Edge/Firefox browser cache and update files

- `*\Chrome\User Data\*\Cache\*`
- `*\Local\Microsoft\Edge\User Data\Default\Cache\*`
- `*\Local\Mozilla\Firefox\Profiles\*\cache\*`

N-central cache directories

- `*\PME\archives\*`
- `*\NablePatchCache\*`
- `*\SolarWinds.MSP.CacheService\cache\*`
- `*\N-able Technologies\UpdateServerCache\*`

AV Defender cache files

- `*\ThreatScanner\Antivirus*\Plugins\cache.*`

EDR/SentinelOne

- `*\ProgramData\Sentinel\data\*`

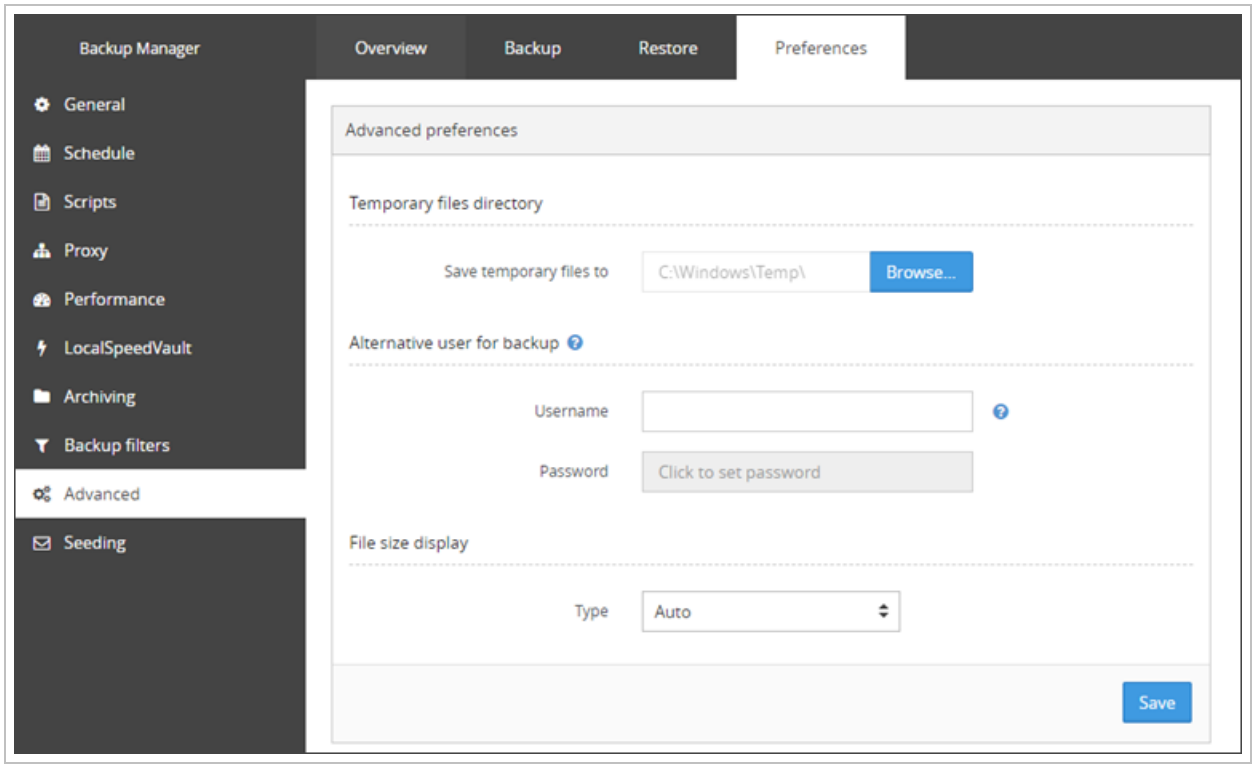
Save

You must make sure to save any changes you make before moving away from this page.

Advanced

In the Advanced tab of the Preferences section on Backup Manager, there is functionality to change the directory of temporary files, configure an alternative user for backup and the format in which the file size will be displayed.

> It is recommended to restart the Backup Service Controller after any changes are made in the Advanced tab so that the changes may take effect.



Temporary files Directory

Here is how to change the location of temporary files for Backup Manager.

1. Click **Preferences > Advanced**
2. Click **Browse** next to the 'Save temporary files to' text box
3. Navigate through the file tree to select the new location of the temporary files
4. Click **Save**

Alternative user for backup (only available for Windows devices)

This setting allows you to specify an alternative set of user account credentials which will be used to allow Backup Manager permission to backup any files or data sources which are restricted on the device.

1. Click **Preferences > Advanced**
2. Specify the credentials of the alternative account to be used

   > The username can be added as either domain\username or username

3. Click **Save**

File size display

1. Click **Preferences > Advanced**
2. Using the **Type** dropdown, select the format you would like to view the file size in

> The choices for type are **Auto**, **KB**, **MB** or **GB**

3. Click **Save**

Save

You must make sure to save any changes you make before moving away from this page.

Seed backup in Backup Manager

Backing up a large volume of new data can take time if a user's Internet connection is slow. For such cases Backup Manager users have the option to use our seeding function. It works both for initial and subsequent backups.

> Seed backup is a **self-service** operation. End users can perform it all by themselves without the involvement of their service provider.

Once the below requirements have been met, see the following instructions on using the Seed Backup feature:

- Step 1. Set seeding path
  - Step 1. Set seeding path
  - Step 2. Enable seeding
  - Step 3. Transfer seeding folder to storage

Terms

- **Seed backup**
  1. Any backup session performed while a device is in the **seeding mode**
  2. The process of uploading backup data to the cloud in bulk. Seed backups are performed to a **temporary storage medium** and then transferred to the cloud from a different machine with a high-speed Internet connection (see the scheme below). Also called *seeding*

- **Seeding path** - a path to a folder on a temporary storage medium (required by the Backup Manager). This is where a seeding folder is created
- **Seeding folder** - a directory that is created automatically for seed backup purposes. It contains backup files in a compressed and encrypted format, ready for cloud storage. The folder is titled using the name of the backup device it belongs to
- **Seeding mode** - the mode that starts as soon as seeding is enabled and ends when a user clicks **Complete seeding**. In the seeding mode, all backups are performed to the seeding folder (rather than directly to the cloud)
- **Post-seeding mode** - the mode that starts when a user clicks **Complete seeding** and ends shortly after seed data is uploaded to the cloud. While in the post-seeding mode, regular cloud backups are available but it is not possible to restore data that has been backed up since the seeding mode started

Options available in the seeding mode:

Option	What it does	Available	Location
Run seeding	Starts a seed backup session (can be used multiple times)	In the seeding mode	"Backup" tab
Disable seeding	Disables the seeding mode (subsequent backups will be performed to the cloud)	In the seeding mode **until the first backup** is performed	Notification ribbon (all tabs)
Complete seeding	Sets to Backup Manager to the post-seeding mode	In the seeding mode **after the first backup** is performed	Notification ribbon (all tabs)

Requirements

Source machine requirements

The source machine on which the seed folder is created can function on Windows, macOS or Linux (view list of supported versions).

This is the machine whose data needs to be backed up.

Temporary storage medium requirements

Seeding can be performed to any of the following storage media:

- A removable storage device (a USB drive or hard disk)
- A network share or network-attached storage device (NAS)

> The user being used for the backup on the device **must** have **both** read and write access to the Network Share. If not, the backup will fail with an **Access denied** error

The **removable storage device** must operate on a standard file system. A non-standard file system such as HFS can make seeding data unreadable (you will get a warning if this is the case). The following file systems are recommended for removable drives:

- **Windows** - exFAT, NTFS
- **macOS** - exFAT
- **Linux** - exFAT, NTFS

Host machine requirements

The host machine from which you transfer the seeding data to the cloud must run on **Windows**.

It is possible to upload multiple devices' seed backups at the same time if the host machine's disk and internet can handle the increased load.

Optional Preparatory setup

If you plan to use the LocalSpeedVault with the device, consider enabling the feature **prior to starting your initial seed**. This will help prevent data seeded to the cloud from later having to be downloaded and synchronized to the LocalSpeedVault.

> ✖ Care must be taken when transferring the seeding folder to the cloud (see step 3 of the instructions). Some users specify a path to the LocalSpeedVault directory instead, which results in errors.

If in doubt, you can differentiate the LocalSpeedVault from the seeding directory by its name. Both of them are titled using the device name, but the LocalSpeedVault directory also has an ID attached. To avoid confusion, configure unique paths such as these:

- `x:\localspeedvault\` and `y:\seed\` (local)
- `\\server\backup\speedvault` and `\\server\backup\seed\` (network)

Troubleshooting

If missing or corrupt data is identified on the seed drive, you may receive an error message offering you to invalidate the missing data. This is done by adding the `-invalidate-missing-data` parameter to the `seeds.upload` command.

```
C:\Users\Administrator\Downloads\mxb-st-windows-x64>ServerTool.exe seeds.upload -
path F:\Seed\sony-vaio-hdqtrs -threadscount 3 -invalidate-missing-data
```

> Missing data invalidation is a **destructive operation** and should only be done if you understand why the data is missing and the risks that can occur. Consulting technical support is recommended.

> If a seed upload or download is interrupted and restarted, the seed will pick up where it left off after a scan is ran of the data.

Supported features

Operating systems for backup and recovery

You can back up and restore data located on Windows OS, macOS and GNU/Linux. Please see the table below for the full list of supported operating systems:

Windows versions	macOS versions	GNU / Linux versions
▪ Windows 8 / 8.1 ▪ Windows 10 ▪ Windows 11 ▪ Windows Server 2012 / 2012 R2 (limited[1])	▪ 10.15 Catalina ▪ 11 Big Sur ▪ 12 Monterey ▪ 13 Ventura	▪ CentOS 5, 6, 7 ▪ Debian 5, 6, 7, 8 ▪ OpenSUSE 11, 12

[1]New features such as Docker-based containers, Storage Spaces Direct and Shielded VMs are not.

Windows versions	macOS versions	GNU / Linux versions
▪ Windows Server 2016 (limited[1]) ▪ Windows Server 2019 (limited[2]) ▪ Windows Server 2022 (limited[3])	▪ 14 Sonoma	

Parallels are not officially supported for Backup Manager when backing up macOS with Windows parallels. If you wish to use Backup Manager in this situation, there may be abnormalities so please test the backup by doing a restore as soon as possible. Two backup accounts may be necessary to backup both the macOS Files and Folders and the Windows Files and Folders.

Backup on devices using Operating Systems which are not officially supported may still work, but as we no longer test these versions, we cannot guarantee full functionality. In situations where the device cannot be upgraded to a supported OS, you may encounter issues with new features, or there may be abnormalities so please test the backup by doing a restore as soon as possible.

Note for Windows:

On Windows devices, Backup Manager supports 32 or 64-bit architecture.

Note for macOS:

Pre 10.14 Mojave: as of version 21.10 of Backup Manager, macOS versions prior to 10.14 are no longer officially supported.

10.14 Mojave and later releases: Ensure you enable macOS Full Disk Access for the Backup Manager *before* running backups.

Note for GNU/Linux:

In addition to the major Linux distributions that are regularly tested in-house, it is possible to run the Backup Manager practically on any GNU/Linux distribution that meets the following requirements:

- Architecture: **x86** or **x86_64/amd64**
- Kernel: **2.6.9+** with NPTL
- glibc: **2.4** or greater (all data sources except for MySQL); **2.5** or greater for the backup and recovery of MySQL
- LVM for the backup and recovery of the system state

Data sources for backup and recovery

The Backup Manager handles **individual files and directories** as well as **complex systems** such as these:

- MS SQL
- VMware

---

[1]Only the features compatible with Windows Server 2012 R2 are supported.
[2]Only the features compatible with Windows Server 2012 R2 are supported.
[3]Only the features compatible with Windows Server 2012 R2 are supported.

- Hyper-V
- MS Exchange
- MS SharePoint
- Oracle
- MySQL

You can also back up and recover the configuration of your **operating system** (the "System State" data source) and Microsoft 365 protection.

Please view Data sources for system compatibility details.

Backup-related features

"Yes" next to the name of an operating system means that the feature is available on **all supported versions** of that operating system.

Feature	Windows	macOS	GNU/Linux
One-time backups (initiated manually)	Yes	Yes	Yes
Scheduled backups	Yes	Yes	Yes
Flexible backup selection (manual file selection, exclusion filters, priority files)	Yes	Yes	Yes
Automatic file selection (adding certain types of files to the backup selection automatically)	Yes	No	No
Seed loading backups (for large data sets)	Yes	Yes	Yes
Pre- and post-backup scripts (for example, shut down the system after backup)	Yes	Yes	Yes
LocalSpeedVault (a backup copy on a local drive or a network share for faster backups and restores)	Yes	Yes	Yes
Archiving (archived backup sessions will never be deleted from the Cloud)	Yes	Yes	Yes
Detailed reports on the statuses of backup sessions (displayed on the **Overview** tab)	Yes	Yes	Yes
Backup of open files (especially files belonging to MS SQL, MS Exchange, MS Hyper-V and MS SharePoint)	Windows 7 and later	No	No
Backup of encrypted files	Yes[1]	Yes	Yes
Backup of archived files (all common types of archives are supported)	Yes	Yes	Yes

[1]In versions 15.8 and earlier, encrypted files must be backed up under the same user account that was used for their creation. To configure access to that account, go to "Preferences > Advanced > Alternative user for backup".

Feature	Windows	macOS	GNU/Linux
Backup of data located on local disks, removable storage drives mounted as fixed drives (Windows and Linux) and local network resources	Yes	Yes	Yes
Backup Accelerator (speedy subsequent backups of large files)	Yes	No	No

Recovery-related features

"Yes" next to the name of an operating system means that the feature is available on **all the supported versions** of that operating system.

Feature	Windows	macOS	GNU/Linux
One-time restores (initiated manually)	Yes	Yes	Yes
Continuous restores (synchronous with backups)	Yes	Yes	Yes
Flexible data selection	Yes	Yes	Yes
Choice of target location (the ability to recover data to the original location or a new one)	Yes	Yes	Yes
Detailed reports on the statuses of restore sessions (displayed on the **Overview** tab)	Yes	Yes	Yes
Bare metal recovery (recovering a failed system directly to bare hardware without a prior OS installation)	Windows 7 and later	No	No
Virtual disaster recovery (recovering a failed system to a virtual machine)	Windows 7 and later	No	No

All the recovery-related features except for the bare metal recovery are available in the Recovery Console (a multi-instance recovery tool for system administrators).

Common features

The rest of the features are available on **all** the supported operating systems.

- **Multi-lingual support** -
  The Backup Manager can be used in any of these 9 languages:
  - English
  - Dutch
  - Russian
  - German
  - Spanish
  - French
  - Portuguese

    - Norwegian
    - Italian

- **Interface selection** - You can operate the Backup Manager through the command line or use the graphic user interface
- **Custom branding** - You can brand the Backup Manager for your end users removing references to the developer (this is done through the Backup & Disaster Recovery Console). Use a custom name, logo, color scheme, and icons
- **Remote management** - You can install the Backup Manager remotely through the Backup & Disaster Recovery Console and send remote commands to the Backup Manager devices of your end users
- **Proxy connection** - The Backup Manager can work from behind a proxy server
- **Email reports** - Enable the delivery of email notifications on the statuses or recent backup and recovery sessions. This can be done by an end user in the Backup Manager or remotely by a service provider or a system administrator
- **Bandwidth usage control** - Be sure your bandwidth usage will never exceed a specified limit
- **Updates** - You can update the Backup Manager to the latest version by downloading the latest version and installing it on top of the current one or by letting the app update itself automatically. For full details see Update Backup Manager

  > Linux devices on versions pre-16.11 do not auto-update

Data processing technologies

Backup data is processed locally on the client side and then sent to remote storage. Data processing is not platform-dependent so all users can benefit from advanced data processing technologies such as deep deduplication, delta slicing, directory hashing, compression, secure encryption, caching and so on.

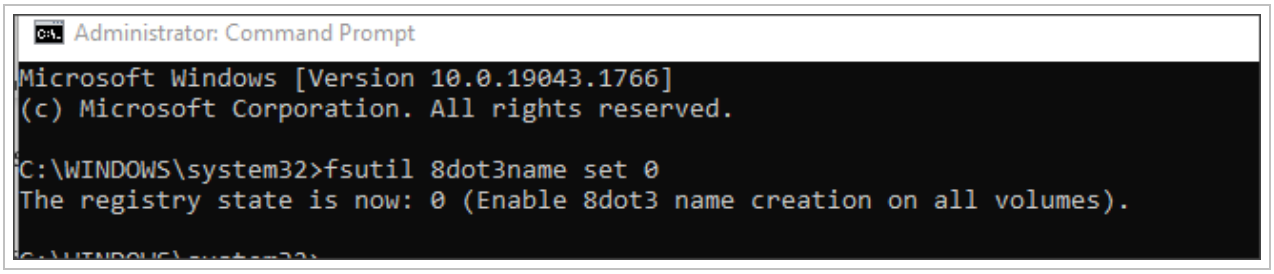
8dot3

Cove Data Protection (Cove) supports the use if 8dot3 names.

The host PC (Recovery Console, VDR) must be configured with **"Enable 8dot3 name creation on all volumes on the system"**. This can be done by:

1. Log on to the device as an account with Administrator permissions
2. Open command line as an Administrator
3. Run the command:

```
fsutil 8dot3name set 0
```



Data sources

Practically any file located on a workstation or server can be protected against loss using the Backup Manager. Some files are not subject to backup – for example files from the Backup Manager installation folder and temporary files on Windows.

Complex systems such as databases, virtual machines and content management systems require specific approaches to keep backup data consistent (this guarantees that the system will continue working after recovery). That is why you will find different data sources in the Backup Manager (a separate data source for each type of data).

Data source	Description	Available on Windows	Available on macOS	Available on Linux
Files and folders	Individual files and directories located on the computer that the Backup Manager is installed on	Yes	Yes	Yes
System state	The operating system with its configuration	Yes	No	No
MS SQL	Databases powered by Microsoft SQL Server: ▪ 2008 ▪ 2008 R2 ▪ 2012 ▪ 2014 ▪ 2016 (mainstream editions) ▪ 2017 ▪ 2019 ▪ 2022	Yes	No	No
VMware	Virtual machines running on VMware ESXi ▪ 6.0 ▪ 6.5 ▪ 7.0 ▪ 8.0	Windows 7 and later (**64-bit** versions)	No	No
Hyper-V	Virtual machines running on MS Hyper-V ▪ 2.0 ▪ 3.0	Windows 7 and later (**64-bit** versions)	No	No
MS Exchange	Messaging systems powered by Microsoft Exchange Server ▪ 2010 ▪ 2013	Yes	No	No

Data source	Description	Available on Windows	Available on macOS	Available on Linux
	▪ 2016 (limitation[1]) ▪ 2019			
MS SharePoint	Content management systems powered by Microsoft SharePoint: ▪ 2007 ▪ 2010 ▪ 2013 ▪ 2016 (single-server installations)	Windows Server. At the moment MS SharePoint 2016 can be backed up only on Windows Server 2012 R2.	No	No
Oracle	Databases powered by Oracle Database Standard Edition 11g	Yes	No	Yes (remotely from Windows[2])
MySQL	Databases powered by MySQL Server versions: ▪ 5.0.22 ▪ 5.1 ▪ 5.5 ▪ 5.6 ▪ 5.7 ▪ 8 and all its minor releases	Yes (glibc 2.5 or higher required)	Databases powered by MySQL Server: ▪ 5.0.22 ▪ 5.1 ▪ 5.5	8.0.22 and earlier have no restrictions. 8.0.23 and higher only for Linux x64 with glibc version 2.17 or higher
Network shares	Individual files and directories located on a local network resource	Yes	Yes (pre-backup setup required[3])	Yes (pre-backup setup required[4])

Starting from the 18.6 release, a new data source has been available - **Microsoft 365**. It works as a service and does not involve the Backup Manager installation. Learn more.

---

[1]Exchange Database Availability Groups (DAGs) and replica databases are not supported

[2]You can back up Oracle databases on Linux remotely from Windows devices located in the local network. For that purpose, you need to create a folder for RMAN backup and make the folder available as a shared network resource that does not require authorization. If the shared folder requires authorization, it must be mapped as a network drive to the Windows machine.

[3]To back up network shares on macOS, you need to permanently connect the network resource to your desktop (it will be recognized as the Files and Folders data source after that).

[4]To back up network shares on Linux, you need to permanently connect the network resource to your desktop (it will be recognized as the Files and Folders data source after that).

Ensure you use the appropriate data source for the data you need to backup. For example, do not use the **Files and folders** data source to backup **MS SQL** databases.

Files and folders

Use the Files and folders data source to protect against loss any **individual files and directories** on your hard drive.

This data source does not have any particular requirements or settings of its own. Please follow general instructions for backup and recovery.

Virtual Disaster Recovery and Bare Metal Recovery

Be aware that in order to successfully restore using the Virtual Disaster Recovery or Bare Metal Recovery methods, you must back up the full Files and Folders data source (the whole system disk `C:\` or any other depending on the configuration of your computer)

Limitations

Files and Folders contained within USB drives or sticks cannot be backed up. Drives marked as removable media by the operating system are not detected for backup.

The software will only detect USB drives that are mounted as fixed drives.

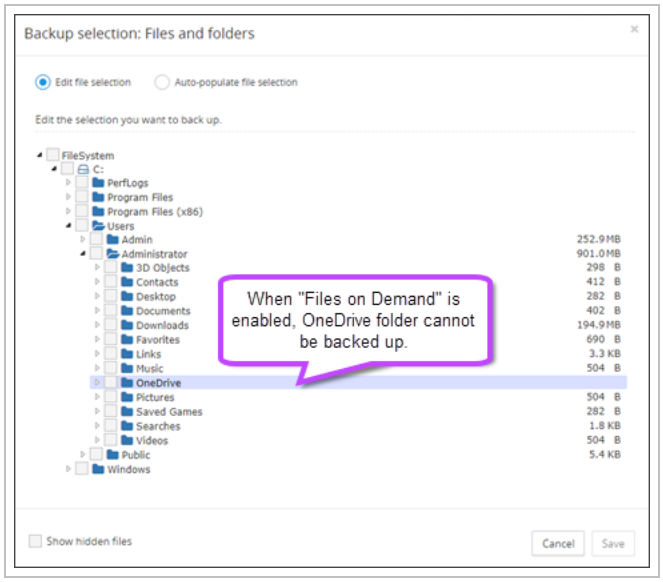
The software will not follow iSCSI targets mounted to an empty NTFS folder. Only iSCSI volumes mounted with a drive letter are available for backup

OneDrive backup and recovery

Under **Files and folders**, you can set up backup and recovery service for a local **OneDrive** directory.

Requirement for Windows 10

On Windows 10, you must **disable** the **Files On-Demand** feature in OneDrive in order to backup all OneDrive files. When the feature is on, the contents of the directory are not physically available on the hard drive. This makes them inaccessible for backup and will mean they are skipped during backup and an error is no longer given to advise of an issue accessing these files.



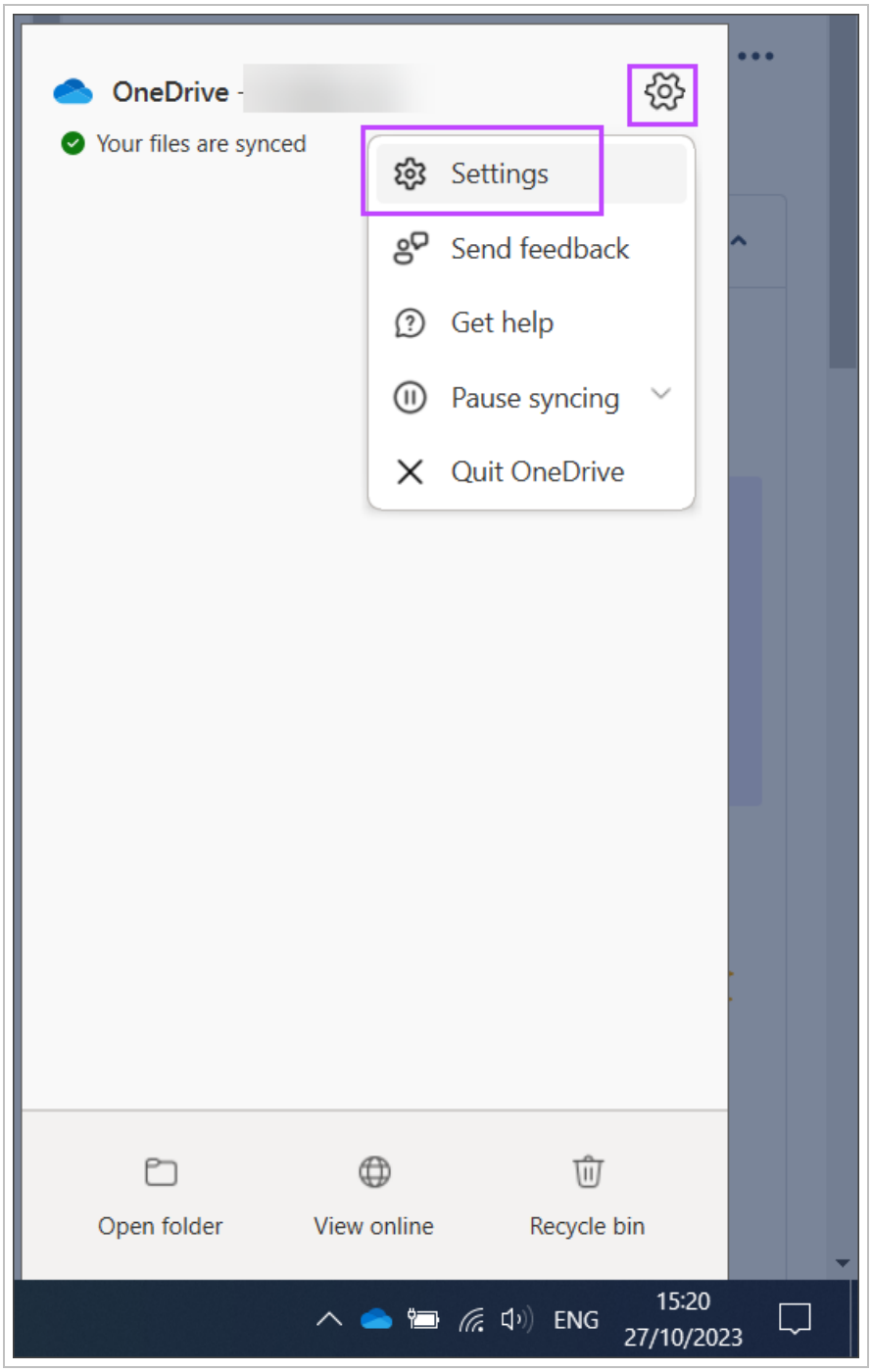
More about "Files On-Demand"

In the October 2017 build for Windows 10, Microsoft introduced the **Files On-Demand** setting, where the files are no longer physically available on the local computer, but stored in a cloud at Microsoft, and are only downloaded on request. Although this feature saves space for the users themselves, the backup process might be disturbed.

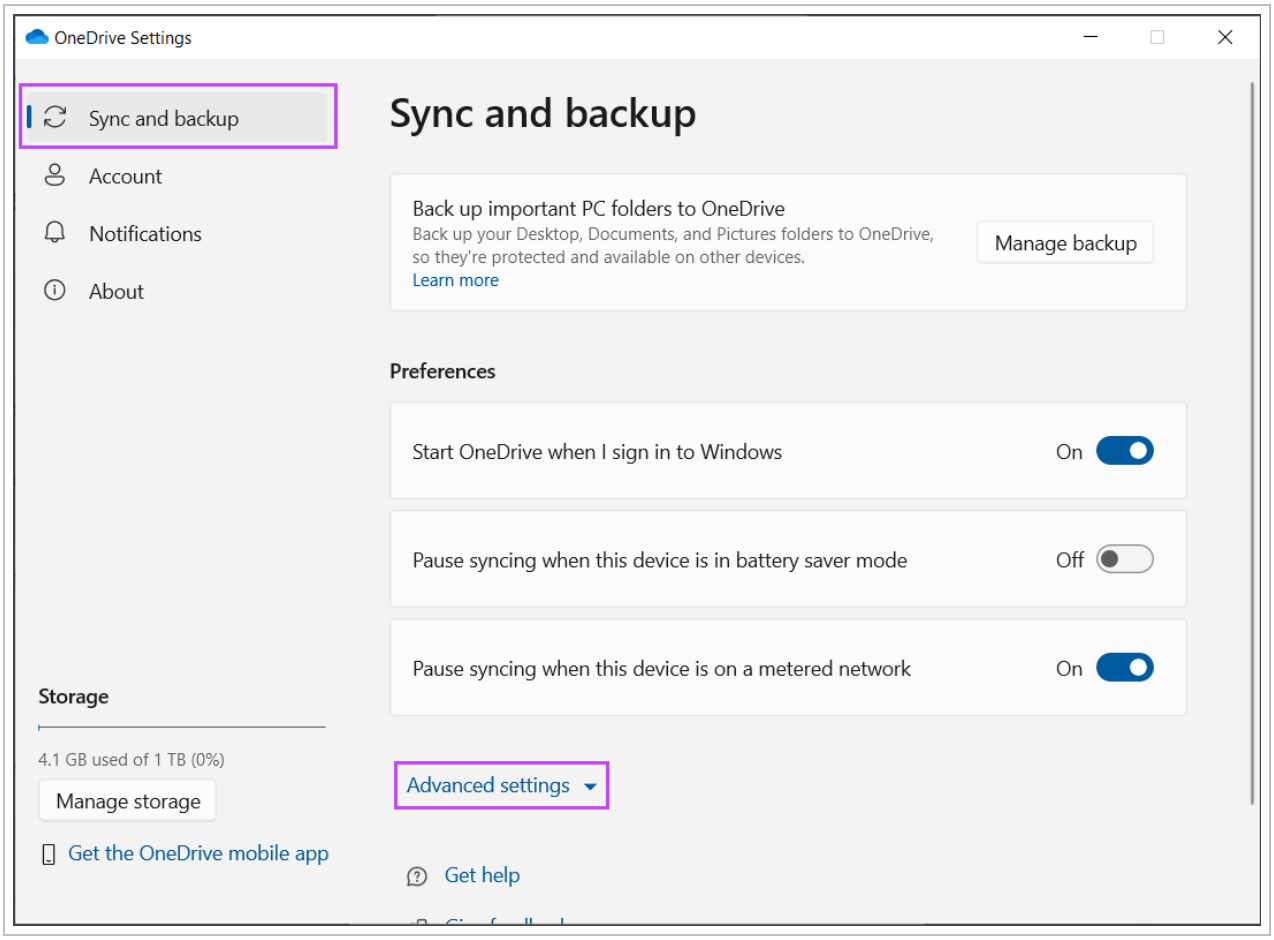
When the feature is activated (which is not done by default after the upgrade to the latest build of Windows 10), the files are uploaded to the cloud and their local versions replaced by symlinks. We cannot backup these symlinks as a replacement of the original file.

Here is how to make sure the **Files On-Demand** setting is disabled in your system.

1. Right-click the OneDrive icon in the notification area or in the File Explorer
2. Click **Settings**, and then open the **Settings** tab



3. In the **Sync and backup** tab, expand the **Advanced Settings** section



4. Scroll down to **Files On-Demand** and ensure this is disabled so your settings look
5. Click to agree that the files will be downloaded back to your computer

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

System state

The System state data source in Backup Manager lets you back up the configuration of your operating system and critical system components such as the Registry, boot files, SYSVOL directory and Active Directory. In case of a failure you can switch to a different computer faster without the need to reconfigure your operating system.

When backing up System State, this includes the following aspects of the system:

- Registry
- Boot files
- System files
- Disk partition information

- Active directory
- MS Search information
- Performance monitor information
- Task scheduler information
- VSS components
- WMI components

System state does not back up user data or program files. To ensure that a full recovery of the system is possible, please select the operating system partition in the Files and Folders datasource as well. This is usually the C:\ drive, but may be another drive letter depending on how the device is configured.

Virtual Disaster Recovery and Bare Metal Recovery

> Be aware that in order to successfully restore using the Virtual Disaster Recovery or Bare Metal Recovery methods, you must back up the full System State data source

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

What's inside:

System state backup requirements

System configuration

You can back up and recover a system containing **dynamic disks**. If a dynamic disk uses the **MBR** partition table, the total size of its dynamic volumes must not exceed 2TB.

Free system disk space

Backups depend on snapshots created using native Microsoft tools. When a backup session completes, snapshots are automatically deleted.

By default, snapshots are created on the system disk. There must be enough space for them. Space requirements vary depending on your system but sometimes a snapshot can reach the size of the system.

> If it is not possible to allocate enough space on the system disk, consider changing the snapshot location to another drive.

Shadow Copy Service (server versions only)

On the server versions of Windows, the Shadow Copy option must be enabled for all drives in the system.

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

System state recovery requirements

Hardware requirements

The hardware you want to perform recovery to must be the same model as the original. Some differences are critical (for example, different drivers), others are not (for example, the new hardware with more disk space than the original hardware).

> You can try recovery to dissimilar hardware at your own risk but we cannot guarantee that all the features will function correctly.

Software requirements

1. The operating system must be the same as the original
2. The build versions and service packs must be the same
3. (For domain controllers) An empty Active Directory must be available (you can create it using DCPromo)
4. If the device being restored is an Active Directory, the device must be booted into Directory Services Restore Mode (DSRM)

Alternative recovery options

If some of the requirements cannot be met, consider the following alternatives to pure System State recovery:

- Virtual disaster recovery (full operating system recovery to a virtual machine)
- Bare metal recovery (full operating system recovery to new hardware)

Virtual Disaster Recovery and Bare Metal Recovery

> Be aware that in order to successfully restore using the Virtual Disaster Recovery or Bare Metal Recovery methods, you must back up the full System State data source

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

Network shares

The Network Shares data source lets you back up data from a local network (NAS). The Network Shares data source on the Backup Manager is currently available on **Windows** devices only.

See the Network Share backup requirements - Windows page for details on the requirements for backing up Network Shares on Windows devices and see Backup Network Shares - Windows for steps on configuring these.

Solutions for macOS and GNU/Linux

If you want to back up shared network drives on a **macOS** or **Linux** device, these need to be mounted first (connect to your computer) so Backup Manager can recognize them in the **Files and Folders** data source.

There is no common way to mount a network share on **Linux**, follow specific instructions from a respected source for the required distribution.

For details on configuring a macOS device, see: Pre-backup settings for macOS

There is no limit to the number of network shares you can back up.

Limitation

- Network Shares are **only** supported if they utilizes SMB (Server Message Block protocol)

  > Other share setups may work, but are **not** supported

- Network Shares cannot be backed up on DFS replication

Network shares versus Files and folders backup

Backing up data on a shared network drive is almost the same as backing up files and folders on the main computer (the one that Backup Manager is installed on). There are only two differences:

- Network shares often need **user authorization**
- Network shares do not support the backup of **open files** (because the Volume Shadow Copy Service used for that purpose is unavailable on the network)

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

What's inside:

Network Share backup requirements - Windows

The Network Share backup has the following requirements that must be met:

- The network share must be available during backups.

  > If the network resource goes into the sleep mode or gets disconnected from the local network, it may not be possible to complete the backup.

- If computers in your local network are united into domains, the target network share must belong to the same domain as the main computer (otherwise there may be cross-domain authentication issues on Windows).

There is no limit to the number of network shares you can back up.

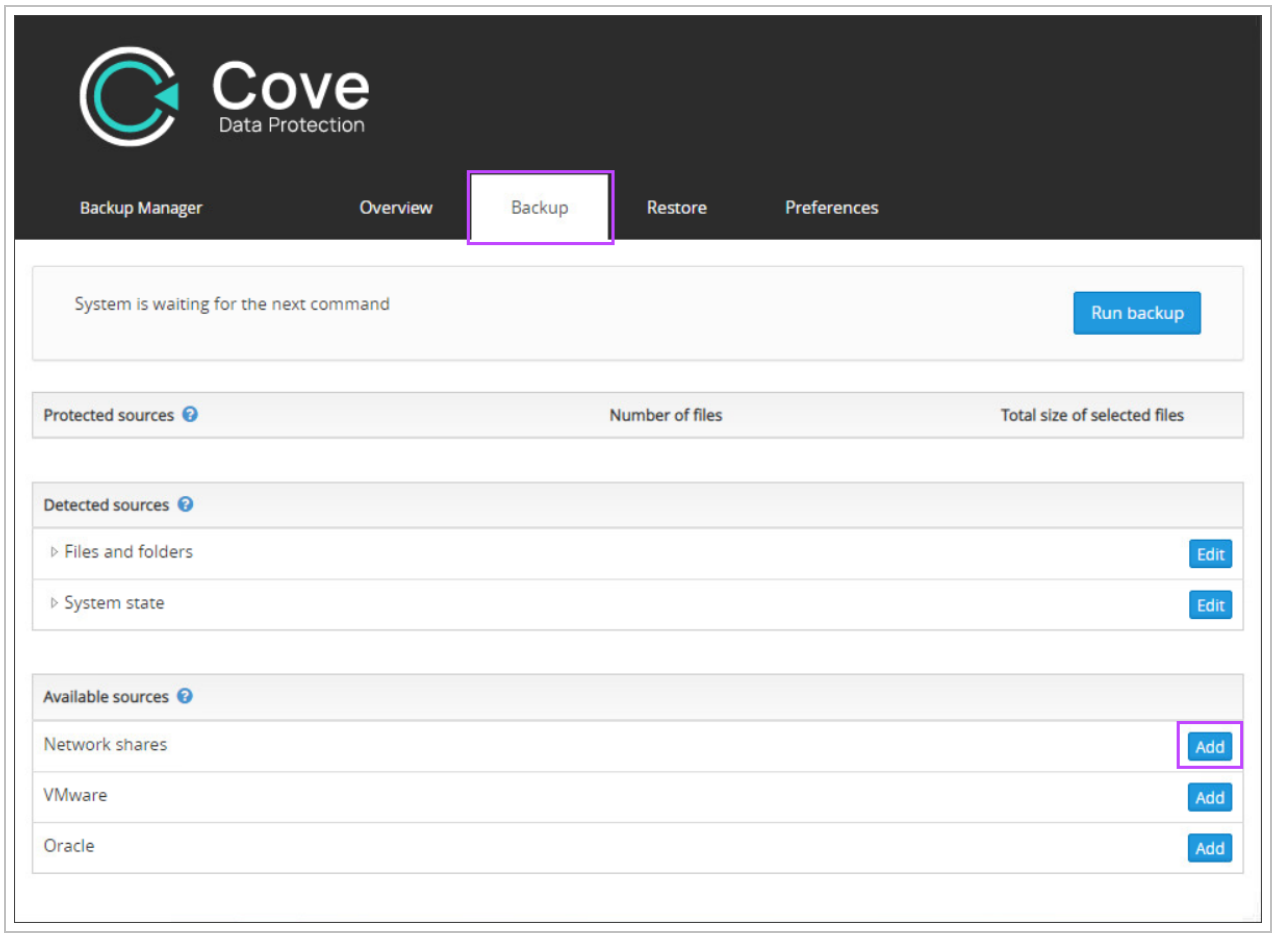
Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

Backup Network Shares - Windows

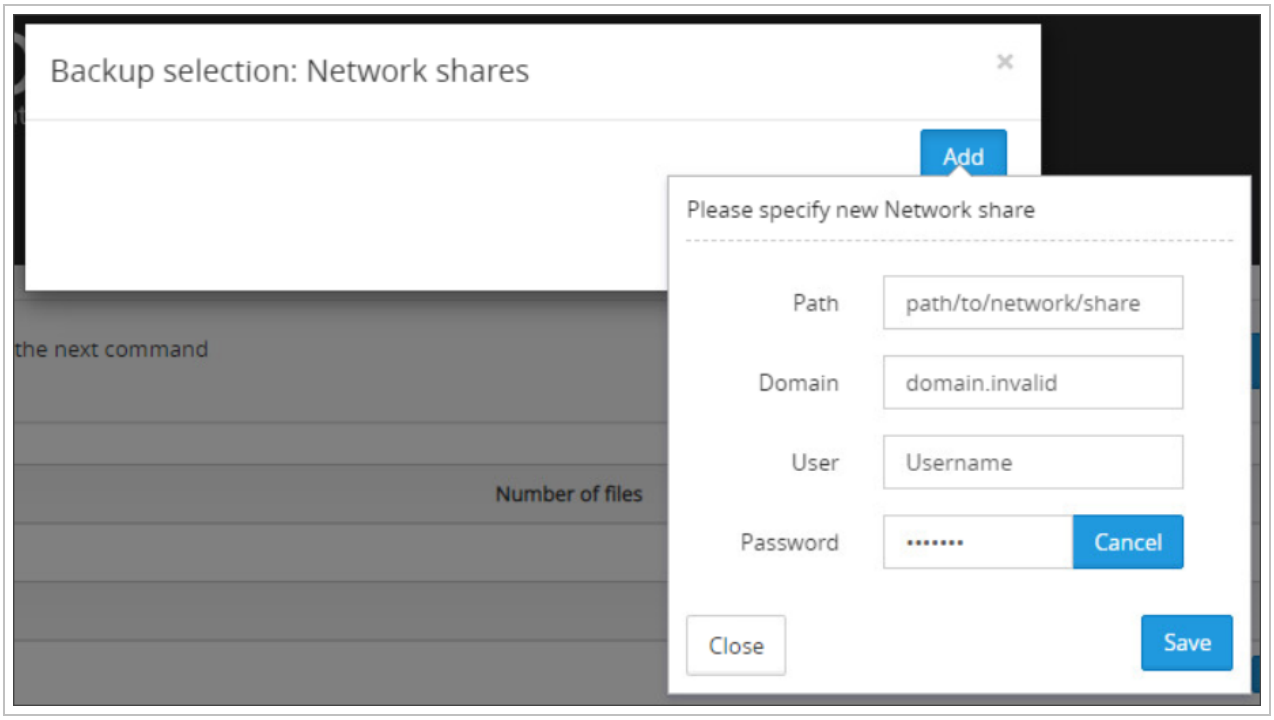
To configure Cove Data Protection (Cove) to backup data from Network Shares. You must configure the Network Shares data source on the Backup Manager.

1. Launch the Backup Manager for the device you wish to backup Network Shares from
2. Navigate to the **Backup** tab
3. Click **Add** for the Network Shares data source under **Available Sources**



4. Click **Add** on the **Backup Selection: Network Shares** box

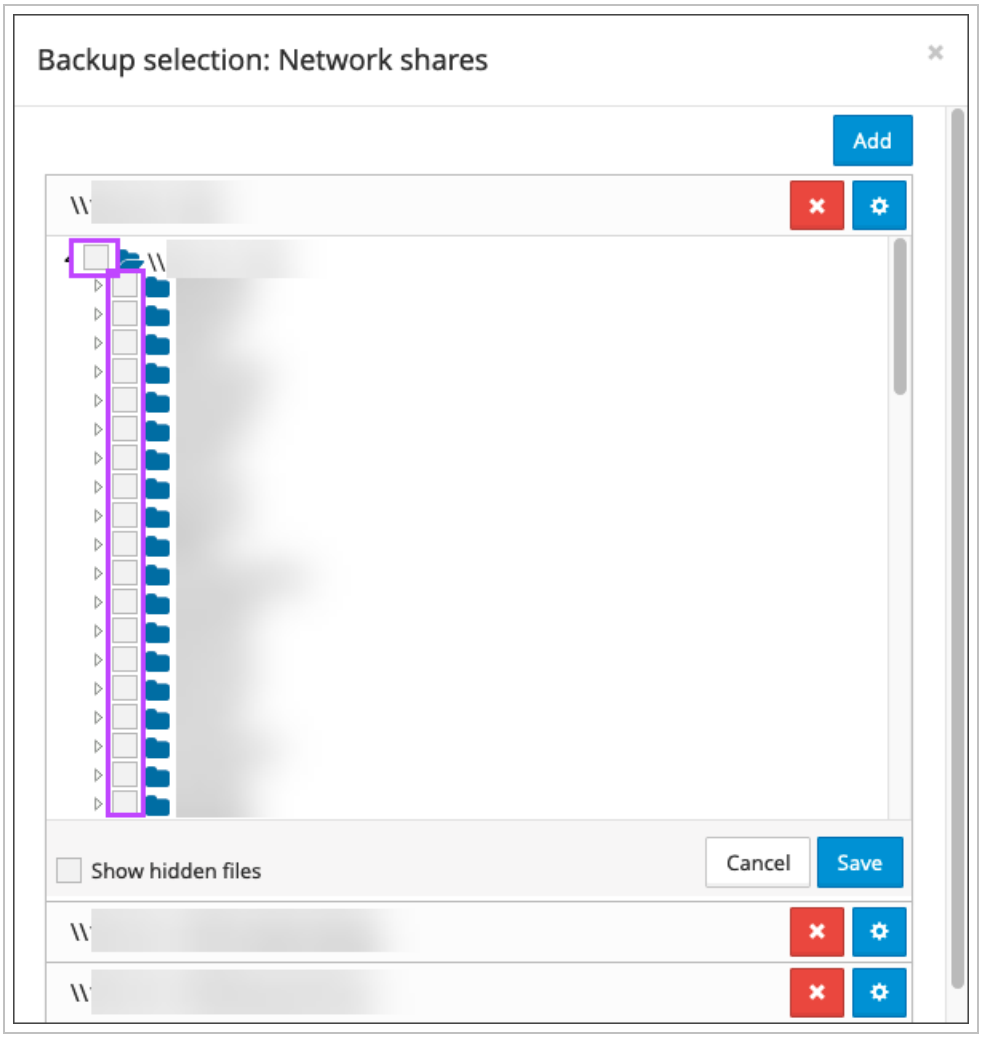
5. You must now provide the network share details:



- **Path** - This is the network share location: a full network path to the root folder of the network share or to a particular directory
- **Domain** - Add the domain name. If the computer belongs to a Windows network domain, you need to specify that domain (for example, COMPANY.COM). If there is no domain, you can leave the field blank in most cases. On some networks, however, you will need to enter the host name of the target machine (for example, WORKSTATION-PC)
- **User** - Enter the user account name of an account that has "read" permissions to the directories intended for backup (it will be necessary to scan the file tree and get file content)
- **Password** - Enter the user account password of the user account name that has "read" permissions to the directories intended for backup (it will be necessary to scan the file tree and get file content)

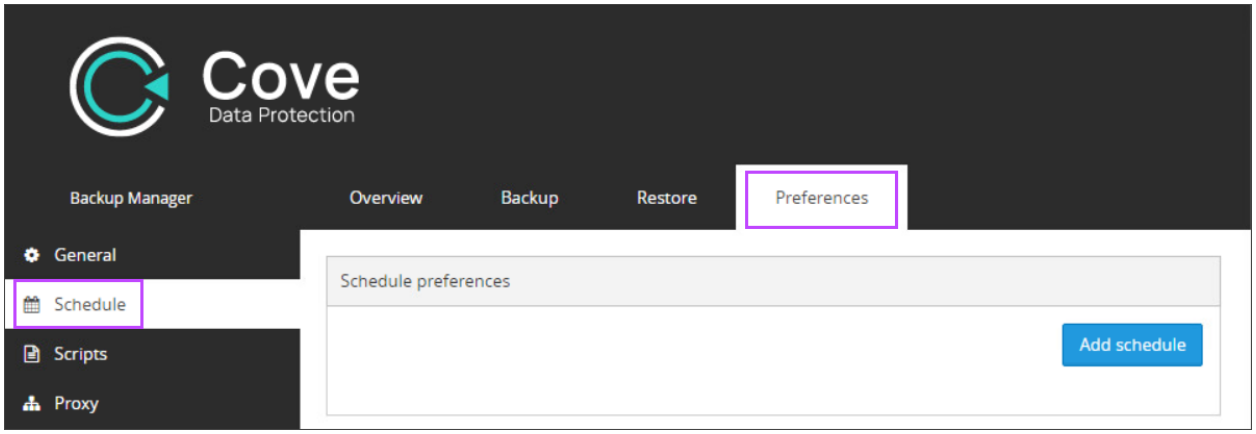
6. Once added, click **save**

7. Select files or folders you wish to be included in the backup by placing a check mark in the box to the left of each required file or folder

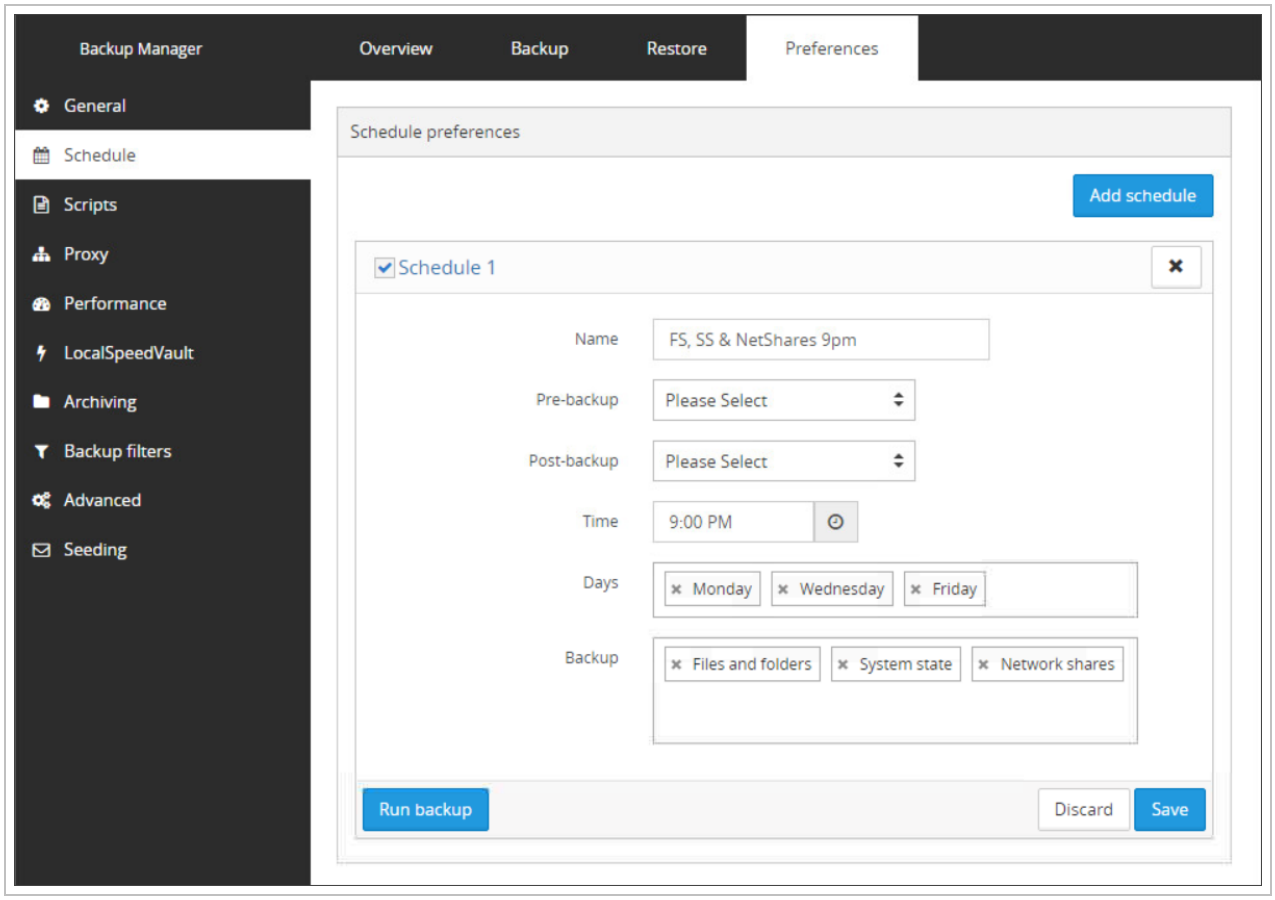


8. Click **save**
9. Move to the **Preferences** tab

10. Navigate to **Schedule** to configure the schedule for the backups



11. Select **Add Schedule** or edit an existing schedule to include the Network Shares data source



12. Give the schedule a name - make this something relevant to the backup configured such as "FS, SS & NetShares 9pm"
13. If you have created any scripts, these can be selected to run before the backup (Pre-backup) or after the backup (Post-backup) by selecting them from the given dropdowns (Optional)
14. Set the time for the backup to run

15. Choose the days on which you want the backup to run
16. Select the data sources to backup (ensuring that Network Shares is included)
17. Click **Save**

You may now either run the initial backup manually by selecting **Run Backup**, or wait for the backup to run as per the schedule configured.

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

Pre-backup settings for macOS

If you wish to back up a local network resource on a macOS computer, you need to permanently **connect it to your desktop**. This is done once. After that you will be able to add the network resource to your backup selection in the Backup Manager and create a backup schedule for it.

1. Launch the Backup Manager for the device
2. Navigate to the **Backup** tab
3. Click **Edit** next to the Files and Folders data source
4. Expand the file tree and find the mapped network resource in the "Volumes" directory
5. Add the mapped source to the backup selection
6. Click **Save**

How to map network resource

The below instructions detail mounting the network share on macOS version 10.9 Mavericks, these steps may differ on newer or older OS versions:

1. Open the Finder
2. From the menu bar, choose **Go > Connect to server**
3. Open the address of the network resource you want to map (for example `smb://192.168.0.55/share`)

   Please see this Apple instruction for supported network address formats.
4. Click **Connect**
5. Enter your access credentials for the network resource
6. From the Apple menu, choose **System preferences**
7. Click **Users & Groups > Login items > Add an item**
8. Locate the network drive you have mounted (you will find it under "Shared" in Sidebar)
9. Click **Add**

Instructions for other versions may differ. You can find all necessary details by visiting Apple Support area.

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

Enabling backups in Backup Manager

Two types of backups are available:

1. **Schedule-based** backups (run on a certain day/time basis)
2. **Frequency-based** backups (run at a specified interval)

Requirements

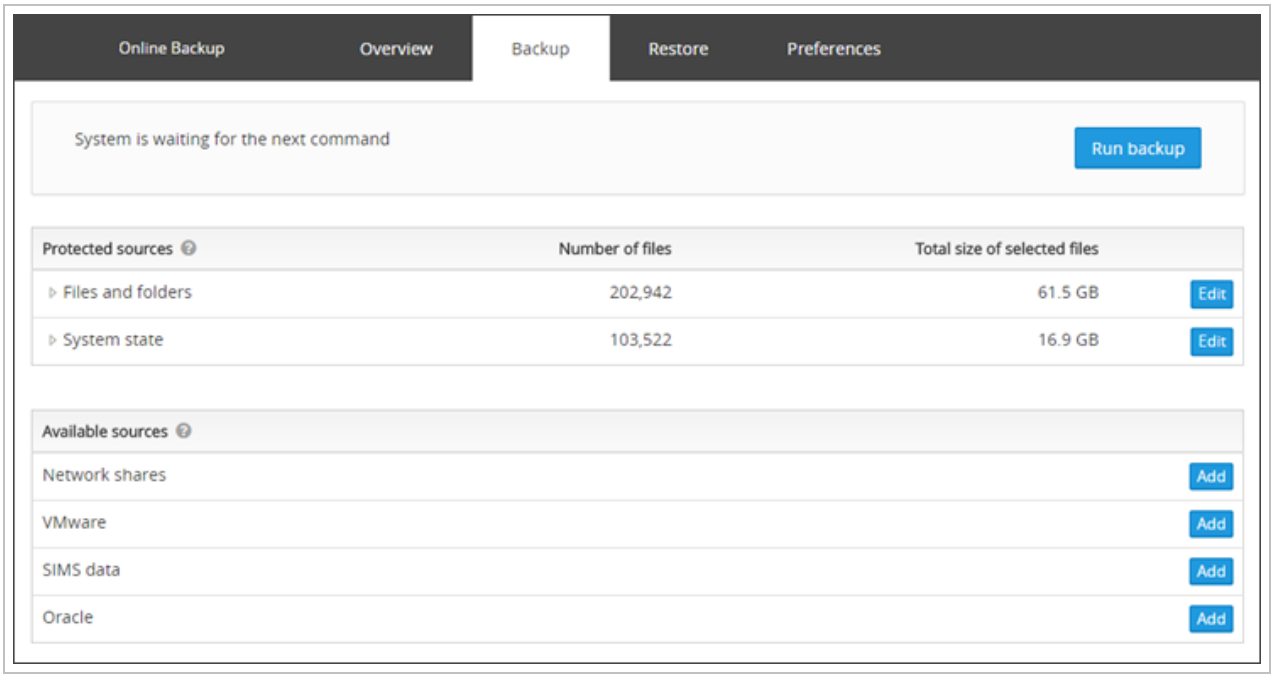
The computer must be online (turned on and must not enter the sleep mode) during backups. If a machine is offline, it will cause the backup to fail to start and will not begin until the machine is turned on or woken up.

If a backup is already running when the machine is turned off, the backup will be aborted. If the machine enters sleep mode while a backup is in progress, the backup will pause until the machine is woken up.

> Be aware that in order to successfully restore using the Virtual Disaster Recovery or Bare Metal Recovery methods, you must back up the full Files and Folders data source (the whole system disk `C:\` or any other depending on the configuration of your computer)

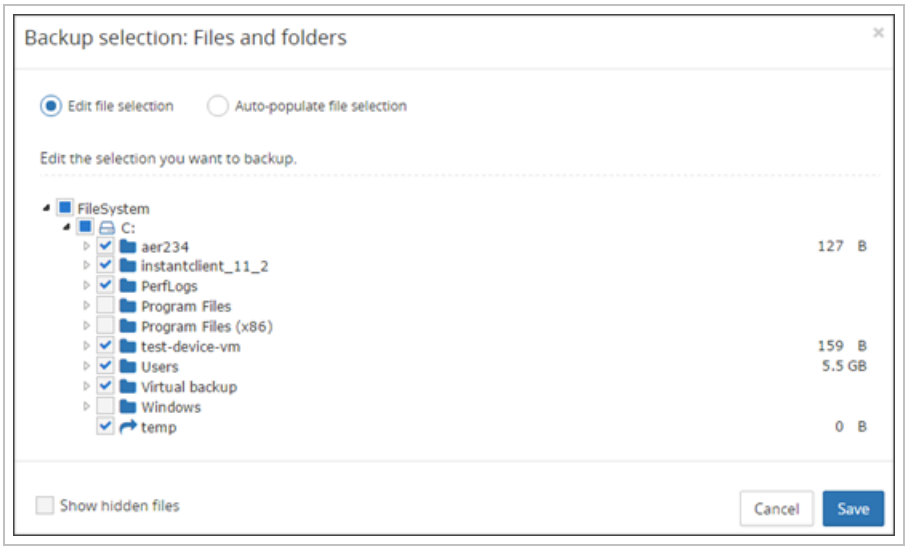
Configure backup selection

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Add** next to the data sources you want to back up



> The below steps detail adding **Files and Folders** for selection, but the process is similar for most data sources. Sources such as Network Shares and VMware require you to supply additional information, such as server details, paths, usernames and passwords.

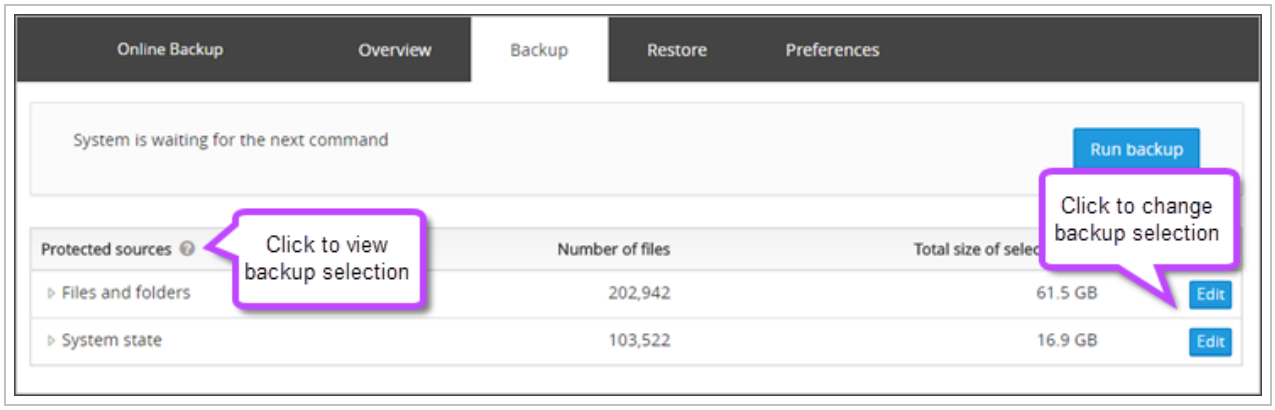
4. Select the files, folders, components (such as data bases, virtual disks, etc.) to back up. You can let the Backup Manager help you choose data for backup using the Automatic File Selection feature



5. Click **Save**

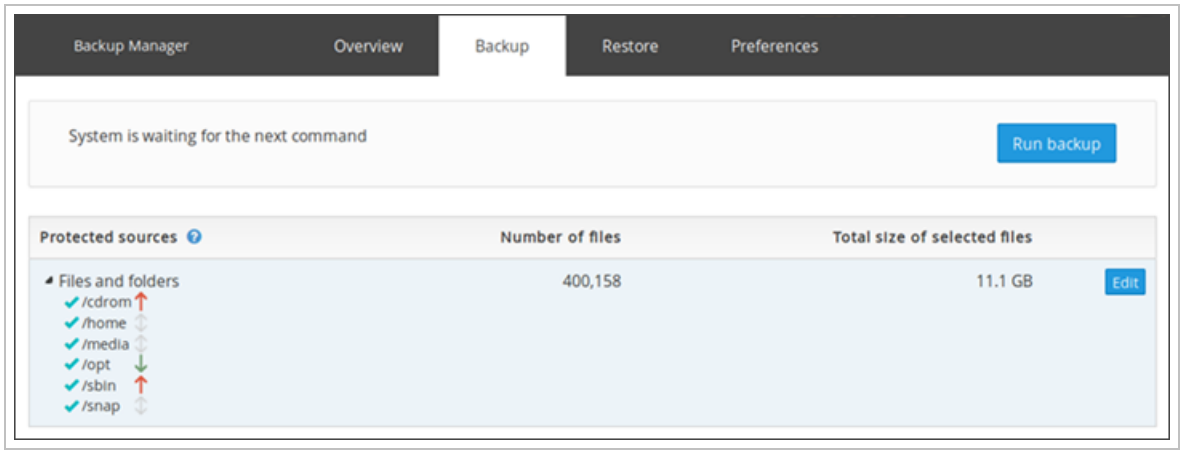
To make sure all necessary data has been included into your backup selection, click on the name of the data source. This will provide a list of the selection made.

Seeing a green tick followed by "\" means the whole data source is selected for backup.



> If you clear your backup selection after at least one backup has been completed, you will be offered to **remove all backup copies** of these files from the Cloud. This means the **entire backup history** of this data source will be deleted. **This action is irreversible.**

If you have selected only part of the disk, you have an option to set the priority of the files in the backup selection.



To do this:

1. Click on the name of the data source
2. Click the arrow to the right of the selection to choose the priority:
   - Click once to get a red up arrow - This indicates a high priority and will be backed up first
   - Click twice to get a green down arrow - This indicates a low priority and will be backed up last
   - Do not click or click to remove a priority to get a grey double-sided arrow - This indicates no priority set and will be backed up between the high and low priority jobs

> Data of the same priority will be completed in alphabetical order.

Starting a Backup

Start a one-time backup

You can initialize a backup manually at any time.

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Run backup**

The length of the backup depends on the size of your backup selection, the data transfer speed and performance of your computer.

> The **Run backup** button will be unavailable until at least one data source is configured for backup. This can be done by following the Configure backup selection steps above.

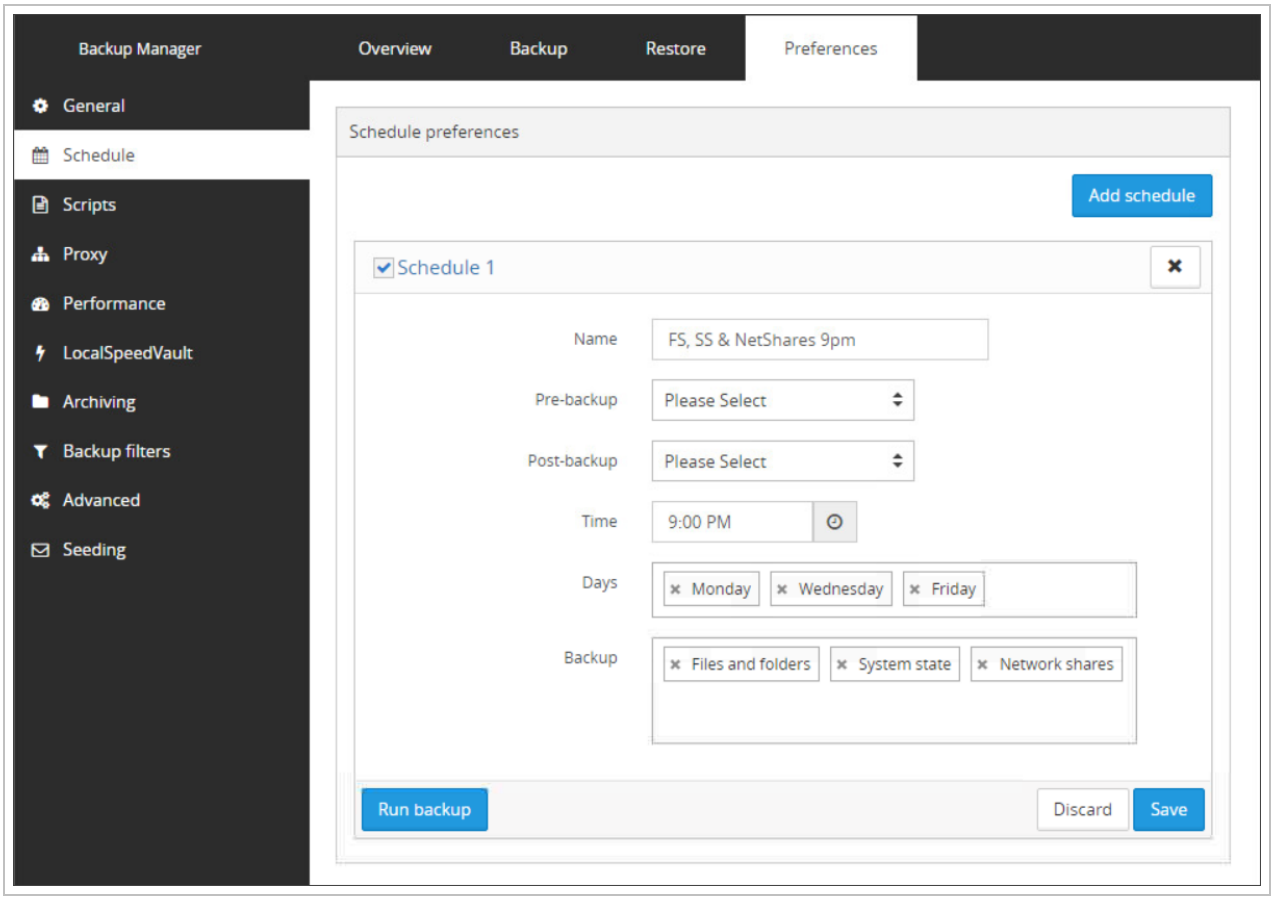
Configure schedule-based backups

The most convenient method of configuring backups is to set up a **backup schedule** which will automatically run the backups without requiring you to intervene.

You can create multiple schedules for each device, for example if you want Files and Folders to run at 9am but you want Files and Folders, System State and MySQL to run at 9pm.

To create a backup schedule:

1. Launch the Backup Manager for the device
2. Open the **Preferences** tab
3. Click **Schedule**
4. Select **Add Schedule**



5. Give the schedule a name - make this something relevant to the backup configured such as "FS, SS & MyS 9pm"
6. Optional - If you have created any scripts, these can be selected to run before the backup (Pre-backup) or after the backup (Post-backup) by selecting them from the given dropdowns.
7. Set the time for the backup to run
8. Choose the days on which you want the backup to run
9. Select the data sources to backup
10. Click **Save**

> If you want to back up a data source regularly, it **must** be configured for backup as well as selected in a schedule or a profile. This can be done by following the Configure backup selection steps above.

If you have multiple schedules listed in this page, you can enable or disable them by ticking the check box beside the name of the schedule. Disabling a schedule does not delete it, but will stop it from running until you manually enable it again.

To edit a schedule, you just need to expand the schedule in question, make the necessary changes and click **Save**.

To delete a schedule, simply click the **X** to the right of the schedule name, you will be prompted to confirm deletion of the schedule - click **Yes**.

> Please note, once a schedule has been deleted, it cannot be undeleted and would have to be recreated manually.

> If you have not configured the backup selection, the schedule will run, but as no data source configuration exists, nothing will be backed up.

Configure frequency-based backups

To enable frequency-based backups on a device, you need to create a **backup profile** with the required backup settings and apply the profile to the device.

See Backup Profiles in Management Console for detailed instructions on configuring profiles.

After the profile has been applied to the device, the new backup settings will be displayed under **Preferences > Schedule** in the Backup Manager. However, all editing is done through the profiles in the Management Console.

Network shares backup error (Windows)

In some rare cases a network share backup session may not be completed on Windows. For example, it can happen with an open, unprotected Windows resource that does not ask for authorization but at the same time does not let the LocalSystem account used by Backup Manager to access the data. If you are experiencing such an issue, try force changing the user account through the Services Console. The alternative account you use should meet either of these requirements:

- It must belong to the **Administrators group** that has access to the network resource
- It should exist both on your computer and on the target network resource (same username and password)

Here is how to switch to that account:

1. Open the **Start** menu and in the search box, enter *services.msc*
2. Double-click the program to open the Services Console
3. Right-click the "Backup Service Controller" service and choose **Properties > Log On**
4. Select the **This account** checkbox, then enter access credentials for the alternative account
5. Apply the changes
6. Right-click "Backup Service Controller", and choose **Restart** from the context menu

The network share should be available for backup after that.

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

MS SQL

Backup Manager lets you back up databases powered by Microsoft SQL Server (**Windows** versions).

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

What's inside:

MS SQL Backup

> It is **not** possible to exclude certain tables or files from a backup selection.

Requirements

To backup the MS SQL data source from Cove Data Protection's Backup Manager, the following requirements must be met:

- The minimum backup unit for MS SQL backups is a **single database**
- The Backup Manager must be installed on the **same MS SQL server** that you want to back up
- There must be sufficient free space in the VSS Shadow Copy storage area for the selected size of the backup data

  > This is because MS SQL backups depend on **VSS snapshots**. When a backup session is completed, snapshots are automatically deleted, so this space will be freed up after the backup session completes.

Recovery model

We highly recommend setting the database to use the **simple recovery model** before starting backups. Under this model, inactive virtual log files are automatically removed after each checkpoint (or shortly after it).

> This saves space and helps avoid unnecessary processing.

To access the model selection and change it:

1. Log on to the MS SQL server
2. Start the **SQL Server Management Studio**
3. In the **Object Explorer**, right-click the database and then select **Properties** from the context menu that opens
4. In the **Recovery model** list, select **Simple**
5. **Save** and **close**

The simple recovery model makes it possible to restore a database only to the end of the most recent backup. We recommend scheduling backups **frequently** enough to prevent the loss of recent changes

> If you choose to back up a database under the **full recovery model**, you are responsible for truncating the logs

MS SQL Server Configuration

If the **Azure AD Connect** feature is enabled on the MS SQL Server, we recommend running a test backup. If the test backup session fails with a VSS error, this may be due to an Azure AD Connect upgrade released in October 2017.

You can resolve the issue by changing the "Log On" account for the **SQL Server VSS Writer** service from "Local System account" to a domain administrator account. To learn more about possible solutions, see the A COM+ application may stop working on Windows Server 2008 when a user logs off Microsoft help article.

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

Copy-only Backups for MS SQL

Backup Manager supports copy-only backups of MS SQL databases. Unlike regular backups, copy-only backups **do not make any changes** to the database and do not interfere with the normal sequence (Full / Incremental or Full / Differential) of database and log backups (visit MSDN Library to learn more). You can restore copy-only backups in the same way as regular backups.

Enable Copy-Only Backups

To perform a copy-only backup, do the following:

1. Open the Backup Manager configuration file (config.ini) in a text editor as an Administrator

   > See Config.ini location for the file location depending on your operating system

2. Add `UseCopyOnlySnapshot=1` to the `[MsSql]` section

   > If the `[MsSql]` section does not exist already, add this to the bottom of the file.

3. **Save** any changes made to the config.ini file
4. Stop and restart the **Backup Service Controller**

   > See Restarting the internal backup processes and service for details

5. Run the backup or wait for the backup to run on schedule

Enable Full Backups

To switch from performing copy-only backups to performing full backups:

1. Open the Backup Manager configuration file (config.ini) in a text editor as an Administrator

   > See Config.ini location for the file location depending on your operating system

2. Change the value of the `UseCopyOnlySnapshot` parameter to `0` or remove the parameter from the configuration file altogether
3. **Save** the changes to the file
4. Stop and restart the **Backup Service Controller**

   > See Restarting the internal backup processes and service for details

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

Enabling backups in Backup Manager

Two types of backups are available:

1. **Schedule-based** backups (run on a certain day/time basis)
2. **Frequency-based** backups (run at a specified interval)

Requirements

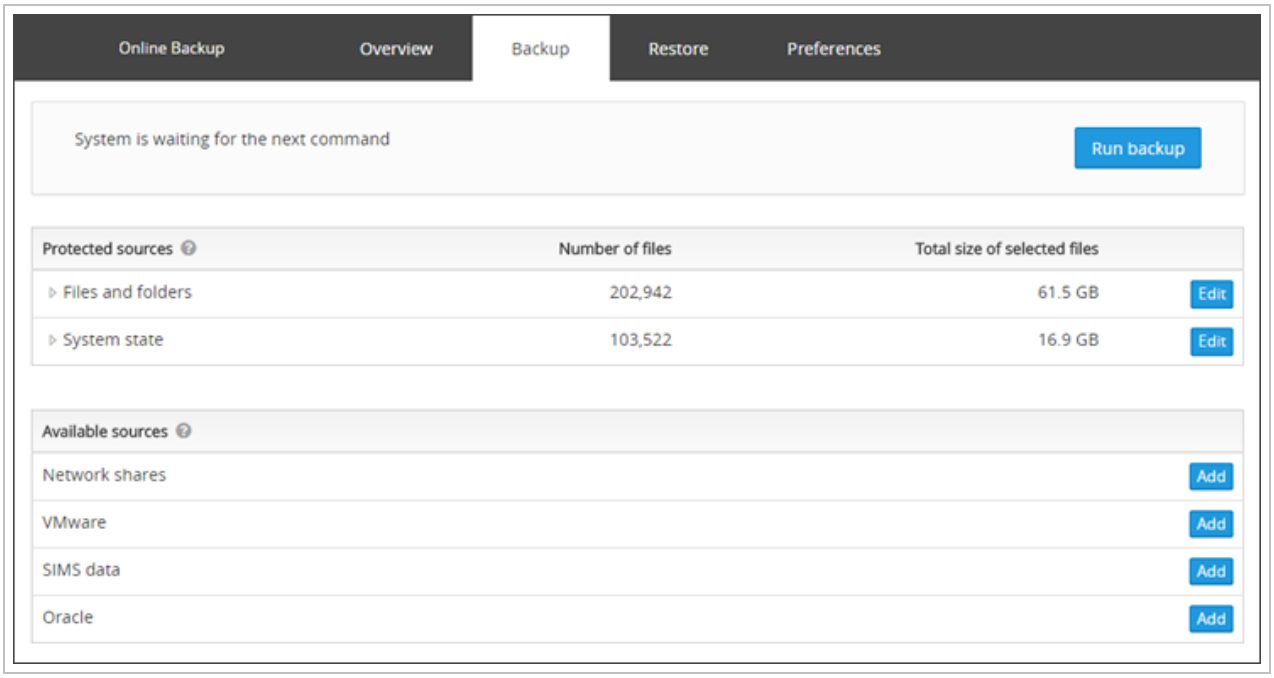
The computer must be online (turned on and must not enter the sleep mode) during backups. If a machine is offline, it will cause the backup to fail to start and will not begin until the machine is turned on or woken up.

If a backup is already running when the machine is turned off, the backup will be aborted. If the machine enters sleep mode while a backup is in progress, the backup will pause until the machine is woken up.

> Be aware that in order to successfully restore using the Virtual Disaster Recovery or Bare Metal Recovery methods, you must back up the full Files and Folders data source (the whole system disk `C:\` or any other depending on the configuration of your computer)

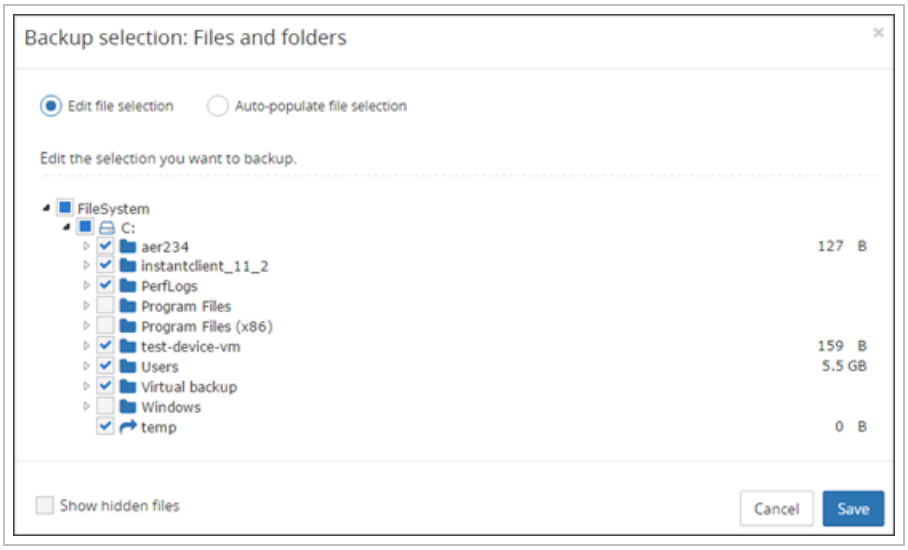
Configure backup selection

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Add** next to the data sources you want to back up



> The below steps detail adding **Files and Folders** for selection, but the process is similar for most data sources. Sources such as Network Shares and VMware require you to supply additional information, such as server details, paths, usernames and passwords.

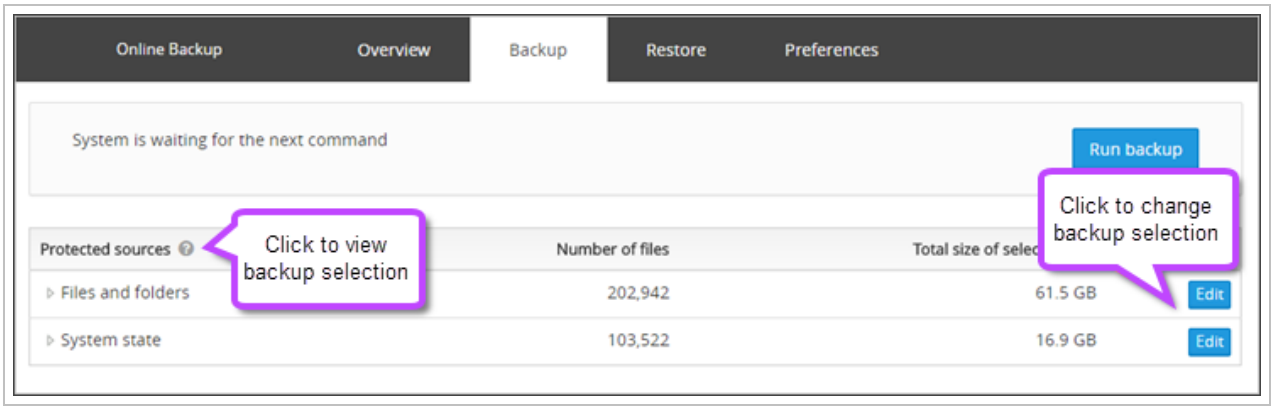
4. Select the files, folders, components (such as data bases, virtual disks, etc.) to back up. You can let the Backup Manager help you choose data for backup using the Automatic File Selection feature



5. Click **Save**

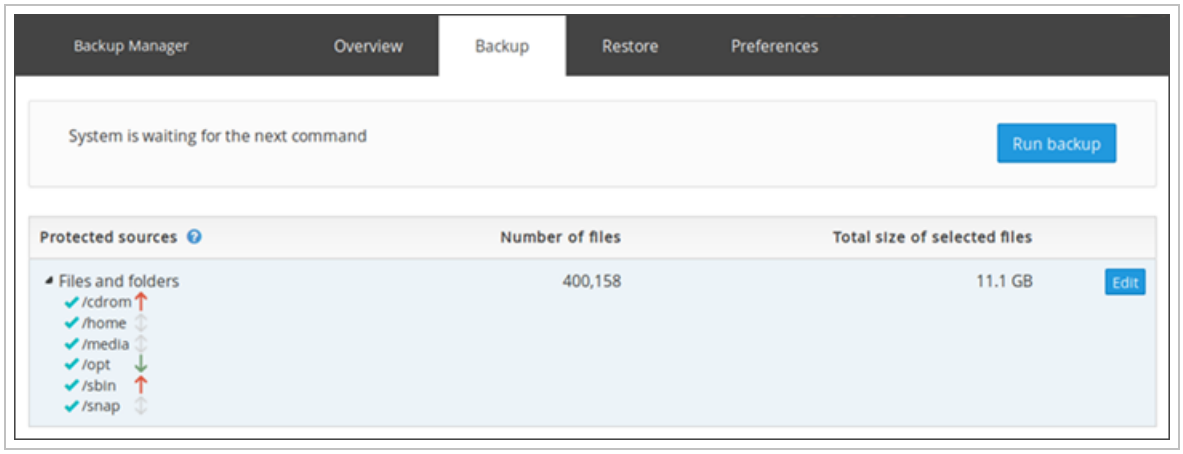
To make sure all necessary data has been included into your backup selection, click on the name of the data source. This will provide a list of the selection made.

Seeing a green tick followed by "\" means the whole data source is selected for backup.



> If you clear your backup selection after at least one backup has been completed, you will be offered to **remove all backup copies** of these files from the Cloud. This means the **entire backup history** of this data source will be deleted. **This action is irreversible.**

If you have selected only part of the disk, you have an option to set the priority of the files in the backup selection.



To do this:

1. Click on the name of the data source
2. Click the arrow to the right of the selection to choose the priority:
   - Click once to get a red up arrow - This indicates a high priority and will be backed up first
   - Click twice to get a green down arrow - This indicates a low priority and will be backed up last
   - Do not click or click to remove a priority to get a grey double-sided arrow - This indicates no priority set and will be backed up between the high and low priority jobs

> Data of the same priority will be completed in alphabetical order.

Starting a Backup

Start a one-time backup

You can initialize a backup manually at any time.

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Run backup**

The length of the backup depends on the size of your backup selection, the data transfer speed and performance of your computer.

> The **Run backup** button will be unavailable until at least one data source is configured for backup. This can be done by following the Configure backup selection steps above.

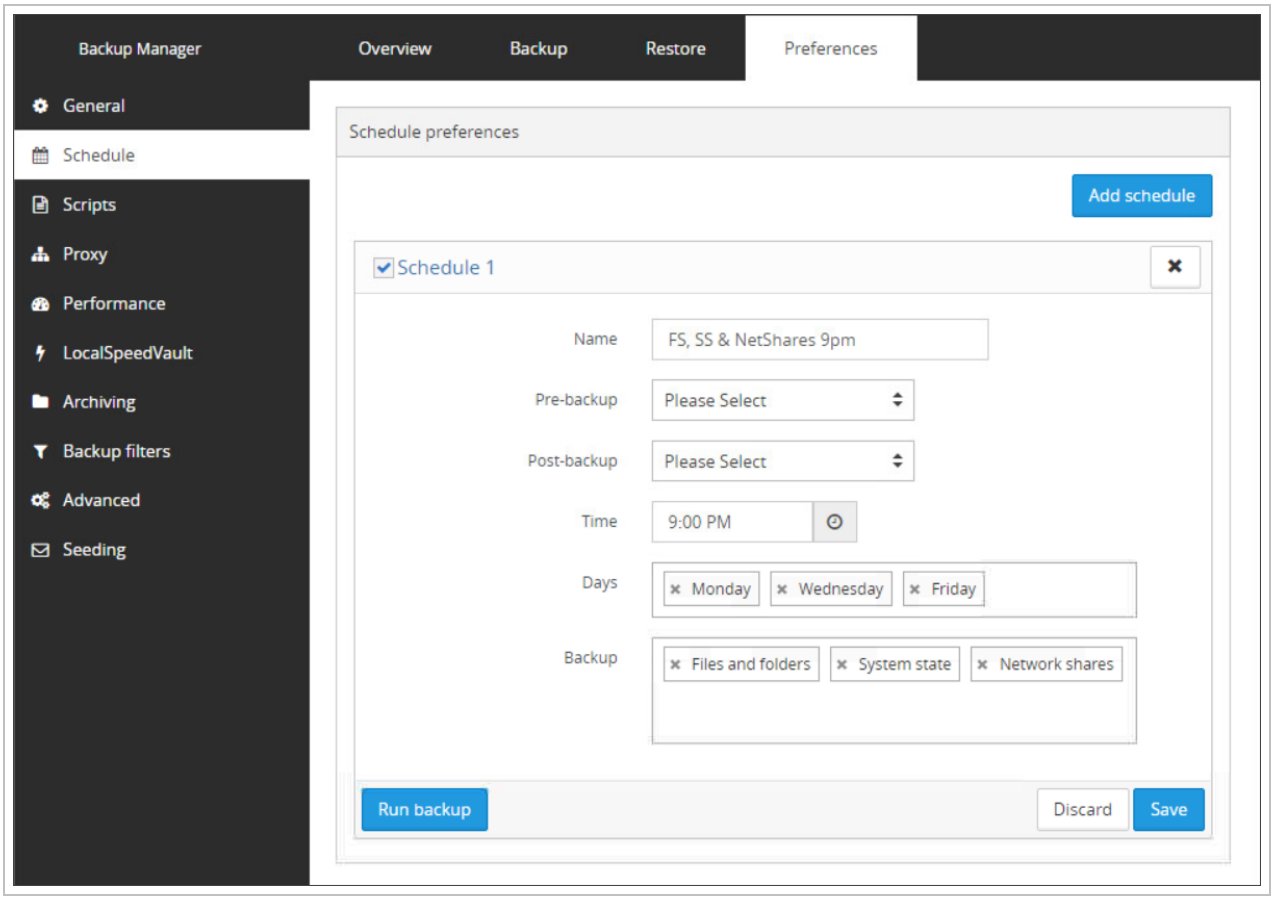
Configure schedule-based backups

The most convenient method of configuring backups is to set up a **backup schedule** which will automatically run the backups without requiring you to intervene.

You can create multiple schedules for each device, for example if you want Files and Folders to run at 9am but you want Files and Folders, System State and MySQL to run at 9pm.

To create a backup schedule:

1. Launch the Backup Manager for the device
2. Open the **Preferences** tab
3. Click **Schedule**
4. Select **Add Schedule**



5. Give the schedule a name - make this something relevant to the backup configured such as "FS, SS & MyS 9pm"
6. Optional - If you have created any scripts, these can be selected to run before the backup (Pre-backup) or after the backup (Post-backup) by selecting them from the given dropdowns.
7. Set the time for the backup to run
8. Choose the days on which you want the backup to run
9. Select the data sources to backup
10. Click **Save**

> If you want to back up a data source regularly, it **must** be configured for backup as well as selected in a schedule or a profile. This can be done by following the Configure backup selection steps above.

If you have multiple schedules listed in this page, you can enable or disable them by ticking the check box beside the name of the schedule. Disabling a schedule does not delete it, but will stop it from running until you manually enable it again.

To edit a schedule, you just need to expand the schedule in question, make the necessary changes and click **Save**.

To delete a schedule, simply click the **X** to the right of the schedule name, you will be prompted to confirm deletion of the schedule - click **Yes**.

> Please note, once a schedule has been deleted, it cannot be undeleted and would have to be recreated manually.

> If you have not configured the backup selection, the schedule will run, but as no data source configuration exists, nothing will be backed up.

Configure frequency-based backups

To enable frequency-based backups on a device, you need to create a **backup profile** with the required backup settings and apply the profile to the device.

See Backup Profiles in Management Console for detailed instructions on configuring profiles.

After the profile has been applied to the device, the new backup settings will be displayed under **Preferences > Schedule** in the Backup Manager. However, all editing is done through the profiles in the Management Console.

MS SQL Recovery

Backup Manager lets you recover databases powered by Microsoft SQL Server.

Requirements

In order to restore MS SQL, the following requirements must be met:

- Backup Manager must be installed on the machine that you want to recover the data to. It can be your MS SQL Server or any other Windows computer (Windows 7 or greater)
- MS SQL must be installed on the machine you want to recovery the data to

> If MS SQL is not installed, you can restore to a flat database and then import the file into MS SQL afterward.

Recovery Options

Like with other data sources, you can recover MS SQL databases to either of the following:

- Original location
- Intermediate location

Recovery to the Original Location

To recover MS SQL to the original location, leave the **Restore to** field blank. In that case the recovered data will be merged with the current data.

> This feature requires **SQL Server** installation.

If you include the **master database** into your recovery selection, **stop** the SQL Server service before you start the recovery.

1. Start the **Services Console** (services.msc)
2. Right-click **SQL Server (MSSQLSERVER)**

3. Choose **Stop** from the context menu

> When the recovery completes, you will need to **start** the SQL Server service again. It can be done through the Services Console or by rebooting the machine.

Recovery to an Intermediate Location

You can recover MS SQL to an intermediate location. It does not need the SQL Server installation. When the recovery completes, you will need to copy the recovered data to the target location manually.

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

VMware

Backup Manager offers backup and recovery for **VMware vSphere (ESXi)** virtual machines. This is done by creating an identical virtual machine with the same operating system, hardware device settings (drivers for modems, network adapters, printers), and all the same content, including documents. The machine is created automatically at the location you specify so it can be on the same server as the original machine or on a different one.

> Installation of the Backup Manager on VMWare devices is done in the same way as installing on any other workstation, see Quick Installation of the Backup Manager for full details.

Guest Level Versus Host Level Backups

VMware VM's can be backed up by either of the following methods:

- **Guest Level** backups - This is the equivalent of backing up a physical machine, where Backup Manager is installed **inside** the VMware virtual machine and you can standardize backup settings, make data source selections, and apply filters and exclusions to avoid backing up unnecessary data
- **Host Level** backups - This method is configured at the hypervisor level, where Backup Manager would be installed and you can configure the selection to backup entire VMs, including their configurations and file structure

> We **strongly** recommend using **guest level** backups as this will give more granularity and flexibility. Guest level backups are also more efficient.

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

What's inside:

VMware Backup Requirements

Supported operating systems

VMware backup and recovery is available on **Windows** devices. Here is the list of supported Windows versions:

- Windows 7, 8[1], 8.1, 10, 11 – Pro and Enterprise editions only (due to Microsoft licensing limitations)
- Windows Server 2012[2], 2012 R2, 2016, 2019 and 2022 – Standard and Data-center editions only (due to Microsoft licensing limitations)

Supported ESXi versions

The following **ESXi** versions are officially supported:

- 6.0
- 6.5 (requires Backup Manager **17.4** or later)
  - In the Recovery Console, this target is available only to those backup devices that are running Backup Manager 17.3 or later
- 7.0
- 8.0

> When a version of a third-party product reaches End of Life, we will endeavor to provide best effort support. However, if versions which are no longer supported by their company begin to fail, the assistance our Support Teams can provide is limited.

Access to most backup and recovery options requires a **paid version** of ESXi. There is an alternative solution for free ESXi users, but it takes some extra steps.

Free ESXi backup

1. Install Backup Manager on each of your VMware virtual machines (a separate device for each VM)
2. Back up the virtual machine. Here is the minimum requirement:
   - The system state of your VM (the System State data source)
   - The whole system disk – `C:\` or another disk that has your operating system and that the operating system boots from (the Files and Folders data source)
3. Perform recovery in either of these ways:
   - Create a new virtual machine with required characteristics and perform bare metal recovery there (recommended as a faster option)
   - Perform virtual disaster recovery to a VMDK file. Use VMware vCenter Converter to convert the local VMDK file from the workstation format to the appropriate format and to attach it to the ESXi server

> For restore purposes, you **must** ensure the version of VMWare ESXi on the restore device is the same or higher as is on the backup device.

---

[1] If the source machine is booted from a GPT disk (UEFI firmware), virtual disaster recovery must be performed from a recent version of Windows: Windows 8.1, Windows 10, Windows Server 2012 R2 or Windows Server 2016.
[2] If the source machine is booted from a GPT disk (UEFI firmware), virtual disaster recovery must be performed from a recent version of Windows: Windows 8.1, Windows 10, Windows Server 2012 R2 or Windows Server 2016.

Recommended pre-backup settings

Before you start backups, it can be a good idea to enable Changed Block Tracking (CBT) on your virtual machines. It is a highly effective feature that reduces the duration of subsequent backups.

For requirements and instructions, please refer to article 1020128 from the VMware Knowledge Base (Changed Block Tracking (CBT) on virtual machines).

> Note that the CBT feature does **not** influence statistics in the **Size of processed files** and **Transferred size** columns in backup reports.

> The CBT feature is not available when creating a new role in vCenter 7.

Configure VMDK Connection Transport Method

It is possible to configure a transport method for VMDK Connections in the Backup Manager configuration file (`config.ini`):

1. Stop the Backup Service Controller. See Restarting the internal backup processes and service for details
2. Open a text editor as an **Administrator**
3. Open the Backup Manager configuration file `config.ini`. See Config.ini location for where to find the file
4. If it does not already exist, add a new section containing the following information:

   ```
   [VMWare]
   VDDKTransportMode=value
   ```

   > Where `value` is replaced with one of the applicable Transport Mode Values.

5. **Save** and close the `config.ini` file
6. Start the Backup Service Controller

Transport Mode Values

> The choice of which transport mode is selected is made by the Virtual Disk Development Kit (VDDK).

The options of values that can be used for the VDDKTransportMode are:

Value
`auto` (Default)
`nbd`
`san`
`hotadd`

Value
`nbdssl`
`file`

You can find more information on Virtual Disk Transport Methods on the VMware documentation.

Limitations

We cannot support backup for:

- Templates
- vApps

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

VMware backup MS SQL and MS Exchange log truncation

If your VMware machine has MS SQL or MS Exchange installed, you can enable **automatic log truncation** for these applications. The operation involves unneeded logs only and is performed strictly after successfully completed backup sessions.

Log truncation works on the **US English versions of MS Windows Server**. See the table below for other software compatibility details.

Guest systems	VMware versions	MS Exchange versions	MS SQL versions
Windows Server 2012 and greater (US English versions)	▪ 6.0 ▪ 6.5 ▪ 7.0 ▪ 8.0	Exchange Server: ▪ 2010 ▪ 2013 ▪ 2016	SQL Server: ▪ 2012 ▪ 2014 ▪ 2016

> When a version of a third-party product reaches End of Life, we will endeavor to provide best effort support. However, if versions which are no longer supported by their company begin to fail, the assistance our Support Teams can provide is limited.

Prerequisites

To enable log truncation, make sure the following conditions are met:

- The target virtual machine has VMware tools installed and are running
- PowerShell is installed on the guest OS
- The target virtual machine is started

Enable Log Truncation

To enable the Log Truncation feature from the Backup Manager client:

1. Launch the Backup Manager for the device
2. Navigate to the **Backup** tab
3. Scroll to the **VMware** data source
4. Click **Edit** to update the backup selection
5. Select **Manage logs** > **Enable log truncation**
6. Enter your access credentials (an administrator account is required)
7. **Save** and close

> For restore purposes, you **must** ensure the version of VMWare ESXi on the restore device is the same or higher as is on the backup device.

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

Enabling backups in Backup Manager

Two types of backups are available:

1. **Schedule-based** backups (run on a certain day/time basis)
2. **Frequency-based** backups (run at a specified interval)

Requirements

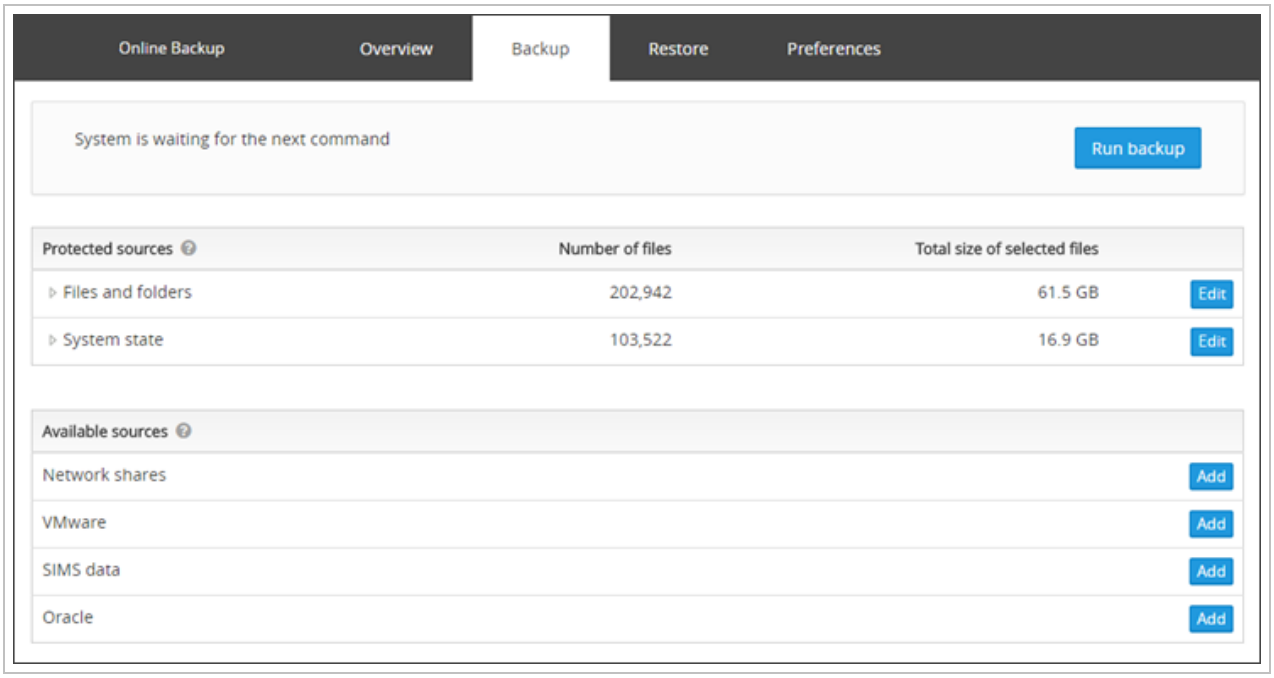
The computer must be online (turned on and must not enter the sleep mode) during backups. If a machine is offline, it will cause the backup to fail to start and will not begin until the machine is turned on or woken up.

If a backup is already running when the machine is turned off, the backup will be aborted. If the machine enters sleep mode while a backup is in progress, the backup will pause until the machine is woken up.

> Be aware that in order to successfully restore using the Virtual Disaster Recovery or Bare Metal Recovery methods, you must back up the full Files and Folders data source (the whole system disk `C:\` or any other depending on the configuration of your computer)

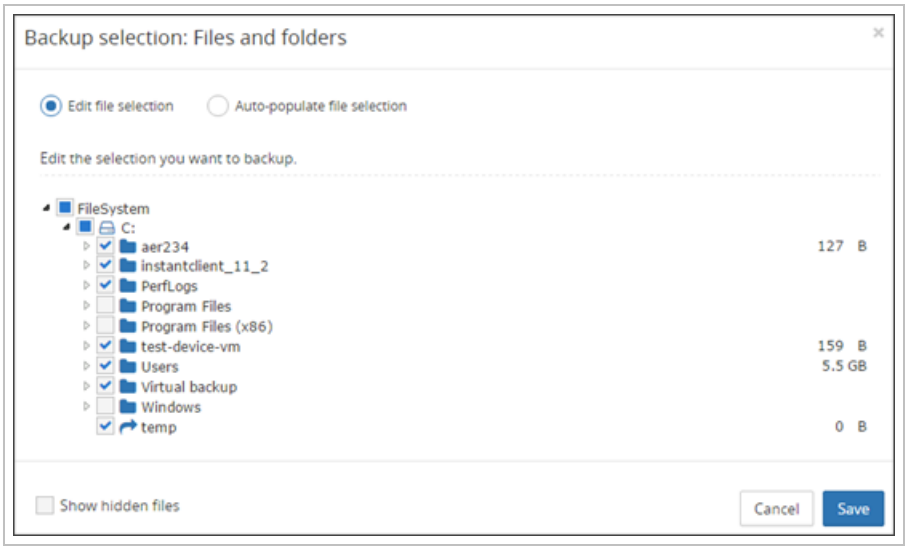
Configure backup selection

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Add** next to the data sources you want to back up



> The below steps detail adding **Files and Folders** for selection, but the process is similar for most data sources. Sources such as Network Shares and VMware require you to supply additional information, such as server details, paths, usernames and passwords.

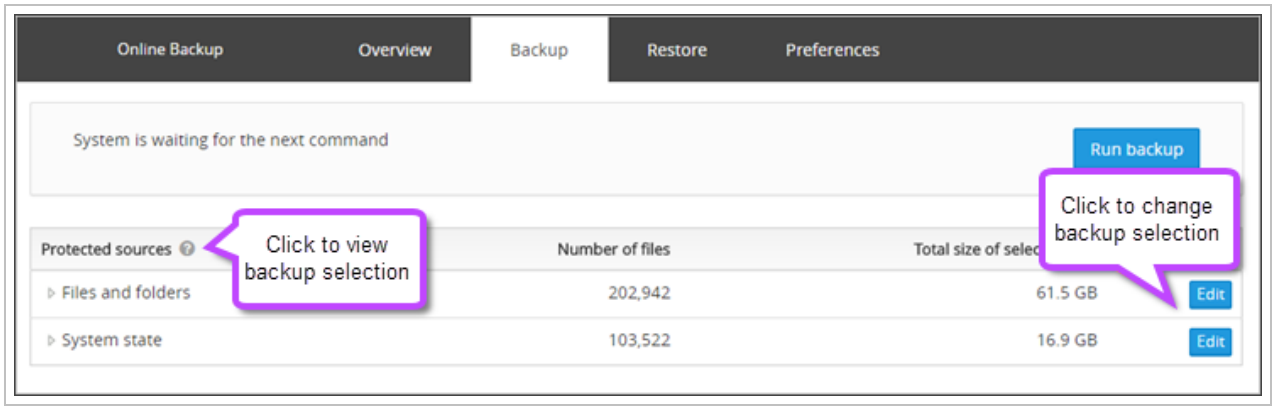
4. Select the files, folders, components (such as data bases, virtual disks, etc.) to back up. You can let the Backup Manager help you choose data for backup using the Automatic File Selection feature



5. Click **Save**

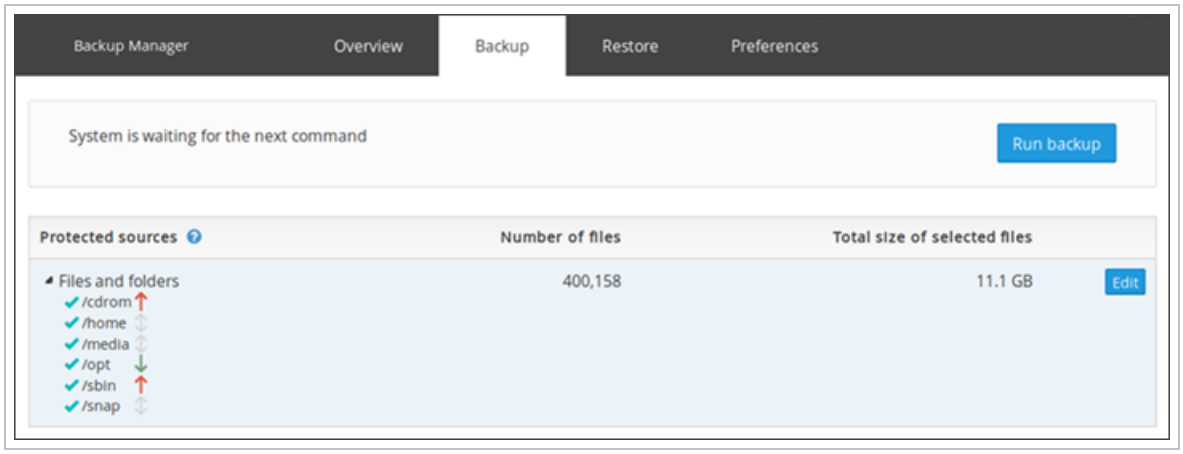
To make sure all necessary data has been included into your backup selection, click on the name of the data source. This will provide a list of the selection made.

Seeing a green tick followed by "\" means the whole data source is selected for backup.



> If you clear your backup selection after at least one backup has been completed, you will be offered to **remove all backup copies** of these files from the Cloud. This means the **entire backup history** of this data source will be deleted. **This action is irreversible.**

If you have selected only part of the disk, you have an option to set the priority of the files in the backup selection.



To do this:

1. Click on the name of the data source
2. Click the arrow to the right of the selection to choose the priority:
   - Click once to get a red up arrow - This indicates a high priority and will be backed up first
   - Click twice to get a green down arrow - This indicates a low priority and will be backed up last
   - Do not click or click to remove a priority to get a grey double-sided arrow - This indicates no priority set and will be backed up between the high and low priority jobs

> Data of the same priority will be completed in alphabetical order.

Start a one-time backup

You can initialize a backup manually at any time.

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Run backup**

The length of the backup depends on the size of your backup selection, the data transfer speed and performance of your computer.

> The **Run backup** button will be unavailable until at least one data source is configured for backup. This can be done by following the Configure backup selection steps above.

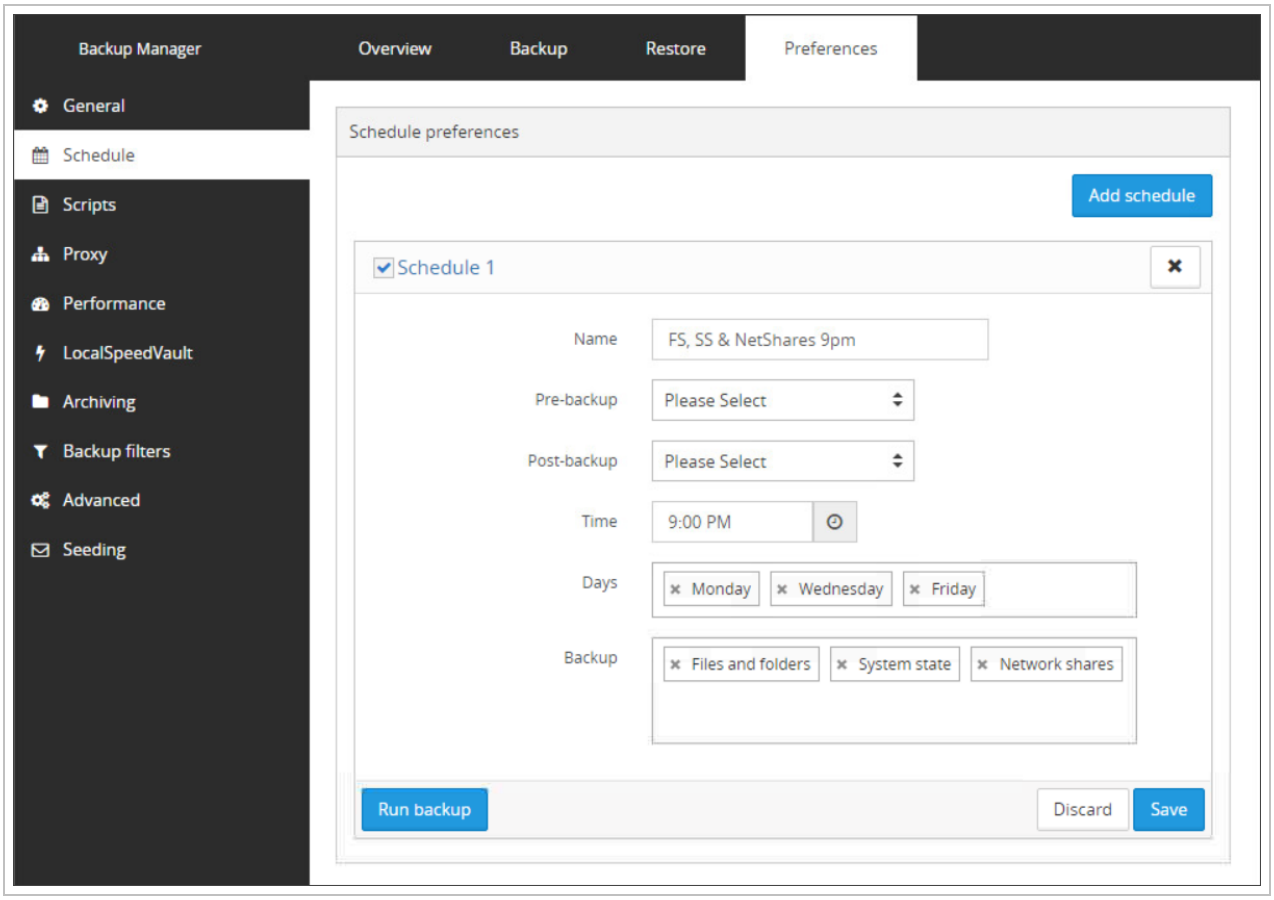
Configure schedule-based backups

The most convenient method of configuring backups is to set up a **backup schedule** which will automatically run the backups without requiring you to intervene.

You can create multiple schedules for each device, for example if you want Files and Folders to run at 9am but you want Files and Folders, System State and MySQL to run at 9pm.

To create a backup schedule:

1. Launch the Backup Manager for the device
2. Open the **Preferences** tab
3. Click **Schedule**
4. Select **Add Schedule**



5. Give the schedule a name - make this something relevant to the backup configured such as "FS, SS & MyS 9pm"
6. Optional - If you have created any scripts, these can be selected to run before the backup (Pre-backup) or after the backup (Post-backup) by selecting them from the given dropdowns.
7. Set the time for the backup to run
8. Choose the days on which you want the backup to run
9. Select the data sources to backup
10. Click **Save**

> If you want to back up a data source regularly, it **must** be configured for backup as well as selected in a schedule or a profile. This can be done by following the Configure backup selection steps above.

If you have multiple schedules listed in this page, you can enable or disable them by ticking the check box beside the name of the schedule. Disabling a schedule does not delete it, but will stop it from running until you manually enable it again.

To edit a schedule, you just need to expand the schedule in question, make the necessary changes and click **Save**.

To delete a schedule, simply click the **X** to the right of the schedule name, you will be prompted to confirm deletion of the schedule - click **Yes**.

> Please note, once a schedule has been deleted, it cannot be undeleted and would have to be recreated manually.

> If you have not configured the backup selection, the schedule will run, but as no data source configuration exists, nothing will be backed up.

Configure frequency-based backups

To enable frequency-based backups on a device, you need to create a **backup profile** with the required backup settings and apply the profile to the device.

See Backup Profiles in Management Console for detailed instructions on configuring profiles.

After the profile has been applied to the device, the new backup settings will be displayed under **Preferences > Schedule** in the Backup Manager. However, all editing is done through the profiles in the Management Console.

VMware recovery requirements

You can recover the whole VMware machines as a working unit, one of its disks or individual files and folders from a disk.

If you choose to restore files and folders from a virtual disk, there are some **additional requirements**:

- The **Virtual Drive** tool is installed and running
- The **file system** on the computer where Backup Manager is installed must support the file systems in the virtual machine that is being recovered (for example, NTFS or FAT). This is necessary to be able to expand the contents of the virtual disks

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

Hyper-V Overview

Microsoft Hyper-V virtual machines can be protected against data loss using the Cove Data Protection (Cove) Backup Manager.

Guest Level Versus Host Level Backups

Hyper-V VM's can be backed up by either of the following methods:

- **Guest Level** backups - This is the equivalent of backing up a physical machine, where Backup Manager is installed **inside** the Hyper-V virtual machine and you can standardize backup settings, make data source selections, and apply filters and exclusions to avoid backing up unnecessary data
- **Host Level** backups - This method is configured at the hypervisor level, where Backup Manager would be installed and you can configure the selection to backup entire VMs, including their configurations and file structure

> We **strongly** recommend using **guest level** backups as this will give more granularity and flexibility. Guest level backups are also more efficient.

Guest Level Backup Advantage

There are several advantages to using Guest Level backups.

Backup

- The use of Cove's Automatic Deployment feature via any remote deployment tool
- The ability to standardize backup settings using Profiles, which would mean no differences between backing up physical or virtual machines
- Improve efficiency by the using filters and exclusions to avoid backing up unnecessary files such as temp and cache files, which result in sending less data and therefore faster backups and restores
- High frequent backups, increase RPO
- No performance impact incurred on the hypervisor

Restore

- Simple and fast granular restore to original or alternative location
- Flexible cross platform restore: Virtual-to-virtual or Physical-to-virtual
- Automated Recovery Testing to the cloud and local target available
- Standby Image support to perform a full system restore back into a virtual machine

  > This can be done as a continuous restore to provide business continuity and increase RTO

Host Level Backup Advantage

Guest level backups are especially useful for Linux VMs, as these cannot use Virtual Disaster Recovery or Standby Image.

Host Level Backup Limitations

We do not recommend Hyper-V or VMware host-level backups even though they are possible for a number of reasons. Several limitations of host level backups are:

Backup

- No use of backup filter and exclusion options
- More data is sent during backups due to temporary disk changes
- Hyper-V clusters are not supported, meaning Backup only includes locally hosted Hyper-V VMs
- Running more frequent backups can affect the hypervisor and bandwidth and impact performance
- It is not possible to back up a CSV and non-CSV volume in the same set on Windows Server 2012 and 2012 R2, due to a Windows limitation
- Backups may fail if the selection contains a Hyper-V cluster deployed on Windows Server 2008 R2 or an earlier version

Restore

- Limited delta restores when restoring single files/databases
- Restore target is limited to the same hypervisor version
- No business continuity included, meaning delta restores will take same amount of time as initial restore
- Automated Cloud Recovery Testing is not included
- Standby Image is not supported

- It is not possible to restore directly to a CSV

  > Instead we recommend restoring to the host locally and then moving the VM over via the Virtual Machine Management Service

Snapshots

Due to the nature of Hyper-V backups, if you restart a backup a snapshot remains on the device. This is because the backup was unable to complete and remove the snapshot itself.

> These snapshots **can** be deleted manually.

What's inside:

Pre-backup settings for Hyper-V

The following settings must be configured **before** creating the backup selection and schedule to set the Backup of the Hyper-V VM or host.

For SMB 3.0 shares used as storage for Hyper-V

Starting from Backup Manager version 16.5, it is possible to back up and restore Hyper-V machines that have **some or all** of their virtual disks on an **SMB 3.0 share**.

The following conditions **must** be met before you start backing up such a virtual machine.

1. The Hyper-V host and the SMB3 server must belong to the **same Active Directory domain**
2. The **File Server VSS Agent Service** must be installed on the SMB3 server
3. The network share on the SMB3 server must be created with the "Applications" profile (under **Select Profile**, select **SMB Share – Applications**

   > See Microsoft instructions for detailed instructions

4. The Hyper-V host (namely its Local System account) must have **full access** to the network share (the Permissions step of the installation wizard)

   > See this Microsoft article for detailed instructions

Increasing backup speed (optional)

To take advantage of the best possible backup speed, you can enable the **volume snapshot** integration service (also referred to as the **volume checkpoint** in the newer versions of Hyper-V).

This lets the Backup Manager use the help of native VSS writers during backups. This improves backup speed and reduces the amount of data transmitted to the cloud.

1. Start the Hyper-V Manager
2. Right-click the virtual machine you want to back up
3. Choose **Settings** from the context menu

4. Go to **Management > Integration services**
5. Enable the **Backup (volume checkpoint)** option or **Backup (volume snapshot)** depending on the version of Hyper-V

Hyper-V Backup Configuration

We strongly recommend the use of Hyper-V Guest Level backups over Host Level backups, as detailed in Guest Level Versus Host Level Backups.

Backup configuration will differ, depending on which method of backup you have decided on.

> Before configuring any Backup to run, check the Pre-backup settings for Hyper-V to ensure these are set.

Guest Level Backup Configuration

For Guest Level backups, the Backup Manager must be installed inside the Hyper-V Virtual Machine. This can be done using Automatic Deployment, or Manual Installation.

Once Backup Manager is installed, you can either configure the device manually by:

1. Follow the Enabling backups in Backup Manager instructions on how to Configure backup selection
2. Then Configure schedule-based backups
3. Set additional device-based preferences, scripts, filters and exclusions

> As Backup Manager is installed within the VM, the data source selection will look just like the selection for any physical device, where we strongly recommend selecting the Files and Folders and System State data sources.

Or

1. Apply a profile to the device which sets the data source selection as was previously configured, as well as setting the frequency of backups and any filters and exclusions

Host Level Backup Configuration

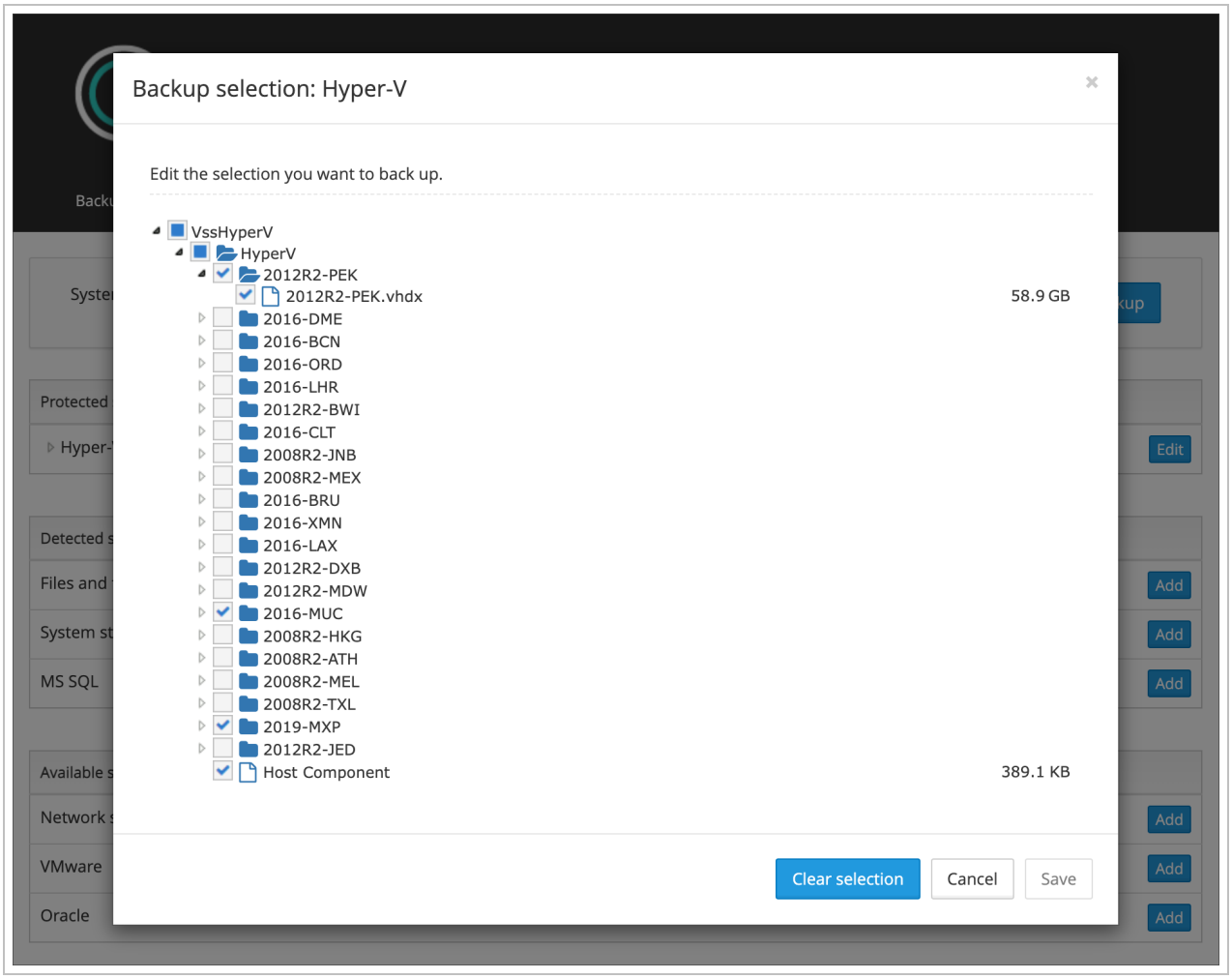
If using Host Level backups, the Backup Manager is installed on the hypervisor, via Manual Installation.

Once the Backup Manager is installed on the host, backups must be configured manually by:

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Add** next to the Hyper-V data source

   > The Hyper-V datasource will be detected automatically, there is no need to authenticate

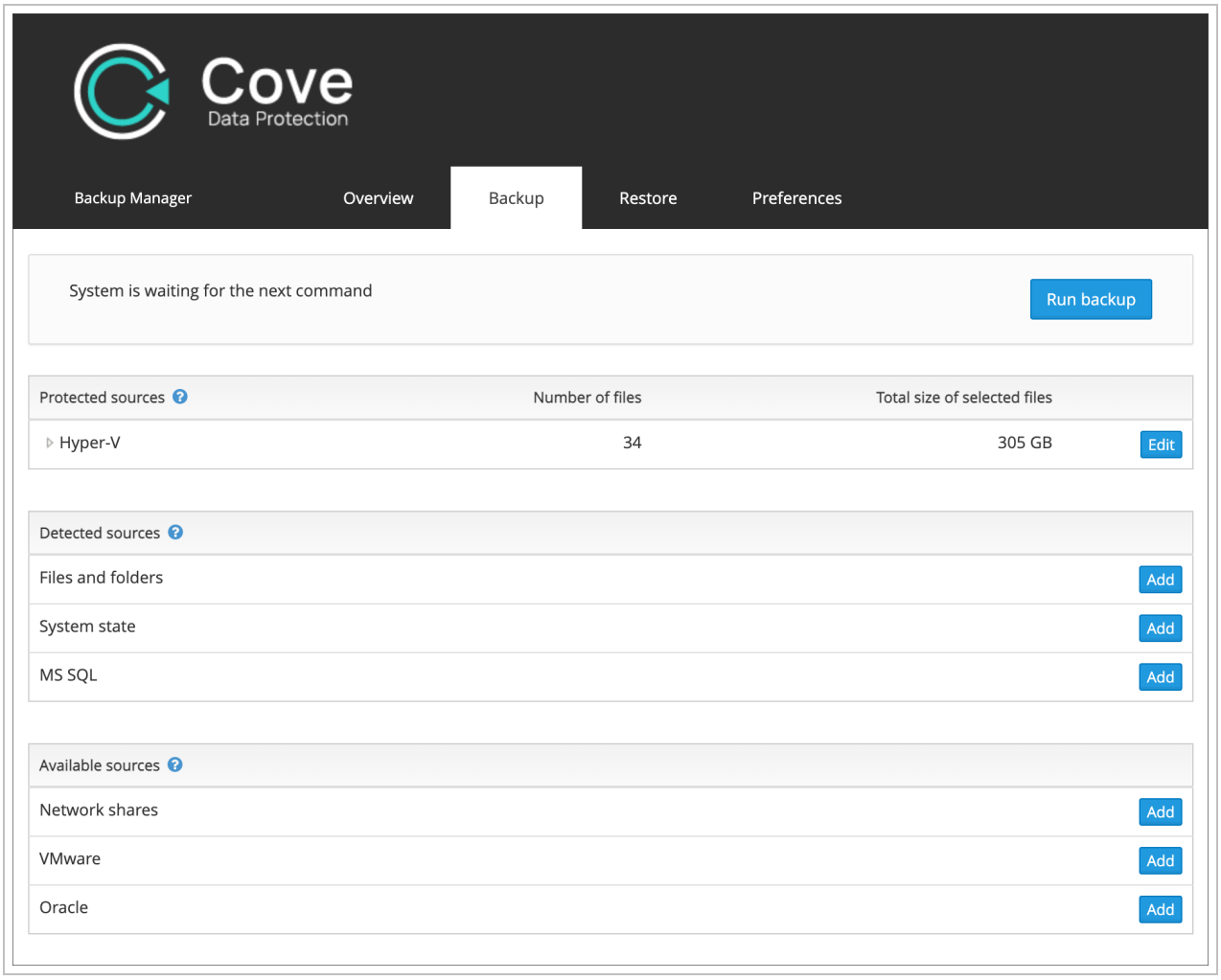
4. Expand the **VssHyper**V folder and make your selection of which Virtual Machines to back up by placing a tick in the box to the left of each VM name



5. Click **Save**

> Hyper-V machines are backed up together with their **snapshots**. This lets you return a machine to a previous state after recovery.

The data source will now display in the **Protected Sources** section



6. Now navigate to the **Preferences** tab and Configure schedule-based backups, being sure to add **Hyper-V** to the **Backup** field
7. **Save** the new schedule

Enabling backups in Backup Manager

Two types of backups are available:

1. **Schedule-based** backups (run on a certain day/time basis)
2. **Frequency-based** backups (run at a specified interval)

Requirements

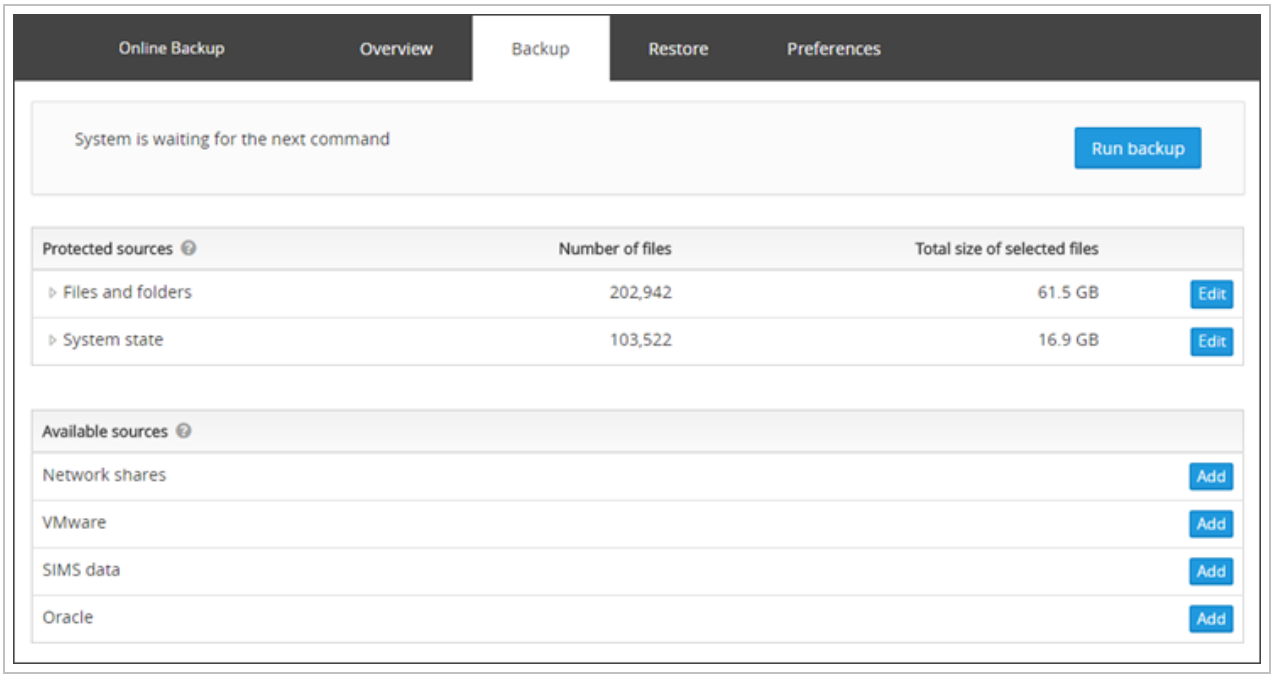
The computer must be online (turned on and must not enter the sleep mode) during backups. If a machine is offline, it will cause the backup to fail to start and will not begin until the machine is turned on or woken up.

If a backup is already running when the machine is turned off, the backup will be aborted. If the machine enters sleep mode while a backup is in progress, the backup will pause until the machine is woken up.

> Be aware that in order to successfully restore using the Virtual Disaster Recovery or Bare Metal Recovery methods, you must back up the full Files and Folders data source (the whole system disk `C:\` or any other depending on the configuration of your computer)

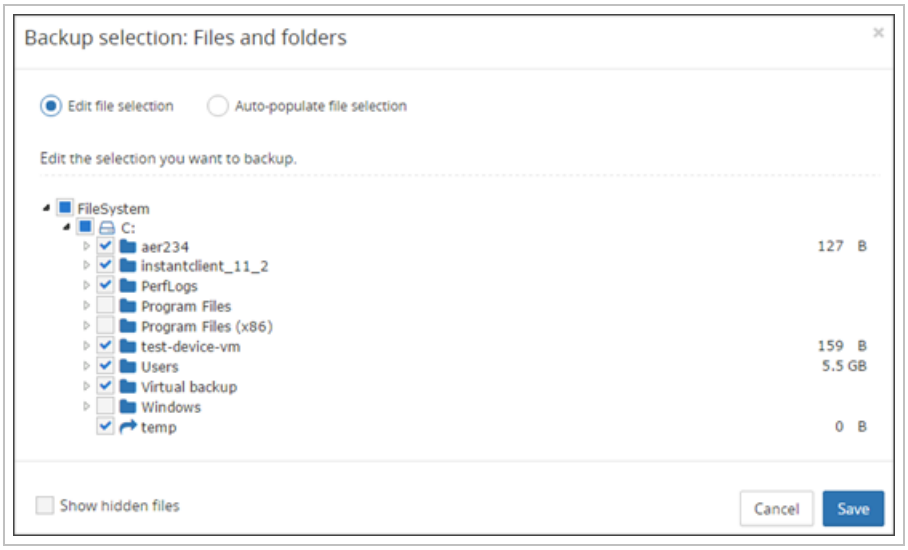
Configure backup selection

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Add** next to the data sources you want to back up



> The below steps detail adding **Files and Folders** for selection, but the process is similar for most data sources. Sources such as Network Shares and VMware require you to supply additional information, such as server details, paths, usernames and passwords.

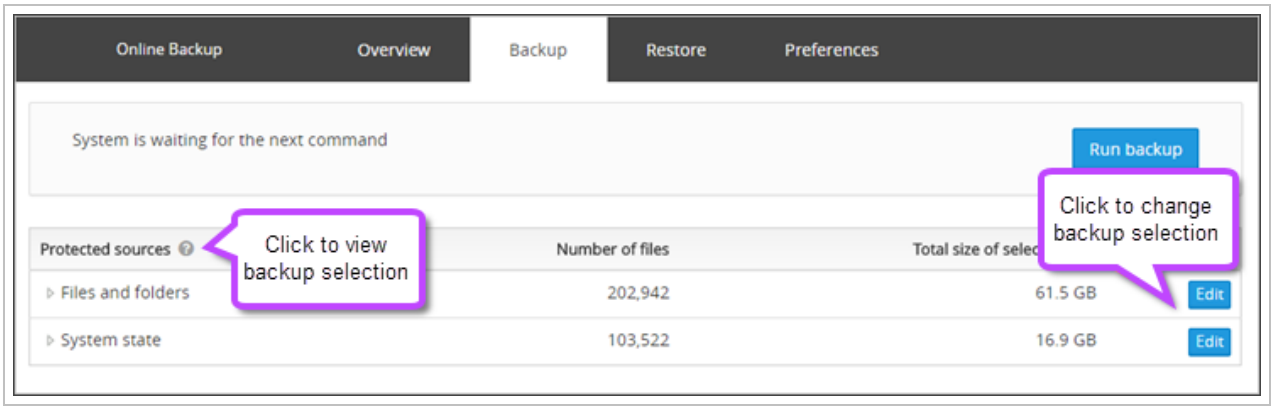
4. Select the files, folders, components (such as data bases, virtual disks, etc.) to back up. You can let the Backup Manager help you choose data for backup using the Automatic File Selection feature



5. Click **Save**

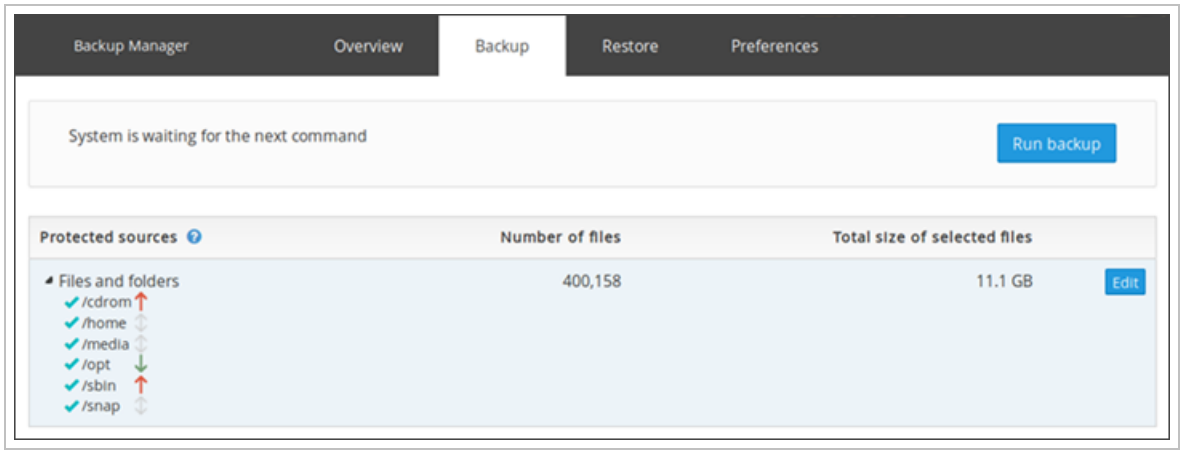
To make sure all necessary data has been included into your backup selection, click on the name of the data source. This will provide a list of the selection made.

Seeing a green tick followed by "\" means the whole data source is selected for backup.



> If you clear your backup selection after at least one backup has been completed, you will be offered to **remove all backup copies** of these files from the Cloud. This means the **entire backup history** of this data source will be deleted. **This action is irreversible.**

If you have selected only part of the disk, you have an option to set the priority of the files in the backup selection.



To do this:

1. Click on the name of the data source
2. Click the arrow to the right of the selection to choose the priority:
   - Click once to get a red up arrow - This indicates a high priority and will be backed up first
   - Click twice to get a green down arrow - This indicates a low priority and will be backed up last
   - Do not click or click to remove a priority to get a grey double-sided arrow - This indicates no priority set and will be backed up between the high and low priority jobs

> Data of the same priority will be completed in alphabetical order.

Starting a Backup

Start a one-time backup

You can initialize a backup manually at any time.

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Run backup**

The length of the backup depends on the size of your backup selection, the data transfer speed and performance of your computer.

> The **Run backup** button will be unavailable until at least one data source is configured for backup. This can be done by following the Configure backup selection steps above.

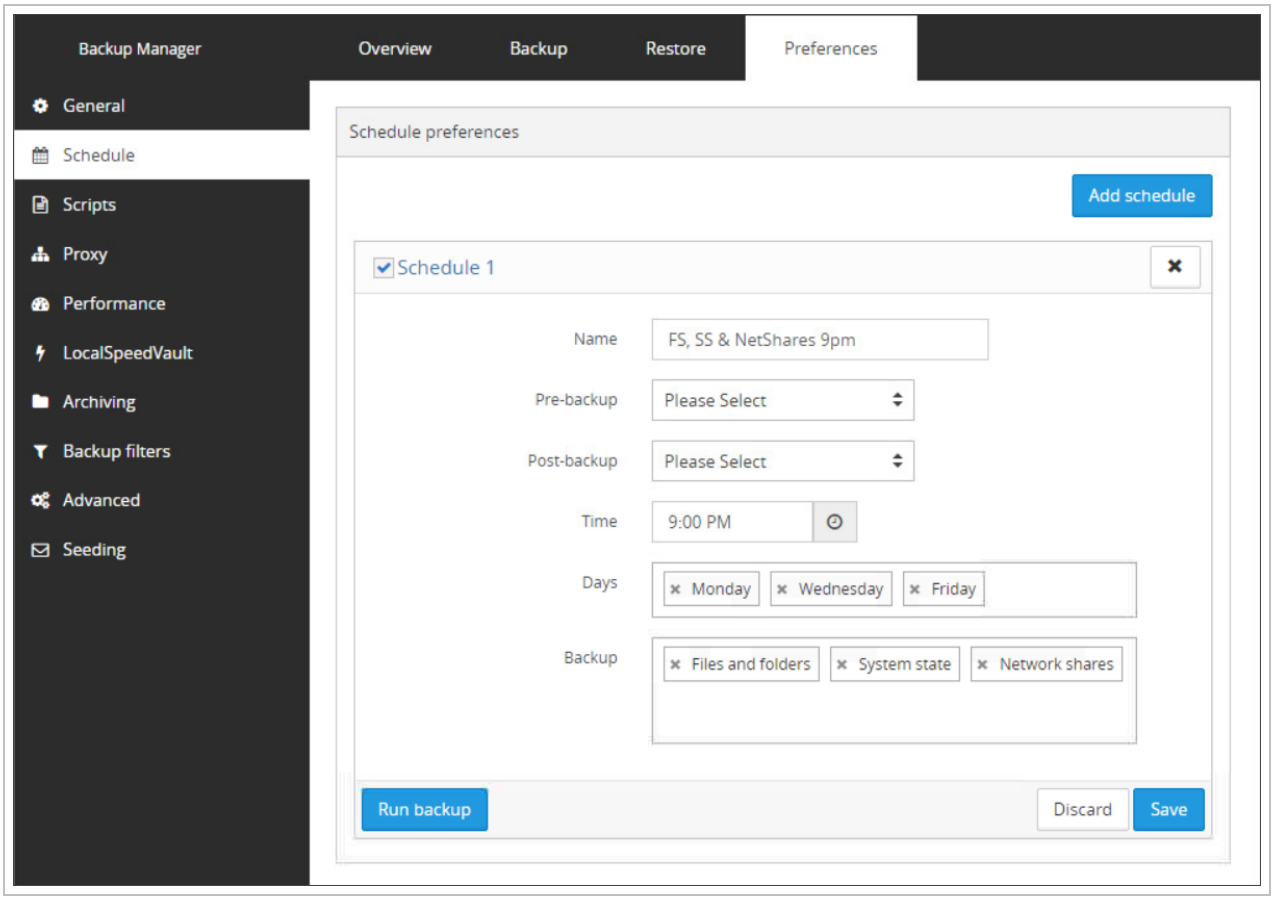
Configure schedule-based backups

The most convenient method of configuring backups is to set up a **backup schedule** which will automatically run the backups without requiring you to intervene.

You can create multiple schedules for each device, for example if you want Files and Folders to run at 9am but you want Files and Folders, System State and MySQL to run at 9pm.

To create a backup schedule:

1. Launch the Backup Manager for the device
2. Open the **Preferences** tab
3. Click **Schedule**
4. Select **Add Schedule**



5. Give the schedule a name - make this something relevant to the backup configured such as "FS, SS & MyS 9pm"
6. Optional - If you have created any scripts, these can be selected to run before the backup (Pre-backup) or after the backup (Post-backup) by selecting them from the given dropdowns.
7. Set the time for the backup to run
8. Choose the days on which you want the backup to run
9. Select the data sources to backup
10. Click **Save**

> If you want to back up a data source regularly, it **must** be configured for backup as well as selected in a schedule or a profile. This can be done by following the Configure backup selection steps above.

If you have multiple schedules listed in this page, you can enable or disable them by ticking the check box beside the name of the schedule. Disabling a schedule does not delete it, but will stop it from running until you manually enable it again.

To edit a schedule, you just need to expand the schedule in question, make the necessary changes and click **Save**.

To delete a schedule, simply click the **X** to the right of the schedule name, you will be prompted to confirm deletion of the schedule - click **Yes**.

> Please note, once a schedule has been deleted, it cannot be undeleted and would have to be recreated manually.

> If you have not configured the backup selection, the schedule will run, but as no data source configuration exists, nothing will be backed up.

Configure frequency-based backups

To enable frequency-based backups on a device, you need to create a **backup profile** with the required backup settings and apply the profile to the device.

See Backup Profiles in Management Console for detailed instructions on configuring profiles.

After the profile has been applied to the device, the new backup settings will be displayed under **Preferences > Schedule** in the Backup Manager. However, all editing is done through the profiles in the Management Console.

Hyper-V Recovery

The method(s) of recovery available to use will be determined by the level at which the Backup was performed:

- Guest Level Backup
- Host Level Backup

Guest Level Recovery

As backups performed at the Guest level, are done *within* the VM, the selection of data backed up is data source driven, therefore recovery can be done in a number of ways:

- **Individual File and Folder Recovery** - this method is done using our **Virtual Drive** tool from the most recent backup session

  > This tool does have **additional requirements relevant to Hyper-V**

- **Data Source Recovery** - this method is done by selecting the data (full data source or selected files and folders) from a specific backup session by Recovering data in Backup Manager
- **Recovery Testing** - the Recovery Testing service is one of our methods of recovery in the Management Console and provides a screenshot as proof that the device is recoverable

  > The virtual machines that are created as part of Recovery Testing are **purged** once the restore is completed and the screenshot taken. This means these restored virtual machines are **not accessible** by the user.

- **Standby Image** - the Standby Image service is one of our methods of recovery in the Management Console and performs continuous restore of a device to a self-hosted environment (Hyper-V or Local VHDX)
- **Recovery Console** - The Recovery Console tool is used for recovery of Windows machines for data ranging from small files and folders selections to full system restores to physical or virtual locations

Individual File and Folder Recovery

The recovery of individual files and folders is done using N-able's Virtual Drive tool.

Requirements

- The Virtual Drive tool must be installed on the VM
- The file system on the computer where the Backup Manager is installed must support the file systems in the virtual machine that is being recovered (for example, NTFS or FAT). This is necessary to be able to expand the contents of the virtual disks
- The virtual disks you are going to recover have been properly backed up (as the **Files and Folders** data source in the Backup Manager)

Host Level Recovery

Host level backup of Hyper-V supports both in-place restores (performed to the **original location**) and restores to a **new location**. In case of an in-place restore, the original Hyper-V machine must be **powered off** at the time of the restore (otherwise it will not be possible to overwrite it).

The following data is available to recover when backups were performed at the Host Level:

- the whole virtual machine
- one of its disks
- files and folders from a virtual disk

Limitations

- It is not possible to restore directly to a CSV, instead we recommend restoring to the host locally and them moving the Virtual Machine over via the Virtual Machine Management Service

Instructions

1. Launch the Backup Manager for the device
2. Switch to the **Restore** tab
3. Select the **Hyper-V** data source from the vertical menu to the left
4. Using the Session date and time picker, select the backup session you want to restore
5. Select the data you want to restore by expanding the file tree and select individual VM's
6. Specify where to restore the selected data: to the original location or to a new one
   a. Enter the target location, if applicable
7. Click **Restore** and wait until the restore process is completed

> You can close Backup Manager in the browser while the recovery is in progress (it will continue in background)

> The speed of recovery depends on a number of factors, such as (but not limited to) the amount of data to restore and the speed of the device's internet connection

Oracle

Backup Manager users can back up Oracle databases powered by **Oracle Database 11g** (Standard and Enterprise editions).

The minimum backup unit is **one** database.

Backup procedure overview

Backup files are created by means of **Oracle Recovery Manager (RMAN)** and saved to the folder you specify (the **backup folder**). A full database backup is performed including the Control File and the Server Parameter File. Backup Manager processes the backup files for secure and efficient transfer and sends them to storage. The files can be cleared immediately after backup or later (depending on your settings).

What's inside:

Oracle backup requirements

Backup Manager must be installed on a **Windows** system. It can be the same machine where Oracle is located or a different one. In the latter case Backup Manager connects to Oracle remotely through **Oracle Client**. You will need to configure some remote connection settings before you start backups (Pre-backup settings for remote access to Oracle).

Read and write access to the backup folder is required.

The backup folder must have a sufficient amount of **free space**. The amount of space you will need depends on the database size and on your retention settings.

For example, if the size of generated *.bck* files during one session is 15 GB and "Retention in backup counts" is set to `1`, you need at least 30 GB of free space.

Please be aware that due to data compression changes the size of the backup folder in the recent versions has increased in comparison to versions 15.9-15.12. However, the amount of data submitted to storage has decreased and is going to decrease further as you continue delta backups.

Pre-backup settings for remote access to Oracle

We recommend installing Backup Manager on the **same machine** where your Oracle database is located. If this is not possible, you need to configure some settings before you start backups.

Step 1. Install Oracle Client

Install Oracle Client to the computer where Backup Manager is running:

1. Download **Oracle Database 11g Release 2 Client** for your system

   To access the installer, visit the Oracle Database Software Downloads page. Under the "Oracle Database 11g Release 2" header, click **See all** next to your version of Windows (32- or 64-bit). A new page will open where you will find the installation file

2. Unpack the archive folder
3. Double click the `setup.exe` file to start the installation
4. Select **Administrator** as the installation type

5. Specify where you want to place Oracle files. Oracle Base is the installation directory, for example `C:\app\username`

   > Software Location is the home directory (inside of Oracle Base), for example: `C:\app\username\product\11.2.0\client_1`

6. Complete the installation as prompted by the installation wizard

When the installation completes, please make sure that Oracle has been configured correctly and all necessary utilities included into the installation package are responsive. This is done using **Command Prompt**.

1. Check Oracle Recovery Manager (RMAN) using the `rman` command, the `RMAN>` response should be returned
2. Use the **Ctrl+C** keyboard shortcut to exit RMAN
3. Check **SQL*Plus** (a basic Oracle Database utility) using the `sqlplus.exe` command. The `Enter user-name:` response should be returned
4. Use the **Ctrl+C** keyboard shortcut to exit SQL*Plus
5. Close Command Prompt

If either of the utilities happens to be unresponsive, you might need to configure your system settings.

1. Right-click the "Computer" icon (or "My Computer" in Windows XP). You can find it on your desktop or in the Start menu
2. Choose **Properties** from the context menu. Click **Advanced system settings > Advanced > Environment Variables**
3. Add a new environment variable - `ORACLE_HOME`. Set its value to the Software Location folder that you specified during the installation
4. Edit the `PATH` variable. Add `%ORACLE_HOME%\bin` to the list of its values. Use a semicolon to separate it from the previous value
5. Restart your computer to apply the new `PATH` value to the system account

Step 2. Connect to the Oracle database

Now it is necessary to connect Oracle Client to your database. To accomplish the task, you will need to edit two files inside of the Software Location folder: *tnsnames.ora* and *sqlnet.ora*. Use Notepad or any other text editing tool. If you do not find the files, you will need to create them manually.

tnsnames.ora

The *tnsnames.ora* file (in the current case `C:\app\USERNAME\product\11.2.0\client_1\network\admin\tnsnames.ora`) must contain the following data:

```
ORCL1 =
(DESCRIPTION =
        (ADDRESS =
                (PROTOCOL = TCP)
                (HOST = 192.168.0.37)
                (PORT = 1521)
        )
        (CONNECT_DATA =
```

```
                (SERVER = DEDICATED)
                (SERVICE_NAME = orcl1.solaris.company.local)
        )
)
```

Please replace the values in bold with the values applicable to your system.

- `ORCL1` is the Oracle TNS alias (network name)
- `192.168.0.37` is the IP address of the Oracle server you are connecting to. A host name can also be used.
- `1521` is the Oracle database Listener port.
- `orcl1.solaris.company.local` is the database service name.

sqlnet.ora

In *sqlnet.ora* (in the current case `C:\app\USERNAME\product\11.2.0\client_1\network\admin\sqlnet.ora`) the `SQLNET.AUTHENTICATION_SERVICES` and `NAMES.DIRECTORY_PATH` parameters should have the following values (there can be other values as well).

```
SQLNET.AUTHENTICATION_SERVICES= (NTS)
NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)
```

When you save the changes, please make sure the connection has been set up correctly. For example, the TNSPING utility can help. Start Command Prompt and run the `tnsping <TNS alias>` command.

```
tnsping ORCL1
```

If the connection is working, you will get the OK response such as `OK (140 msec).`

Step 3. Mount the backup folder as a mapped network drive

Backup Manager requires access to the backup folder on the Oracle server. To provide this access, you need to share the backup folder via the SMB protocol and then map the network drive to the computer on which Backup Manager is installed. The network drive must be mapped for the same account that is used to run Backup Manager.

Backup Manager usually runs under the LocalSystem account. This account is not normally suitable for network access. There are two ways to overcome this limitation.

Option A: Map the network drive for the LocalSystem account

To make the shared folder accessible to the LocalSystem account, you can use the Windows Sysinternals PsExec tool. It helps you map the shared folder as a network drive for the LocalSystem account.

1. Download an installation archive (visit downloads page)
2. Extract the archive to a directory, for example `C:\Pstools`
3. Start Command Prompt. Change the Command Prompt directory to the directory where the installation archive has been unpacked to

```
cd c:\Pstools
```

4. Open another Command Prompt window with the LocalSystem account

```
psexec -i -s cmd.exe
```

5. Run the following command in the newly-created console window:

```
net use o: \\192.168.0.37\oracle\app\oracle\backup /persistent:yes
```

Instead of `\\192.168.0.37\oracle\app\oracle\backup` use the actual path to the shared folder.

Note that the mapped network drive may be invisible to user accounts other than LocalSystem.

Option B: Map the network drive for an administrative user account

Another way to make the shared folder accessible to Backup Manager is by changing the user account under which Backup Manager operates to an account from the Administrators group and mapping the network drive for that account. This option requires fewer settings but in some rare cases it can limit the functionality of Backup Manager.

1. Open the **Start** menu. Start the Services Console *(services.msc)*
2. Right-click the "Backup Service Controller" service. Choose **Properties > Log On**
3. Select the **This account** checkbox. Enter access credentials for the alternative account. Apply the changes
4. Right-click "Backup Service Controller", and choose **Restart** from the context menu

When done, add the network drive:

1. Log in to Windows under the administrator account you have just configured for Backup Manager
2. Start Command Prompt and run the following command:

```
> net use o: \\192.168.0.37\oracle\app\oracle\backup /persistent:yes
```

> Instead of `\\192.168.0.37\oracle\app\oracle\backup` use the actual path to the shared folder.

Oracle backup settings

Oracle server access

Enter access details for the Oracle server. You require an administrator account (SYSDBA). The **Server** field is the TNS alias.

Backup folder access

- If Backup Manager is located on the same machine with your Oracle server, the backup folder is available on a local drive
  - Linux servers: `/export/home/app/oracle/backup`
  - Windows servers: `D:\Export\Home\App\Oracle\Backup`

- If Backup Manager is installed on another machine, specify the path to the network drive that was mounted in step 3 of the pre-backup settings

Retention control settings

You can specify how often the backup folder must be cleaned up.

- **Retention in backups count** – the number of backup sessions that should be completed before the files are deleted
- **Retention in days** – the number of days that should pass before the files are deleted

Enabling backups in Backup Manager

Two types of backups are available:

1. **Schedule-based** backups (run on a certain day/time basis)
2. **Frequency-based** backups (run at a specified interval)

Requirements

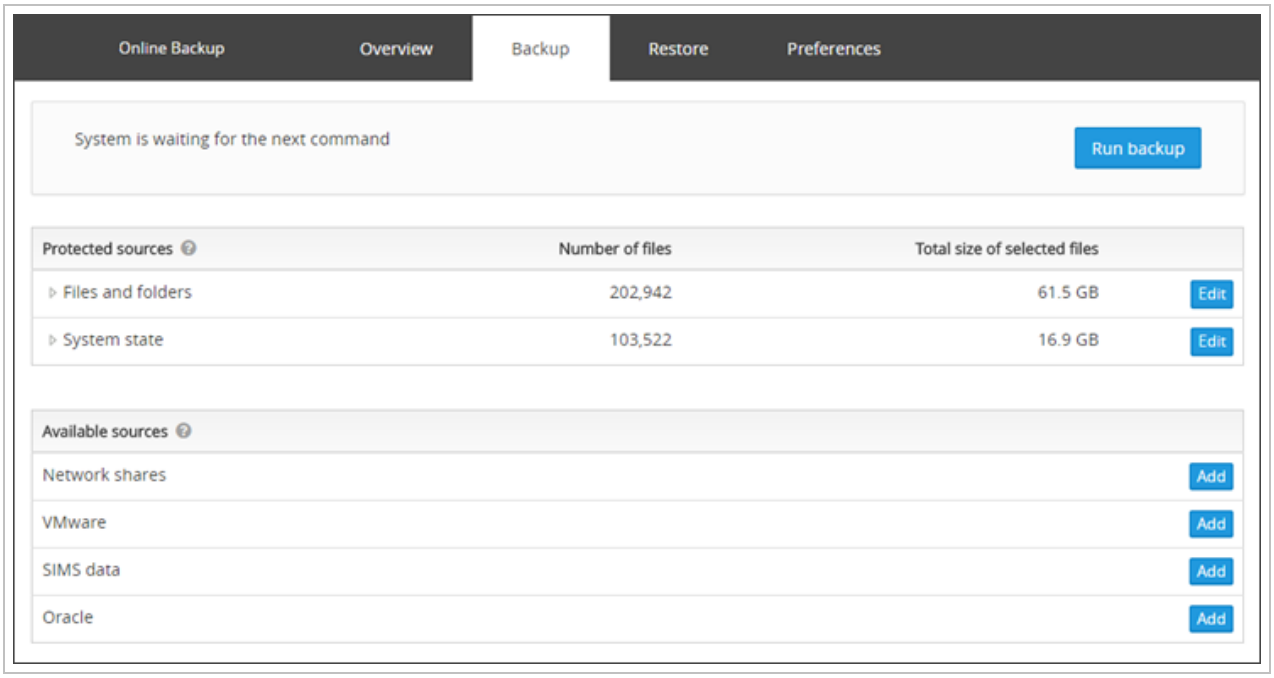
The computer must be online (turned on and must not enter the sleep mode) during backups. If a machine is offline, it will cause the backup to fail to start and will not begin until the machine is turned on or woken up.

If a backup is already running when the machine is turned off, the backup will be aborted. If the machine enters sleep mode while a backup is in progress, the backup will pause until the machine is woken up.

> Be aware that in order to successfully restore using the Virtual Disaster Recovery or Bare Metal Recovery methods, you must back up the full Files and Folders data source (the whole system disk `C:\` or any other depending on the configuration of your computer)

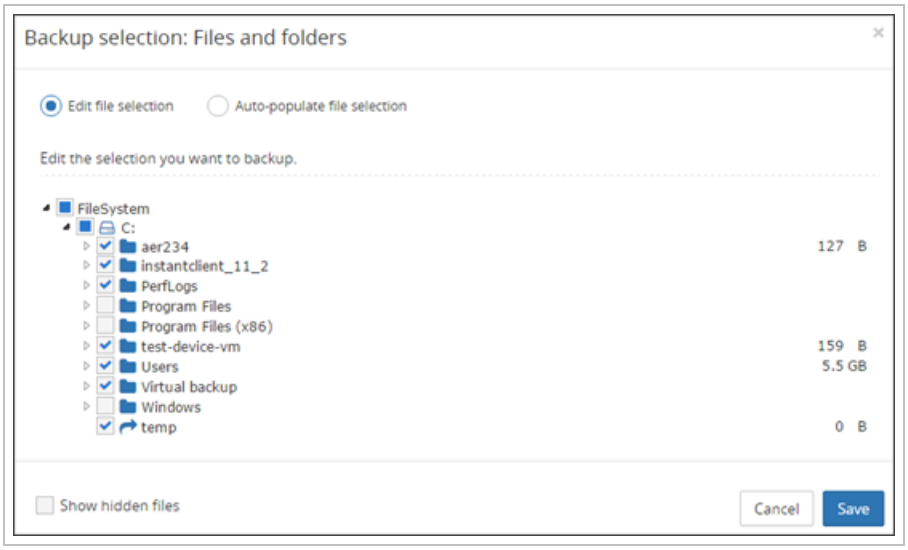
Configure backup selection

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Add** next to the data sources you want to back up



> The below steps detail adding **Files and Folders** for selection, but the process is similar for most data sources. Sources such as Network Shares and VMware require you to supply additional information, such as server details, paths, usernames and passwords.

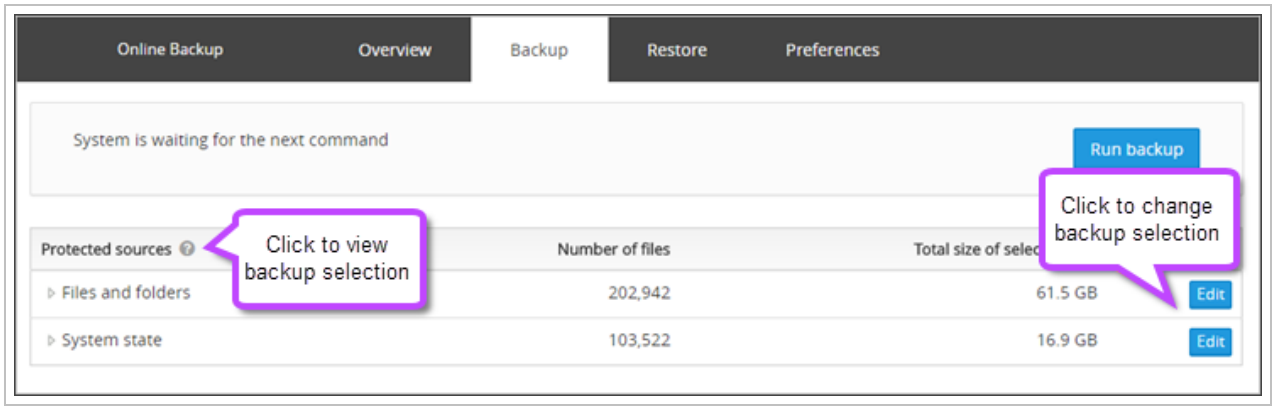
4. Select the files, folders, components (such as data bases, virtual disks, etc.) to back up. You can let the Backup Manager help you choose data for backup using the Automatic File Selection feature



5. Click **Save**

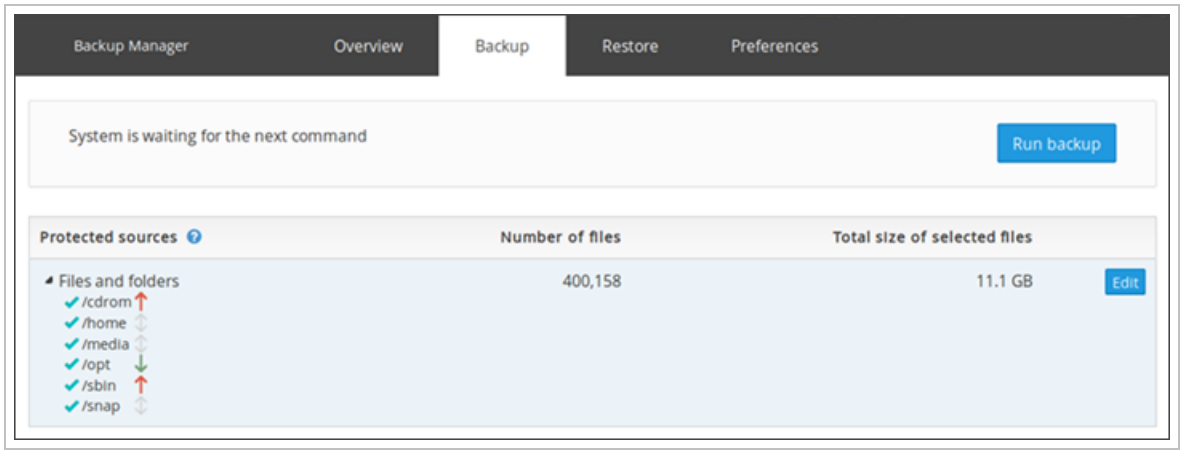
To make sure all necessary data has been included into your backup selection, click on the name of the data source. This will provide a list of the selection made.

Seeing a green tick followed by "\" means the whole data source is selected for backup.



> If you clear your backup selection after at least one backup has been completed, you will be offered to **remove all backup copies** of these files from the Cloud. This means the **entire backup history** of this data source will be deleted. **This action is irreversible.**

If you have selected only part of the disk, you have an option to set the priority of the files in the backup selection.



To do this:

1. Click on the name of the data source
2. Click the arrow to the right of the selection to choose the priority:
   - Click once to get a red up arrow - This indicates a high priority and will be backed up first
   - Click twice to get a green down arrow - This indicates a low priority and will be backed up last
   - Do not click or click to remove a priority to get a grey double-sided arrow - This indicates no priority set and will be backed up between the high and low priority jobs

> Data of the same priority will be completed in alphabetical order.

Start a one-time backup

You can initialize a backup manually at any time.

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Run backup**

The length of the backup depends on the size of your backup selection, the data transfer speed and performance of your computer.

> The **Run backup** button will be unavailable until at least one data source is configured for backup. This can be done by following the Configure backup selection steps above.

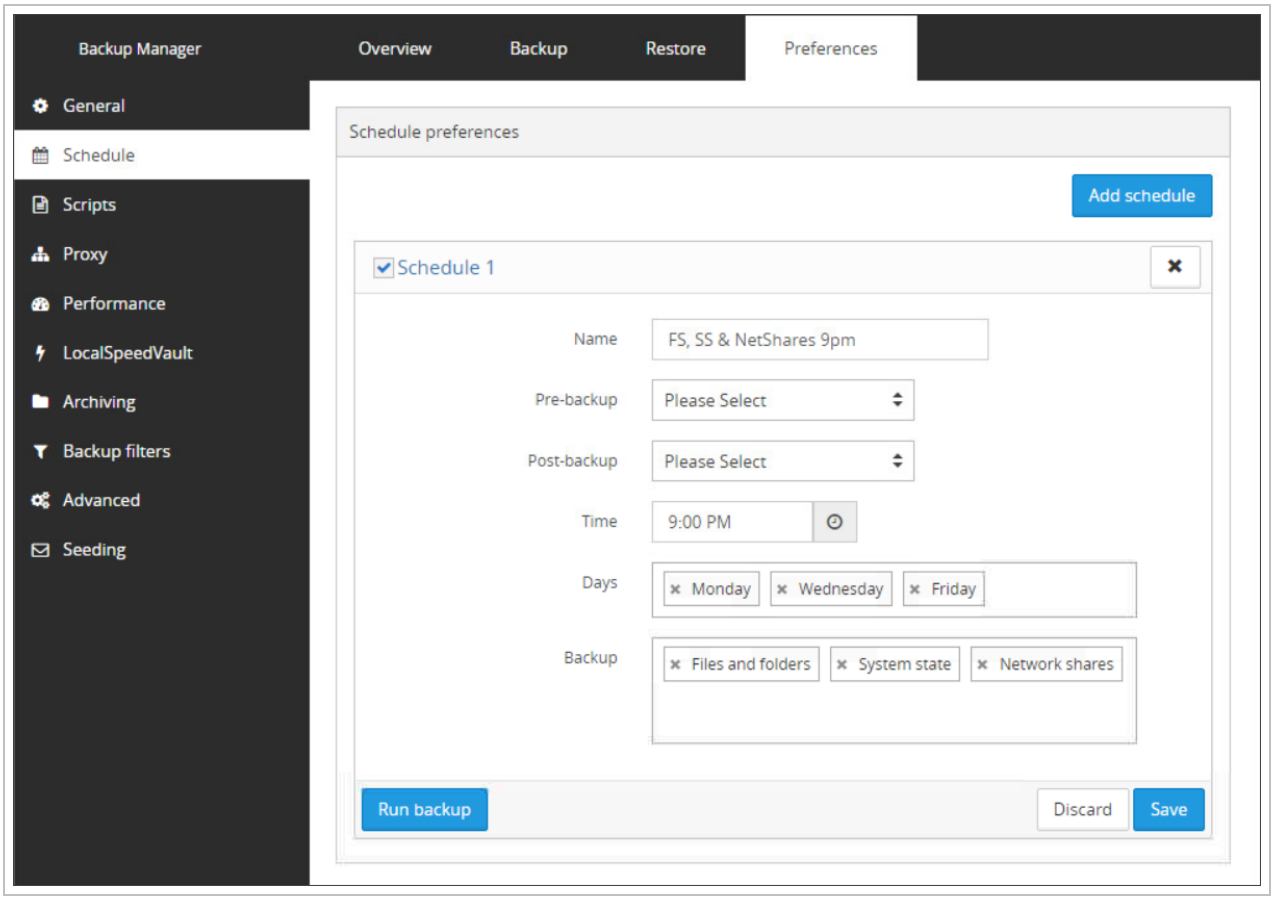
Configure schedule-based backups

The most convenient method of configuring backups is to set up a **backup schedule** which will automatically run the backups without requiring you to intervene.

You can create multiple schedules for each device, for example if you want Files and Folders to run at 9am but you want Files and Folders, System State and MySQL to run at 9pm.

To create a backup schedule:

1. Launch the Backup Manager for the device
2. Open the **Preferences** tab
3. Click **Schedule**
4. Select **Add Schedule**



5. Give the schedule a name - make this something relevant to the backup configured such as "FS, SS & MyS 9pm"
6. Optional - If you have created any scripts, these can be selected to run before the backup (Pre-backup) or after the backup (Post-backup) by selecting them from the given dropdowns.
7. Set the time for the backup to run
8. Choose the days on which you want the backup to run
9. Select the data sources to backup
10. Click **Save**

> If you want to back up a data source regularly, it **must** be configured for backup as well as selected in a schedule or a profile. This can be done by following the Configure backup selection steps above.

If you have multiple schedules listed in this page, you can enable or disable them by ticking the check box beside the name of the schedule. Disabling a schedule does not delete it, but will stop it from running until you manually enable it again.

To edit a schedule, you just need to expand the schedule in question, make the necessary changes and click **Save**.

To delete a schedule, simply click the **X** to the right of the schedule name, you will be prompted to confirm deletion of the schedule - click **Yes**.

> Please note, once a schedule has been deleted, it cannot be undeleted and would have to be recreated manually.

> If you have not configured the backup selection, the schedule will run, but as no data source configuration exists, nothing will be backed up.

Configure frequency-based backups

To enable frequency-based backups on a device, you need to create a **backup profile** with the required backup settings and apply the profile to the device.

See Backup Profiles in Management Console for detailed instructions on configuring profiles.

After the profile has been applied to the device, the new backup settings will be displayed under **Preferences > Schedule** in the Backup Manager. However, all editing is done through the profiles in the Management Console.

Oracle recovery

Backup Manager recovers the backup folder created by Oracle Recovery Manager for backup purposes. The complete database recovery is done using **native Oracle instruments**.

Requirements

Backup Manager can be installed on the same machine where the original Oracle database has been located or a different one. The versions of Windows needn't necessary coincide.

Instructions

To recover the backup folder, do the following:

1. Install Backup Manager on the computer you want to recover the backup folder to
2. Start Backup Manager
3. Click **Restore > Oracle**
4. From the **Session time** list, select the session to recover
5. In the restore tree, select the root of the Oracle database
6. In the **Restore to** field, specify the recovery destination
7. Click **Restore**

The duration of the recovery process depends on the size of your database, the data transfer speed and the performance of your computer.

Complete database recovery

To complete the database recovery process, use Oracle Recovery Manager.

Performing Complete Database Recovery (Oracle support instructions)

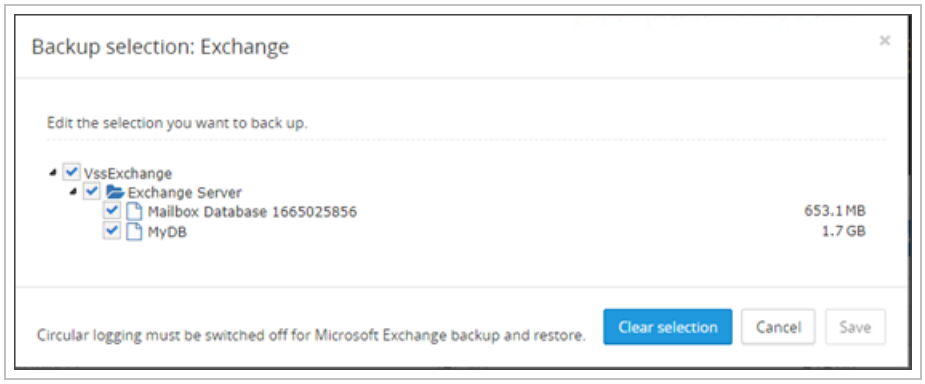
MS Exchange

You can protect MS Exchange against data loss using the Backup Manager.

What's inside:

MS Exchange backup

The minimal backup unit for MS Exchange is a **database**.



> For MS Exchange, database files and logs are backed up. If the backup session completes successfully, the logs on the Exchange server are truncated.

Limitation

- Exchange Database Availability Groups (DAGs) and replica databases are not supported
- Server configuration is not backed up

Preparing the system for backup

Before you start backing up MS Exchange, please make sure your system is properly configured (this is done just once unless the settings get reset in the future).

Disable circular logging

Disable circular logging before you start backing up MS Exchange. This is necessary to keep the database consistent and prevent the loss of recent messages.

1. Start your Exchange management utility:
   - Microsoft Exchange for Exchange 2000 and 2003
   - Exchange Management Console for Exchange 2007
   - Exchange Management Console for Exchange 2010
   - Exchange Admin Center (EAC) for Exchange 2013
2. In the console tree, expand the server object you need:
   - Exchange 2000 and 2003: **System Manager > Server**
   - Exchange 2007: **Server Configuration > Mailbox**
   - Exchange 2010: **Organization Configuration > Mailbox**
   - Exchange 2013: **Servers > Databases**

3. Open the properties of the storage group you are going to back up:
   - In the Microsoft Exchange and Exchange Management Console, right-click the storage group and choose **Properties** from the context menu
   - In the Exchange Admin Center, click the storage group and then click the **Edit** icon above
4. Deselect the **Enable circular logging** checkbox (if it is selected)
5. Click to apply the changes

Check vssadmin list writers

1. Open the Start menu. Run Command Prompt *(cmd.exe)*
2. Execute the following command:

```
vssadmin list writers
```

3. When the list of writers is ready, find the "Microsoft Exchange Writer" entry. Make sure its state is "Stable" and "Last error" is set to "No error"

Make sure the databases are mounted

1. Start your Exchange management utility
2. In the console tree, expand the server object you need:
   - Exchange 2010: **Organization Configuration > Mailbox**
   - Exchange 2013: **Servers > Databases**
3. In the work pane, check if the status of the databases from this mailbox server is "Mounted"

MS Exchange recovery

Please follow instructions for your recovery method:

- Preparation
- Restore to a local drive

If unsure which of the methods suits you better, please check the list of deletion and recovery options below.

Deletion and recovery options in MS Exchange

For Exchange mailbox and item recovery, several scenarios are available. In the case of a complete server or database failure, you may use Backup Manager Exchange restores or Virtual Disaster Recovery. For only restoring a mailbox or some items, the Exchange Server has several built-in features.

To provide reliable Exchange Server protection and quick recovery options, a combination of Backup Manager Exchange backup/restore and the Exchange built-in features can be used.

Since Exchange Server 2010 SP1, Microsoft has changed the architecture for item deletion and recovery. Deleted items remain in the database within the configured retention period for **quick recovery**. Using the **Exchange Single Item Recovery** option, it is also possible to recover accidentally or intentionally deleted items.

To understand the options for recovery, let us first explain different Exchange Server recovery locations and deletion types:

Term	Definition
Deleted Items folder	This visible folder contains deleted items (normal deletion). The end user can move them back by himself.
Recoverable Deletions folder	After the **Deleted Items** folder is emptied, items move to this hidden folder. This folder also contains the Shift-Deleted items. The end user can move them back by himself.
Recoverable Purges folder	Even from the **Recoverable Deletion** folder, a user can purge items. When the **Single Item Recovery** option is enabled, purged items move to this hidden folder.
Recoverable Versions folder	When the **Single Item Recovery** option is enabled, the original email will be stored in this hidden folder when a user edits it.
Recovery Database	In the case, an item is not recoverable using the previous methods, items or even a mailbox can be restored using the **Recovery Database**. Each Exchange database from a successful backup session can mount as Recovery Database, and restore items or mailboxes using the Microsoft tools.

The Recoverable folder structure is the enhanced version of the Exchange 2007 Dumpster. For Exchange 2010 and greater versions this structure is called **Dumpster v2**. The diagram below is a good summary of the flow for Exchange deleted items and this Recoverable Items structure.

Deleted items retention period

For the deleted item locations, described in the previous section, the default retention period differs. The Exchange Administrator can configure these retentions:

#	Location	Default retention
1	**Deleted Items** folder	Default unlimited. Using an Exchange rule or Outlook setting, it is possible to configure automatic cleaning for this folder (Empty the Deleted Items folder upon exiting).
2	**Recoverable** Deletions folder	This retention is configured per Exchange mailbox database, the default value is 14 days. For an on-premises Exchange server, there is no maximum. For recovery, a good starting value is 30 or 60 days. With this retention, the database grows by only a few percent.
3	**Recoverable Purges** folder	By default, the Single Item Recovery feature is disabled for an on-premises Exchange server. For quick recovery, best practices is enabling this feature. Retention for this folder is the same as for the **Recoverable Deletion** folder.
4	**Recoverable Versions** folder	By default, the Single Item Recovery feature is disabled for an on-premises Exchange server. For quick recovery, best practices is enabling this feature. Retention for this folder the same as for the **Recoverable Deletion** folder.
5	Recovery Database	In case the restore of an item or mailbox is required outside the configured retention, an Exchange database in the Backup Manager retention can be mounted as an Exchange Recovery Database. The Exchange database can be mounted directly, without restore, using the Virtual Drive tool and for speed the LocalSpeedVault feature.

Conclusion

With the Exchange deleted items retention set to at least 30 days and the Single Item Recovery feature enabled, restore of Exchange items can be processed in most cases **without the Recovery database**. Database recovery is only required in case of database or server corruption, or other disaster.

MS Exchange mailbox and single item recovery

Exchange Single Item Restore is a built-in Exchange server feature, supported by Microsoft. See the Microsoft TechNet site for a complete description.

Before beginning recovery of mailboxes or single items, a few preparatory steps must be carried out:

- Step 1: Configure Retention
- Step 2: Enable Single Item Restore
- Step 3: Create User

Preparation

The following Exchange PowerShell commands are **examples** to prepare the Exchange server to provide quick Exchange Item Restore using the Microsoft built-in features.

Use the following Exchange PowerShell commands to prepare the Exchange server for single item recovery:

Step 1: Configure Retention

These commands configure the Exchange deleted item retention period to 60 days for all Exchange databases.

> This retention is used for recovery from the Recoverable folder tree (Dumpster).

```
Get-MailboxDatabase | Set-MailboxDatabase -DeletedItemRetention "60.00:00:00"
```

```
Get-MailboxDatabase -Status| FT Name, Server, DeletedItemRetention, LastFullBackup
```

Step 2: Enable Single Item Restore

These commands enable Single Item Restore (SIR) for all existing user mailboxes. It is not possible to force this setting for newly created mailboxes, therefore SIR needs to be set for each new mailbox.

With SIR enabled, recovery from the Recoverable Purges & Versions folders is available.

```
Get-Mailbox -filter {(recipienttypedetails -eq "usermailbox")} | where
{!$_.SingleItemrecoveryEnabled} | Set-Mailbox -SingleItemRecoveryEnabled $True
```

```
Get-Mailbox | FT Name, RetainDeletedItemsFor, SingleItemRecoveryEnabled
```

Step 3: Create User

These commands create an Exchange Security Group for the “Mailbox Import Export” role and adds the user Administrator to this role.

```
New-RoleGroup "Mailbox Import-Export Management" -Roles "Mailbox Import Export"
Add-RoleGroupMember "Mailbox Import-Export Management" -Member Administrator
```

```
Get-RoleGroupMember "Mailbox Import-Export Management"
```

> To make use of this role, restart a new Exchange PowerShell instance once complete.

Instructions to Restore

There are two methods of recovery that can be used for Mailbox and Single Item Restores:

- Recovery using the Deleted Item folder
- Recovery using the "Recover deleted items" tool
- Single Item Recovery (SIR) using the Recoverable Folder structure (Dumpster)

Recovery using the Deleted Item folder

When a user deletes a mail item, this results in moving the item to the **Deleted Items** folder. The Deleted Items folder is visible in both Outlook and Outlook Web Access, items can be moved back by the user.

This self-service item recovery is a standard feature of Outlook Web Access and Outlook for Windows, see also the Microsoft Office support article.

Recovery using the "Recover deleted items" tool

In cases where a deleted item is no longer in **Deleted Items** folder anymore but is still within the Exchange retention, the user can restore the item using **Recover deleted items**.

This feature is available in Outlook Web Access and Outlook for Windows.

To use the Recover Deleted Items tool:

1. Navigate to the **Deleted Items** folder
2. In the top menu ribbon, switch to the **Folder** tab
3. Select **Recover Deleted Items** from the Clean Up section
4. Locate the missing items
5. Select **Ok** to begin recovery

Single Item Recovery (SIR) using the **Recoverable Folder** structure (Dumpster)

When enabled, the Exchange Administrator can recover items or mailboxes using the **Recoverable Folder** structure (Dumpster), for more information, see Microsoft TechNet.

The following steps explain how to use the Microsoft Single Item Recovery. This feature doesn't support restoring the items from the **Recoverable Items** folder structure direct in the original mailbox. Therefore, some extra steps are required:

- Restore the items from the **Recoverable Items** folder to a temporary mailbox
- Export this folder structure to a PST export file
- Import this PST file to the original mailbox

Restore recoverable items using a temporary PST file

The following example parameters are used in the below example:

Parameter	Value
Exchange Administrator username / mailbox	Administrator
Recovery for the Recoverable Items tree for mailbox	Kate James
Folder used for recovered items on target mailbox	RecoveredItems
Temporary PST file for export	\\<server_name>\PST\KateJames.pst

You **must** replace these example values with those relevant to your recovery

1. Execution of the PowerShell commands for recovery is only available for an Exchange Administrator, add this user to the Exchange Security group "Organization Management"
2. The temporary PST file, used for export/import the recovered items, will be created in a shared folder. The Exchange security group "Exchange Trusted Subsystem" requires full read/write permission on this shared folder

3. Use Exchange PowerShell to restore Recoverable Items folder (Dumpster):

> The following command is to restore mailbox "**Kate James**", to the **Administrator** mailbox, sub-folder **RecoveredItems**:

```
Search-Mailbox -Identity "Kate James" -TargetMailbox Administrator -
TargetFolder RecoveredItems -SearchDumpsterOnly

RunspaceId       : 14423653-59f0-4482-b057-9c0d1ee749dc
Identity         : sales.local/UsersExchange/Kate James
TargetMailbox    : sales.local/Users/Administrator
Success          : True
TargetFolder     : \RecoveredItems\Kate James-2-3-2017 14:21:14
ResultItemsCount : 8
ResultItemsSize  : 2.567 MB (2,691,827 bytes)
```

> This example recovers **all** items in the Recoverable Items folder. Using a search query, only specific items can be selected. For example:
>
> ```
> -SearchQuery "from:Marjorie"
> -SearchQuery "subject:acquisition"
> ```

4. Export temporary folder RecoveredItems from mailbox Administrator to the PST export file. The export request is queued and processed by the Exchange Mailbox Replication service (MRS). After completion, cleanup this request:

```
New-MailboxExportRequest -Mailbox Administrator -SourceRootFolder
"RecoveredItems" -FilePath \\<servername>\PST\KateJames.pst

---- // ------------ // ----------- // ---------------
MailboxExport // Completed // Administrator // 100

Get-MailboxExportRequest -Status Completed | Remove-MailboxExportRequest
```

> Microsoft TechNet, New-MailboxExportRequest:

5. Import the temporary PST file in the original target mailbox "Kate James":

```
New-MailboxImportRequest -FilePath \\localhost\PST\KateJames.pst -Mailbox
"Kate James" -TargetRootFolder "RecoveredItems"

Name // Mailbox // Status
---- // ------- // ------
MailboxImport1 // sales.local/UsersExchange/Kate James // Queued

Get-MailboxImportRequest | Get-MailboxImportRequestStatistics
Name // StatusDetail // TargetAlias // PercentComplete
---- // ------------ // ----------- // ---------------
MailboxImport // Completed // kjames // 100

Get-MailboxImportRequest -Status Completed | Remove-MailboxImportRequest
```

> Microsoft TechNet, New-MailboxImportRequest:

After the PST import, the complete **Recoverable Items** folder structure is restored in the original mailbox, "Kate James". It is then possible to search the missing mails in this folder structure and move them back to the original folder.

Alternative solutions

In the case where item or mailbox recovery using the Microsoft methods is not possible, restore of a database backup is required. Using the Virtual Drive tool, it is possible to mount the Exchange database as Recovery Database directly from the backup storage location.

MS Exchange database recovery

To protect a Microsoft Exchange Server against data loss, Cove Data Protection (Cove) offers two methods of data protection:

- Microsoft 365 domain protection of the Exchange service. See Microsoft 365 protection for details
- MS Exchange as a data source using Backup Manager

Exchange database protected by using the Exchange data source via Backup Manager can be recovered in two ways:

1. **Restore to a local drive** and mount the database as Recovery database

   > Use this option to restore **specific items or mailboxes** from a protected Exchange database from a previous backup session, within the Backup Manager retention time or from an archive session

2. **In-place restore** when the original database is replaced in the still available storage group

   > This is useful only when the recovery of the **complete Exchange database** is required, for example in the case of a disaster or corruption

Restore to a local drive

Requirements and recommendations

- Backup Manager **must** be installed on the same machine where the Exchange Server is running
- (Optional) The Virtual Drive can be used to mount the Exchange database
- (Optional) The LocalSpeedVault may also be used to improve the performance

Instructions/example

Restore mailbox data using an Exchange recovery database is supported by Microsoft. This procedure is for the Exchange versions 2010 SP1, 2013 and 2016 or similar, see the Microsoft TechNet site for full information.

> The step-by-step example below is based on information from Microsoft at the time of documentation. Please note that these instructions may differ slightly, depending on a number of factors

The following instructions use these example parameters:

Parameter	Value
Exchange Administrator username/mailbox	Administrator
Recovery mailbox for recipient	Kate James
Folder used for recovered items on target mailbox	RecoveredItems
Exchange database name for this mailbox	MailboxDB01
Database transaction log file prefix	E00
Local drive for restored database	D:\Restored
Exchange Recovery database name	RecoveryDB

> You **must** replace these example values with those relevant to your recovery

1. Restore the Exchange database using the Backup Manager to a local drive:
   a. Start the Backup Manager
   b. Navigate to the **Restore** tab, then select **Exchange** from the list of data sources
   c. Select the required session date and time
   d. In the recovery selection, select the whole storage group (this is necessary to complete the recovery)
   e. Select **Restore to new location**
   f. Type or browse to the location you wish to restore the database to
   g. Click **Restore** to begin the recovery process
2. Once the recovery is complete, close the Backup Manager and proceed to the next step

3. Check Exchange database shutdown state. For an Exchange online backup, the saved database will have the expected **Dirty Shutdown state**. In this example, the transaction log files 0x3f71-0x3f71 are required for recovery.

   See also this Microsoft Blog post for more information

```
ESEUTIL /MH "D:\Restored\Exchange Server\MailboxDB01\File\MailboxDB01.edb"
Created ulVersion: 0x620,20
DB Signature: Create time:06/24/2016 21:28:41.584
cbDbPage: 32768
dbtime: 14923861 (0xe3b855)
State: Dirty Shutdown
Log Required: 16241-16241 (0x3f71-0x3f71)
Log Committed: 0-16242 (0x0-0x3f72)
```

4. Bring the Exchange database to the **Clean Shutdown state**

```
ESEUTIL /R E00 /D "D:\Restored\Exchange Server\MailboxDB01\File" /L
"D:\Restored\Exchange Server\MailboxDB01\Logs" /S "D:\Restored\Exchange
Server\MailboxDB01\Logs"
Initiating RECOVERY mode...
Logfile base name: e00
Log files: D:\Restored\Exchange Server\MailboxDB01\Logs
System files: D:\Restored\Exchange Server\MailboxDB01\Logs
Database Directory: D:\Restored\Exchange Server\MailboxDB01\File
Performing soft recovery...
Restore Status (% complete)
0    10   20   30   40   50   60   70   80   90  100
|----|----|----|----|----|----|----|----|----|----|
....................................................
Operation completed successfully in 0.891 seconds.
```

5. Create an Exchange recovery database for the restored database and transaction log files. Use the **Exchange Management PowerShell** to execute these commands:

```
New-MailboxDatabase -Recovery -Name RecoveryDB -Server $env:COMPUTERNAME -
EdbFilePath "D:\Restored\Exchange Server\MailboxDB01\File\MailboxDB01.edb"  -
LogFolderPath "D:\Restored\Exchange Server\MailboxDB01\Logs"
Name // Server // Recovery // ReplicationType
---- // ------ // -------- // ---------------
RecoveryDB // ServerName // True // None
```

6. Mount the Exchange Recovery database and check the state:

```
Mount-Database -Identity RecoveryDB
Get-MailboxDatabase -status | FT name,server,recovery,mounted,LastFullBackup
Name // Server // Recovery // Mounted // LastFullBackup
---- // ------ // -------- // ------- // --------------
MailboxDB1 // ServerName // False // True // 8-3-2017 10:09:48
RecoveryDB // ServerName // True // True
```

7. Get list of mailboxes in the mounted RecoveryDB database

```
Get-MailboxStatistics -Database RecoveryDB | ft -auto
DisplayName // ItemCount
----------- // ---------
Teri Snow // 55
Ernesto Stephens // 57
Kate James // 63
```

8. Restore mailbox for Kate James, all restored items are saved in the original Kate James mailbox, in the subfolder **RecoveredItems**. The restore request is queued and processed by the Exchange Mailbox Replication service (MRS). After completion, cleanup this request

```
New-MailboxRestoreRequest -SourceDatabase RecoveryDB -SourceStoreMailbox
"Kate James" -AllowLegacyDNMismatch -TargetMailbox "Kate James" -
TargetRootFolder RecoveredItems
Get-MailboxRestoreRequest
Name // TargetMailbox // Status
---- // ------------- // ------
MailboxRestore // sales.local/UsersExchange/Kate James // Completed
et-MailboxRestoreRequest -Status Completed | Remove-MailboxRestoreRequest
```

After the mailbox restore, the complete structure for the mailbox Kate James is restored in the target mailbox. The user can search the missing emails or other items in this folder structure and move them back to the original folder.

See the Microsoft documentation for more information, like specific selection for the restore request.

In-place restore

Requirements

- Backup Manager **must** be installed on the same machine where the Exchange Server is running
- The original data stores must be available

Important

During the in-place Exchange recovery all the previous data gets overwritten except for **transaction logs**. Logs that have not been backed up are added to the recovered version.

> The original storage groups must be available (even if they are corrupted).

Instructions

To recover MS Exchange databases to the original location:

1. Start the Backup Manager
2. Navigate to the **Restore** tab, then select **Exchange** from the list of data sources
3. Select the required session date and time
4. In the recovery selection, select the whole storage group (this is necessary to complete the recovery)
5. Select **Restore to original location**
6. Type or browse to the location you wish to restore the database to
7. Click **Restore** to begin the recovery process

MS Exchange mailbox recovery from the Virtual Drive

You can use the Virtual Drive in combination with Microsoft tools to recover deleted MS Exchange mailboxes and storage groups. The feature is not suitable for the recovery of Public Folder data.

Pre-recovery instructions

Step 1: Confirm Requirements and Install the Virtual Drive

Before beginning, check you meet the Virtual Drive Requirements and Permissions.

Install the Virtual Drive tool if it is not installed yet.

Step 2: Check the status of the mailbox database

Check the status of the mailbox database on the Virtual Drive. This is done using `eseutil.exe` (Extensible Storage Engine Utility), a program included into all MS Exchange server installations.

1. Click the **Start** menu
2. Open the **Command Prompt** (CMD) as an administrator
3. Run the following command:

```
eseutil /mh "<EDB_file_path>"
```

> Where `<EDB_file_path>` is the location in the Virtual Drive of the backed up mailbox database

For example:

```
eseutil /mh "B:\Exchange\2016-07-26\Exchange Server\First SG\Mailbox
Database\Mailbox Database.edb"
```

Check the following fields in the response:

- **State**: If the state of the mailbox database is `Dirty Shutdown`, you must change it to the clean shutdown state
  - See Step 4: Put the database into the clean shutdown state (if applicable) for instructions
- **Log required**: If the value is `0-0`, it means that no logs are required so the database can be safely put into the clean shutdown state. Otherwise you will get the range of required log files (note that the names are in hexadecimal numbers). In that case please refer to Step 3

Step 3: Check the state of log files (if applicable)

If the **Log required** field had the name of a log file, make sure that file is available:

1. Click the **Start** menu
2. Open the **Command Prompt** (CMD) as an administrator
3. Run the following command:

   ```
   eseutil /ml "<log_file_path>"
   ```

> Where `<log_file_path>` is the location in the Virtual Drive of the log file

For example, if the response is `111-111`, this means that just 1 log file is required ("6F" in the decimal format), so the command would read:

```
eseutil /ml "B:\Exchange\2016-07-26\Exchange Server\First SG\Logs\E000000006F.log"
```

Ideally, you will return the list of log files with the state of "OK" next to each one.

1. Find the log files required for the clean shutdown
2. Copy all other logs (especially logs created before the required logs) to a temporary folder on your hard drive, for example to `D:\Exchange\2016-07-26\Exchange Server\First SG\Logs`

   > Please be aware that the logs will be copied (restored) from the cloud, so the process can take a little longer that regular copying/pasting from a local drive

Step 4: Put the database into the clean shutdown state (if applicable)

If the state of the mailbox database is "Dirty Shutdown", you must change it to the clean shutdown state to make it fully functional as a single EDB file:

1. Click the **Start** menu
2. Open the **Command Prompt** (CMD) as an administrator

3. Run the following command:

```
eseutil /r <Checkpoint_file_name> /s "<Log_folder_path>"; /l ";<Log_folder_
path>" /d "<EDB_folder_path>"
```

   Where the parameters mean:

   - `/r` - Puts the database into recovery mode
   - `<Checkpoint_file_name>` - Enter the name of the checkpoint file `(*.chk)` automatically created by MS Exchange e.g. `E00`
   - `<Log_folder_path>` - Enter the location of the folder where transaction log files for the current mailbox database are stored. You can identify transaction logs by their names and extensions, for example the filename may be something like `E0000000060` and the extension will be `.log`
   - `<EDB_folder_path>` - Enter the location where the primary database file is stored. This coincides with the log folder in some versions of MS Exchange, for example in Exchange 2010

   Here is an example:

```
eseutil /r E00 /i /a /s "D:\Exchange\2016-07-26\Exchange Server\First
SG\Logs\" /l "D:\Exchange\2016-07-26\Exchange Server\First SG\Logs\" /d
"B:\Exchange\2016-07-26\Exchange Server\First SG\Mailbox Database\"
```

4. Ensure the database state has changed to "Clean Shutdown" by running the following command:

```
eseutil /mh "<EDB_file_path>"
```

Recovery instructions

MS Exchange 2007 recovery

MS Exchange 2007 is recovered with the help of recovery storage groups. They are created by Microsoft Exchange Troubleshooting Assistant (`extra.exe`).

1. Click the **Start** menu
2. Open the **Command Prompt** (CMD) as an administrator
3. Launch `extra.exe`
4. In the **Welcome** screen, click **Select a task**
5. From the **Related Functions** list, select **Database Recovery Management**
6. Fill out server and user information to establish connection to the Exchange server
7. Under **Manage Recovery Storage Group**, click **Create a recovery storage group**
8. Select the storage group that contains the database
9. Specify a path to the EDB database on the "B:" drive and click **Create the recovery storage group**
10. In the results screen, click **Go back to task center**
11. Under **Manage Recovery Storage Group**, select **Mount or dismount databases in the recovery storage group**
12. Select the database you want to restore and click **Mount selected database**
13. In the results screen, click **Go back to task center**

14. Under **Manage Recovery Storage Group**, select **Merge or copy mailbox contents**
15. Click **Gather merge information**
16. Select the mailbox and click **Perform pre-merge tasks**
17. Select the mailboxes you want to merge, click **Save**
18. Hold on till the backup version is merged with the production database

> Recovered mailboxes can be merged only with existing mailboxes. If you are recovering a **deleted mailbox**, it is necessary to create a new mailbox first. It can have the same name as the original.
>
> The GUID of the new mailbox will differ from the GUID of the original mailbox. That is why the automatic merging described above will not work. You will need to mount the recovered contents to the new mailbox manually.

MS Exchange 2010 recovery

MS Exchange 2010 is recovered with the help of a recovery database. It is created by the Exchange Management Shell.

1. Launch the Exchange Management Console. Open the Start menu. Under **Microsoft Exchange Server 2010**, click **Exchange Management Shell**
2. Run the following command:

   ```
   New-MailboxDatabase -Recovery -Name <Recovery_database_name> -Server
   "<Exchange_server_name>" -EdbFilePath "<EDB_file_path>" -LogFolderPath "<Log_
   folder_path>"
   ```

   Here is a brief explanation of the parameters to submit.

   - `New-MailboxDatabase` is a cmdlet that creates a mailbox database object in the database container in Active Directory (view Microsoft instructions)
   - `-Recovery` - specifies that the new database will be a recovery database
   - `<Recovery_database_name>` - the name of the new database (must be unique within your organization)
   - `<Exchange_server_name>` - the name of the server the new database will be created on
   - `<EDB_file_path>` - the path to the restored mailbox database file
   - `<Log_folder_path>` - the path to the folder that will be used for transaction log files

   For example:

   ```
   New-MailboxDatabase -Name RecoveryDatabase01 -Server TestExchange-2010 -
   Recovery -EdbFilePath "B:\Exchange\2016-07-26\Exchange
   Server\V14\Mailbox\DB\DB01.edb" -LogFolderPath "D:\Exchange\2016-07-
   26\Microsoft\Exchange Server\V14\Mailbox\DB\Logs"
   ```

3. In the Exchange Management Console, go to **Organization Configuration > Mailbox > Database Management**. Select the recovery database that you've just created and click **Mount Database**
4. In the Exchange Management Shell, get the list of mailboxes in the recovery database:

   ```
   Get-MailboxStatistics -Database <Recovery_database_name>
   ```

5. To restore one of the mailboxes from the recovery database, use the following command:

```
Restore-Mailbox <Mailbox_name> -RecoveryDatabase <Recovery_database_name>
```

6. Repeat the command for all other mailboxes that you want to restore

Post-recovery instructions

MS Exchange 2007

Dismount the database and remove the recovery storage group.

MS Exchange 2010

Dismount the recovery database and remove it from the Exchange Management Console.

MS SharePoint

With Backup Manager, you can set up backup and recovery service for content management systems powered by Microsoft SharePoint.

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

What's inside:

MS SharePoint backup requirements

Availability

The feature is available on the **server versions** of Windows. The whole SharePoint Server is included into the backup selection. You can view the sites inside.

Supported versions

We support the following MS SharePoint versions: 2007, 2010, 2013 and 2016.

Host system

1. Backup Manager must be installed on the same SharePoint server that you want to back up
2. SQL databases for SharePoint must be located on the same SharePoint server that you want to back up. Multi-tier configuration is not supported
3. The names of SQL databases for MS SharePoint must not start or end with a space (this is a Microsoft limitation)

Free space

There must be a sufficient amount of free space in the VSS Shadow Copy storage area.

This is because MS SharePoint backups depend on **VSS snapshots**. When a backup session completes, snapshots are automatically deleted.

VSS writers

MS SharePoint backups depend on 3 VSS writers:

1. **SqlServerWriter**
2. **SharePoint Services Writer** (in MS SharePoint 2013, it is disabled by default and needs to be registered – learn more)
3. **OSearch VSS Writer**

You can check the availability of these writers through a system console, for example Command Prompt:

```
vssadmin list writers
```

All the writers must be listed in the response. This is crucial for successful backups.

Learn more about the VSS writers for MS SharePoint backups

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

Enabling backups in Backup Manager

Two types of backups are available:

1. **Schedule-based** backups (run on a certain day/time basis)
2. **Frequency-based** backups (run at a specified interval)

Requirements

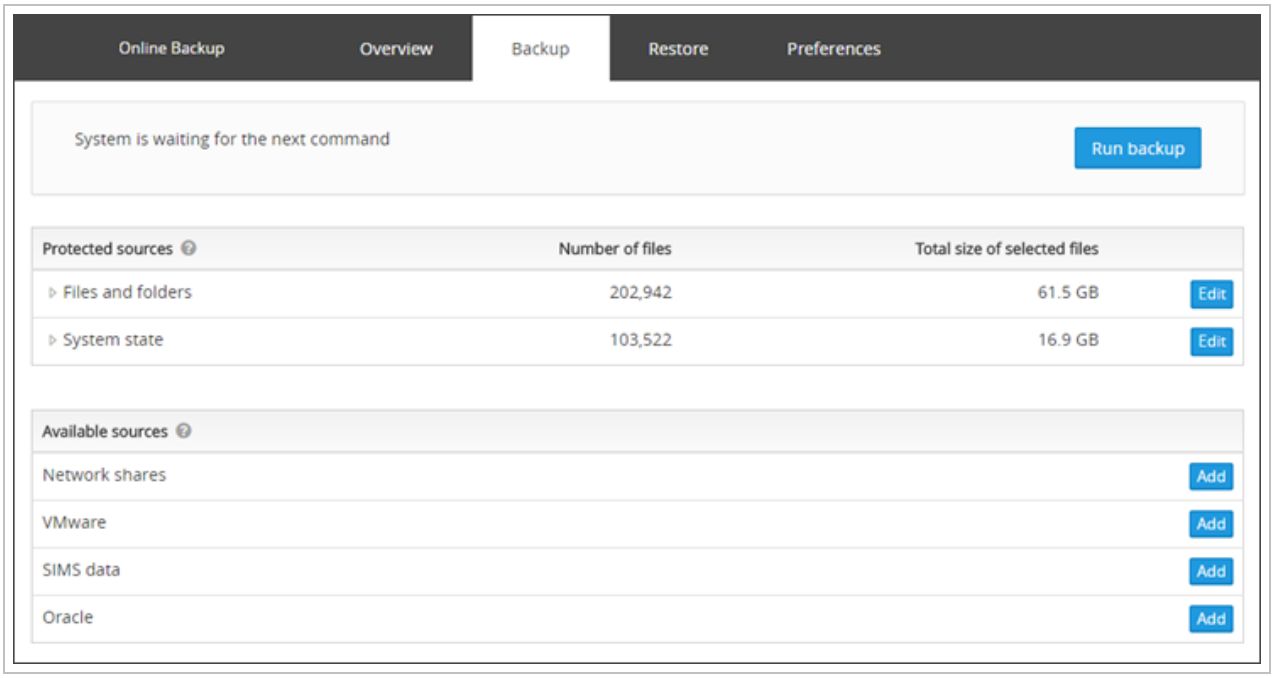
The computer must be online (turned on and must not enter the sleep mode) during backups. If a machine is offline, it will cause the backup to fail to start and will not begin until the machine is turned on or woken up.

If a backup is already running when the machine is turned off, the backup will be aborted. If the machine enters sleep mode while a backup is in progress, the backup will pause until the machine is woken up.

> Be aware that in order to successfully restore using the Virtual Disaster Recovery or Bare Metal Recovery methods, you must back up the full Files and Folders data source (the whole system disk `C:\` or any other depending on the configuration of your computer)

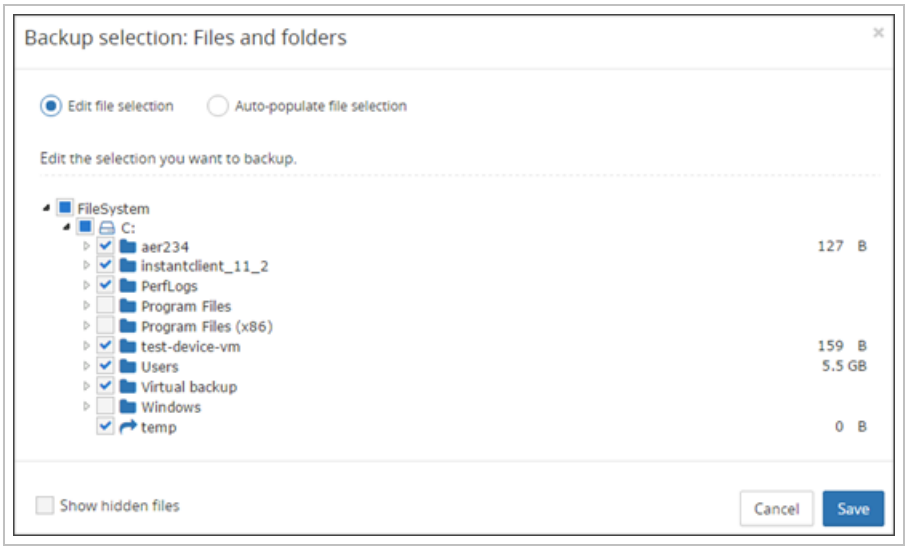
Configure backup selection

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Add** next to the data sources you want to back up



> The below steps detail adding **Files and Folders** for selection, but the process is similar for most data sources. Sources such as Network Shares and VMware require you to supply additional information, such as server details, paths, usernames and passwords.

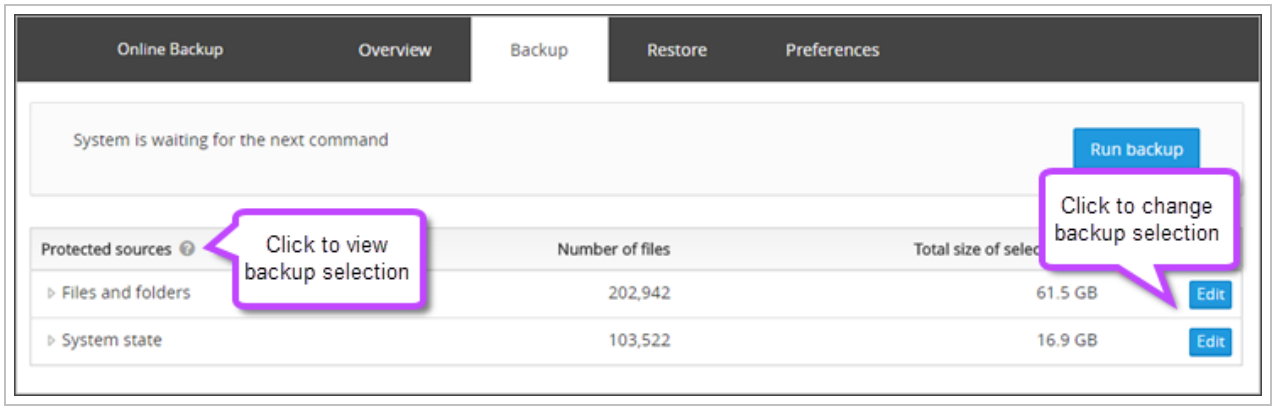
4. Select the files, folders, components (such as data bases, virtual disks, etc.) to back up. You can let the Backup Manager help you choose data for backup using the Automatic File Selection feature



5. Click **Save**

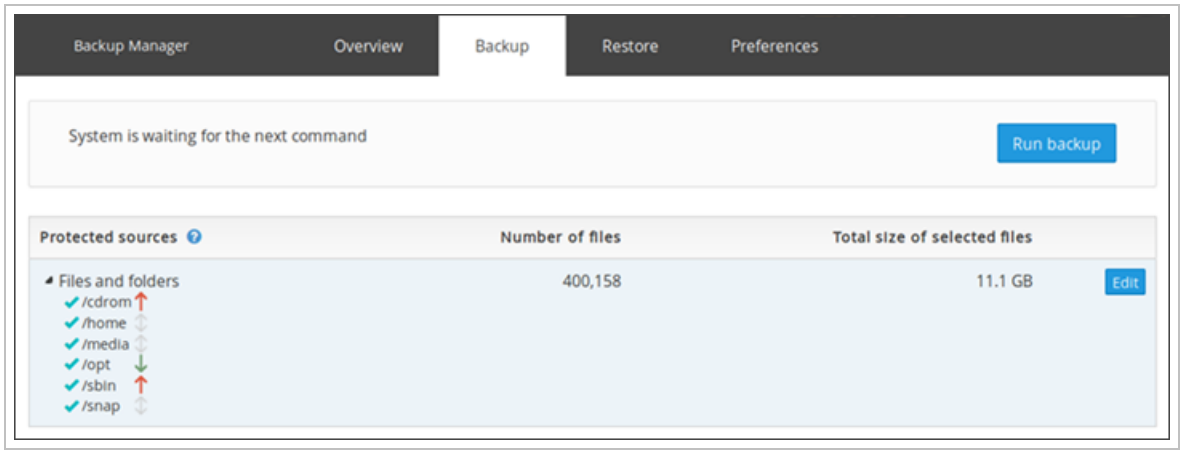
To make sure all necessary data has been included into your backup selection, click on the name of the data source. This will provide a list of the selection made.

Seeing a green tick followed by "\" means the whole data source is selected for backup.



> If you clear your backup selection after at least one backup has been completed, you will be offered to **remove all backup copies** of these files from the Cloud. This means the **entire backup history** of this data source will be deleted. **This action is irreversible.**

If you have selected only part of the disk, you have an option to set the priority of the files in the backup selection.



To do this:

1. Click on the name of the data source
2. Click the arrow to the right of the selection to choose the priority:
   - Click once to get a red up arrow - This indicates a high priority and will be backed up first
   - Click twice to get a green down arrow - This indicates a low priority and will be backed up last
   - Do not click or click to remove a priority to get a grey double-sided arrow - This indicates no priority set and will be backed up between the high and low priority jobs

> Data of the same priority will be completed in alphabetical order.

Start a one-time backup

You can initialize a backup manually at any time.

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Run backup**

The length of the backup depends on the size of your backup selection, the data transfer speed and performance of your computer.

> The **Run backup** button will be unavailable until at least one data source is configured for backup. This can be done by following the Configure backup selection steps above.

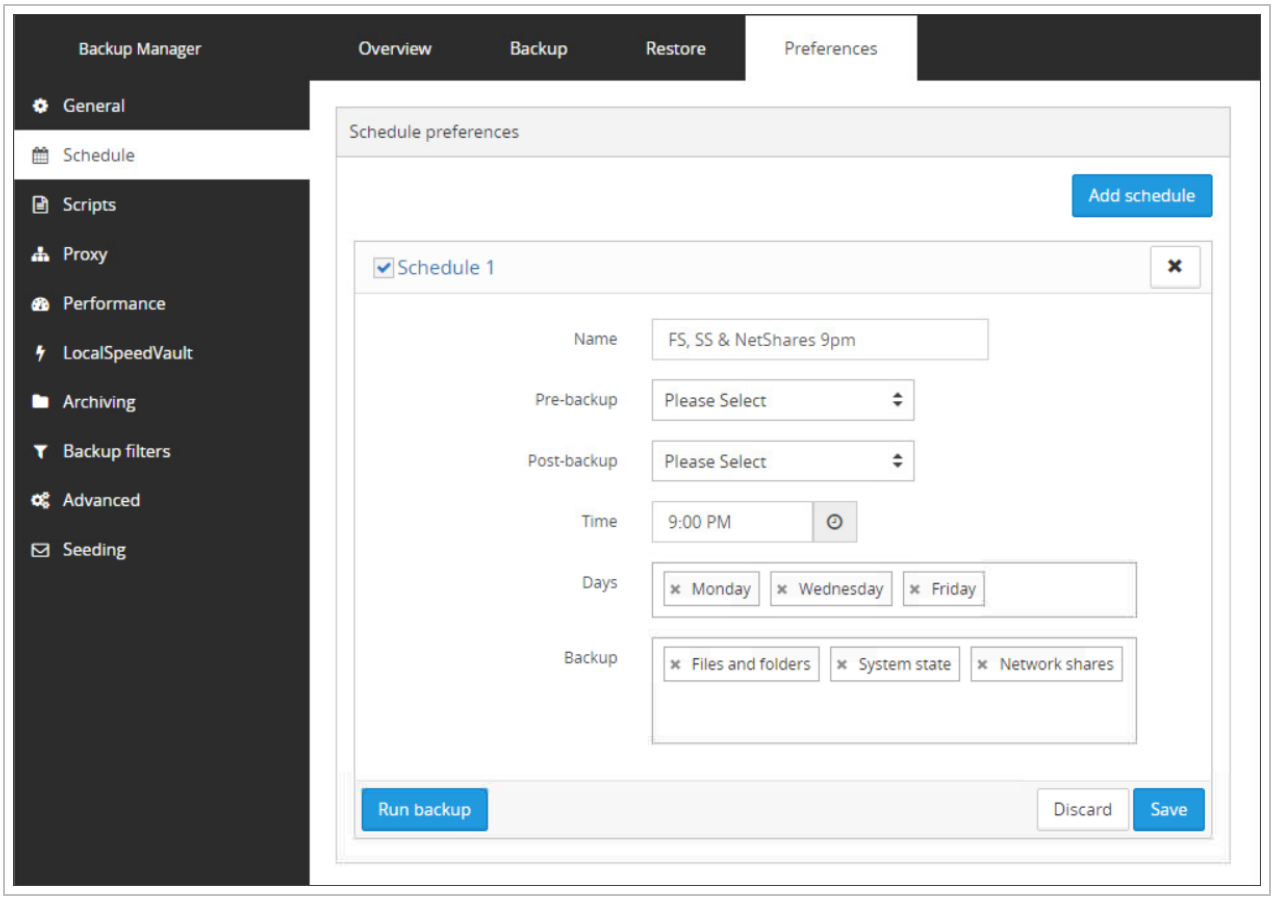
Configure schedule-based backups

The most convenient method of configuring backups is to set up a **backup schedule** which will automatically run the backups without requiring you to intervene.

You can create multiple schedules for each device, for example if you want Files and Folders to run at 9am but you want Files and Folders, System State and MySQL to run at 9pm.

To create a backup schedule:

1. Launch the Backup Manager for the device
2. Open the **Preferences** tab
3. Click **Schedule**
4. Select **Add Schedule**



5. Give the schedule a name - make this something relevant to the backup configured such as "FS, SS & MyS 9pm"
6. Optional - If you have created any scripts, these can be selected to run before the backup (Pre-backup) or after the backup (Post-backup) by selecting them from the given dropdowns.
7. Set the time for the backup to run
8. Choose the days on which you want the backup to run
9. Select the data sources to backup
10. Click **Save**

> If you want to back up a data source regularly, it **must** be configured for backup as well as selected in a schedule or a profile. This can be done by following the Configure backup selection steps above.

If you have multiple schedules listed in this page, you can enable or disable them by ticking the check box beside the name of the schedule. Disabling a schedule does not delete it, but will stop it from running until you manually enable it again.

To edit a schedule, you just need to expand the schedule in question, make the necessary changes and click **Save**.

To delete a schedule, simply click the **X** to the right of the schedule name, you will be prompted to confirm deletion of the schedule - click **Yes**.

> Please note, once a schedule has been deleted, it cannot be undeleted and would have to be recreated manually.

> If you have not configured the backup selection, the schedule will run, but as no data source configuration exists, nothing will be backed up.

Configure frequency-based backups

To enable frequency-based backups on a device, you need to create a **backup profile** with the required backup settings and apply the profile to the device.

See Backup Profiles in Management Console for detailed instructions on configuring profiles.

After the profile has been applied to the device, the new backup settings will be displayed under **Preferences > Schedule** in the Backup Manager. However, all editing is done through the profiles in the Management Console.

Troubleshooting MS SharePoint backups

MS SharePoint backups depend on 3 VSS writers:

1. **SqlServerWriter**
2. **SharePoint Services Writer** (in MS SharePoint 2013, it is disabled by default and needs to be registered)
3. **OSearch VSS Writer**

You can check the availability of these writers through a system console, for example the Command Prompt:

```
vssadmin list writers
```

> When there is difficulty starting or completing a SharePoint backup, it often helps to troubleshoot the writers.

What to do if a writer is unavailable

If one of the writers is unavailable (missing from the response to `vssadmin list writers`), you can try some typical solutions before contacting support.

Name of missing writer	Possible solutions
SqlServerWriter	1. Make sure the **SQL databases** for SharePoint are located on the current server (multi-tier configuration is not supported) 2. Make sure the names of the SQL databases on the current server do not contain spaces (see the **Identifying spaces in the names of SQL databases** section below) 3. Check the status of the **SQL Server VSS Writer** service that handles the writer 4. Make sure the Writer has sufficient access permissions (see the **Granting SQL Server VSS Writer access to the database** section below)
SharePoint Services Writer	1. Check the statuses of the services responsible for the writer: **Volume Shadow Copy** and **SharePoint VSS Writer** 2. (If the services are unavailable). Register the writer in the Windows registry

Name of missing writer	Possible solutions
	3. If MS SharePoint is installed on Windows SBS 2011 Standard, make sure the SharePoint Services Writer has sufficient access permissions (learn more)
OSearch VSS Writer	Activate the SharePoint Server Search 14 service that handles the writer.

Checking the statuses of VSS writers

The VSS writers are activated through appropriate **services**. If any of the writers are not available, please start the Services Console and make sure the following services are available and their statuses are as follows:

1. Volume Shadow Copy - must not be disabled
2. SharePoint Server Search 14 - must not be disabled
3. SQL Server VSS Writer - **Started** and set to the **Automatic startup** type
4. SharePoint VSS Writer - **Started** and set to the **Automatic startup** type

Registering the SharePoint Services Writer

In MS SharePoint 2010 and 2013, you may need to register the SharePoint Services Writer in the Windows registry.

Sometimes the writer can be enabled but not participating in backups. In that case, it needs to be disabled and then enabled again.

Here are steps to follow:

1. Start the Command Prompt (*cmd.exe*)
2. Go to the BIN directory
   - MS SharePoint 2010: `cd "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\BIN"`
   - MS SharePoint 2013: `cd "C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\BIN"`
3. From the BIN directory, run the appropriate command:
   - `stsadm -o unregisterwsswriter` - to disable (unregister) the writer - learn more
   - `stsadm -o registerwsswriter` - to enable (register) the writer - learn more

Identifying spaces in the names of SQL databases

The names of SQL databases for MS SharePoint must not start or end with a space (this is crucial for successful backups). You can check it in the following way:

1. In SQL Server Management Studio, right-click on any database. Select **Run query**
2. From *sys.databases*, run the following query:

```
select '#' + name +'#'
```

If detected, the spaces must be removed.

Granting SQL Server VSS Writer access to the database

Sometimes the access permissions granted to the SQL Server VSS Writer may be insufficient. This can happen in the following cases:

- The Writer is running under a user with insufficient privileges
- The Writer does not have sufficient privileges to access the database

Here is how to resolve the issue:

1. Add permissions for the **NT AUTHORITY/SYSTEM** service logon and any user which you have mentioned as service logon
2. Check SQL server security attributes for the user selected as service logon for SQL writer and add sysadmin privileges

Recovery

Instructions on restoring data from this data source can be found on Recovering data in Backup Manager.

MySQL

Backup Manager offers a backup and recovery service for MySQL databases on all the supported operating systems.

What's inside:

MySQL backup

Backup Manager offers a backup and recovery service for MySQL databases on all the supported operating systems.

> It is possible to add **multiple MySQL instances** to your backup selection (if they are installed on the same machine).

Requirements

- Backup Manager must be installed on the **MySQL server** that you want to back up
- The MySQL service must be **started** at the time a backup session starts
- MySQL backups depend on **VSS Snapshots**, so VSS must be available on the system
- Full permissions (with all privileges) are required to a MySQL database to backup the MySQL data source
- On Linux, **glibc 2.5** or higher is required
- The **Percona** version must be the same as the MySQL server you are trying to backup

Operating Systems and MySQL versions:

- **Windows & Linux** - Backup Manager handles MySQL versions:
  - 5.0.22
  - 5.1
  - 5.5
  - 5.6
  - 5.7
  - 8 and all its minor releases
- **macOS** - Backup Manager handles MySQL versions:
  - 5.0.22
  - 5.1
  - 5.5

Types of backups

Documents has 3 types of MySQL backups:

1. **Cold backups** - the MySQL server is stopped for some time while the backup session runs; it is necessary that no third-party applications should be keeping the database forcibly open at that time
2. **Warm Backups** - the MySQL server is locked for write operations for some time while the backup session runs, but is still accessible for read operations
3. **Hot backups** - the MySQL server keeps functioning while a backup session is running

The type of backup is MySQL version dependent:

<table>
<tr><th>MySQL version</th><th>Windows</th><th>Linux</th><th>Mac</th></tr>
<tr><td>MySQL 5.0.22</td><td rowspan="6">Warm backups</td><td rowspan="6">■ Hot backup for InnoDB tables
■ Warm backup for MyISAM tables</td><td rowspan="5">■ Hot backup for InnoDB tables
■ Warm backup for MyISAM tables</td></tr>
<tr><td>MySQL 5.1</td></tr>
<tr><td>MySQL 5.5</td></tr>
<tr><td>MySQL 5.6</td><td>Currently unsupported</td></tr>
<tr><td>MySQL 5.7</td><td>Currently unsupported</td></tr>
<tr><td>MySQL 8 and all its minor releases</td><td>Currently unsupported</td></tr>
</table>

Backup through the Backup Manager

Enabling schedule-based backups

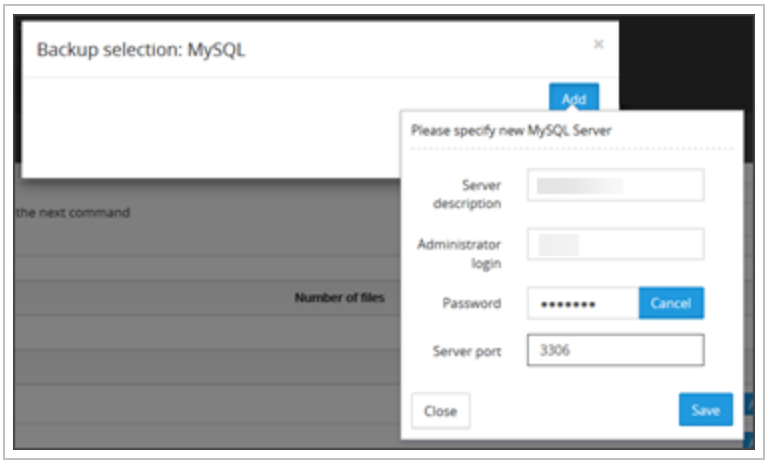
First enable schedule-based backups on the backup device by:

1. Configuring the backup selection to include MySQL
2. Create the backup schedule to run automated backups

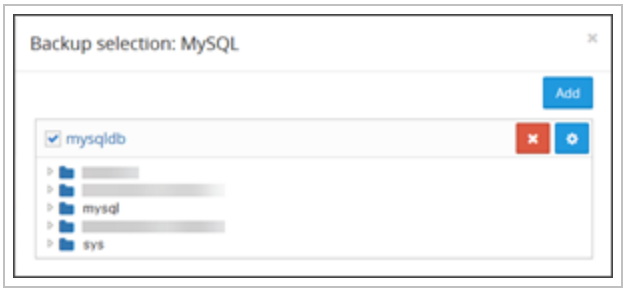
Configure backup selection

1. Launch the Backup Manager for the device
2. Open the **Backup** tab in the Backup Manager
3. Click **Add** next to the MySQL data source

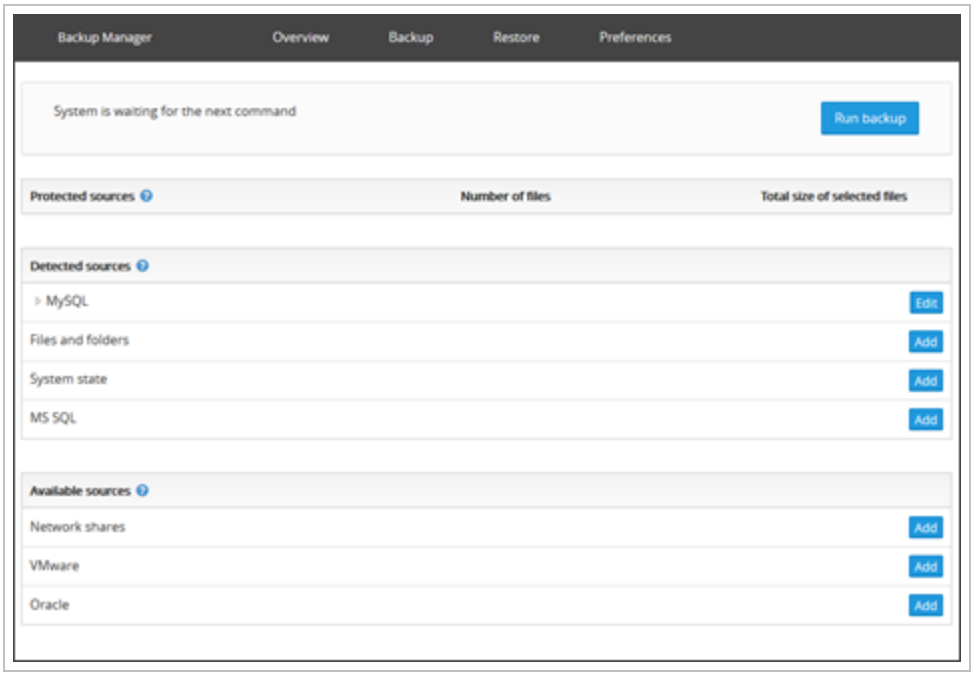
4. Enter the details for an administrator login for the MySQL server
5. Click **Save**



6. Make the selection for backing up the MySQL databases



7. Once the selection is complete, the MySQL datasource will now show as added and editable. You can click on the name of the data source at any time to be sure all necessary data has been included in the backup selection



> If you clear your backup selection after at least one backup has been completed, you will be offered to **remove all backup copies** of these files from the Cloud. The action is irreversible.

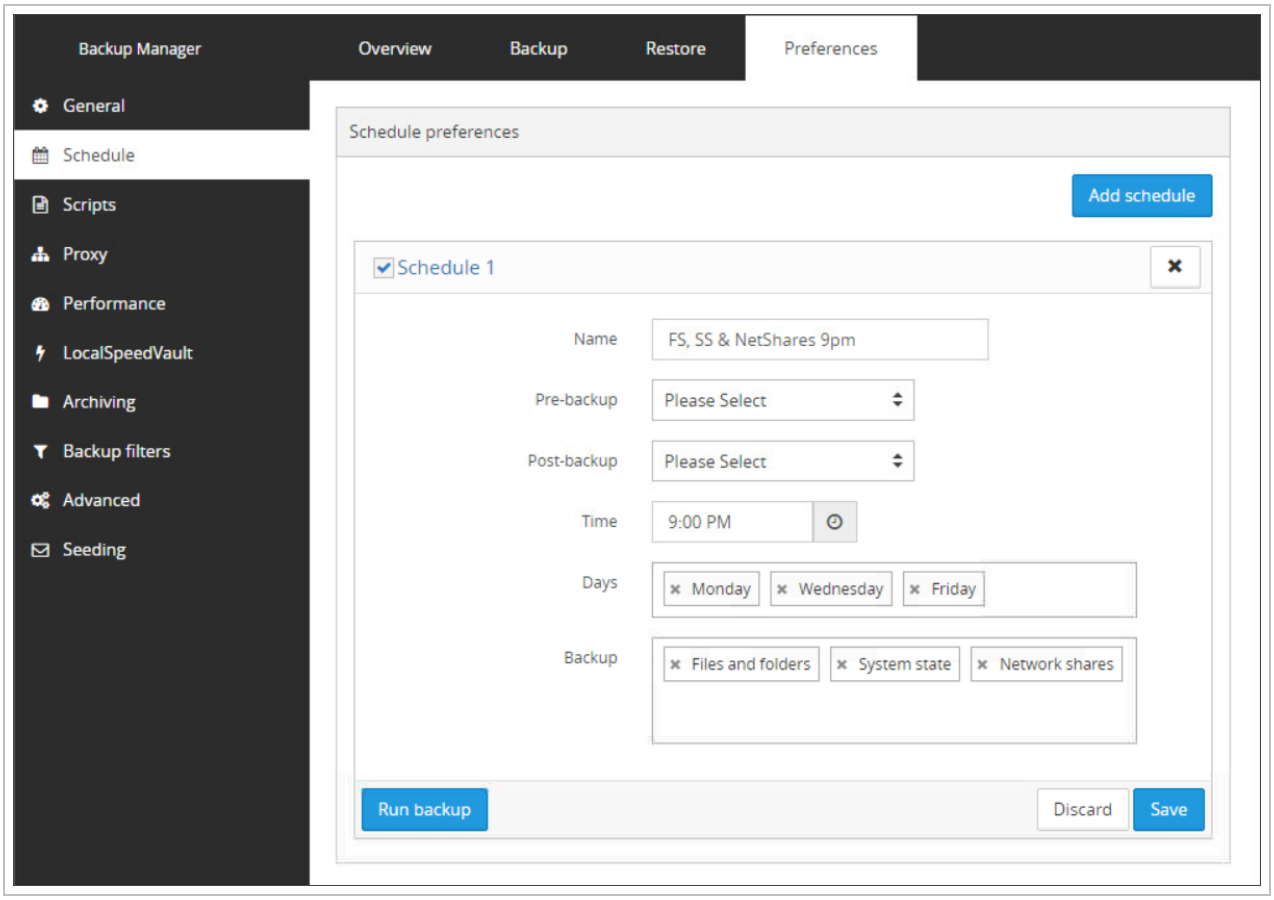
Create backup schedule

The most convenient method of configuring backups is to set up a **backup schedule** which will automatically run the backups without requiring you to intervene.

You can create multiple schedules for each device, for example if you want Files and Folders to run at 9am but you want Files and Folders, System State and MySQL to run at 9pm.

To create a backup schedule:

1. Launch the Backup Manager for the device
2. Open the **Preferences** tab
3. Click **Schedule**
4. Select **Add Schedule**



5. Give the schedule a name - make this something relevant to the backup configured such as "FS, SS & MyS 9pm"
6. Optional - If you have created any scripts, these can be selected to run before the backup (Pre-backup) or after the backup (Post-backup) by selecting them from the given dropdowns.
7. Set the time for the backup to run
8. Choose the days on which you want the backup to run
9. Select the data sources to backup
10. Click **Save**

> If you want to back up a data source regularly, it **must** be configured for backup as well as selected in a schedule or a profile. This can be done by following the Operating Systems and MySQL versions: steps above.

If you have multiple schedules listed in this page, you can enable or disable them by ticking the check box beside the name of the schedule. Disabling a schedule does not delete it, but will stop it from running until you manually enable it again.

To edit a schedule, you just need to expand the schedule in question, make the necessary changes and click **Save**.

To delete a schedule, simply click the **X** to the right of the schedule name, you will be prompted to confirm deletion of the schedule - click **Yes**.

> Please note, once a schedule has been deleted, it cannot be undeleted and would have to be recreated manually.

> If you have not configured the backup selection, the schedule will run, but as no data source configuration exists, nothing will be backed up.

Start a one-time backup

You can initialize a backup manually at any time.

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Run backup**

The length of the backup depends on the size of your backup selection, the data transfer speed and performance of your computer.

> The **Run backup** button will be unavailable until at least one data source is configured for backup. This can be done by following the Operating Systems and MySQL versions: steps above.

Backup through the command line

You can back up and restore data not just using the web interface but through the command line as well. This is done using the **Client Tool**, an executable file included into all Backup Manager installations (view primary Client Tool instruction).

Below is a sample instruction for MySQL, based on a **Linux** case.

> The same work flow can be used on **Windows**, however, changes will be required for the Windows command line versus the below for a Linux terminal, for example, file locations.

1. Start your terminal emulator
2. Navigate to the Backup Manager installation directory (this is where ClientTool is located)

   ```
   cd /opt/MXB/bin
   ```

3. Configure access to the MySQL server that you want to back up

   ```
   ./ClientTool control.mysqldb.add -name mysqldb -user root -password **pass**
   -server-port 3306
   ```

   Where the parameter values (in *italics* above) are replaced with the values required:
   - `-name` - assign a name to the MySQL server as it will appear in the Client Tool and Backup Manager. Latin letters and most punctuation marks are supported, but we cannot support slashes
   - `-user` - the Administrator username for access to the MySQL server (we recommend using the root)
   - `-password` - the Administrator password for access to the MySQL server corresponding to the user
   - `-server-port` - the port number of the MySQL server. If in doubt, check the option file on your machine *(my.cnf)*

4. Add the MySQL server to your backup selection

```
./ClientTool control.selection.modify -datasource MySql -include mysqldb
```

> You can make sure the MySQL server has been included into the backup selection using the `control.selection.list` command.

5. Create a schedule for the MySQL data source, for example:

```
./ClientTool control.schedule.add -name MySQL_Daily -active 1 -datasources
MySql -days All -time 20:00
```

6. Start the backup of the MySQL data source

```
./ClientTool control.backup.start -datasource MySql
```

> You can check the current status of the backup session using the `control.session.list` command.

MySQL recovery

Backup Manager lets you restore the MySQL instances it has backed up. Note that the whole **instance** is restored (it is not possible to select a particular database, file or table from it).

You can recover MySQL (using the Backup Manager or command line) to either of the following:

- To the **current location** (in-place restore) - An in-place restore can only be performed only if the following is true:
  - MySQL configuration is the same as during the backup
  - All MySQL data is inside the datadir folder on Linux, MacOS and Windows

    > On Windows the `innodb_data_home_dir` and `innodb_log_group_home_dir` folders are also supported for in-place restores.
- To a **new location** - In this case you will need to move the files to an appropriate folder where MySQL can recognize them. Please do not forget to stop the MySQL service before doing it

How in-place restores work

How in-place restore works after the Restore is started:

1. Make a request to MySQL server to get the path to the restore data
2. Get the MySQL server user
3. Stop the MySQL service
4. Restore files to the requested location
5. Change the files owner and group to the MySQL server user
6. Start MySQL service

> Right now only the **initd service manager** is supported to stop and start MySQL service.

Starting the MySQL service on Security-Enhanced Linux after recovery

SELinux may prevent the MySQL Server Daemon from accessing the database files after recovery, in this case, it results in `error #13: Can't open the mysql.plugin table.`

In this case, run `mysql_upgrade` to create it.

Once created, you can reset the security context of the database files, for example using the **restorecon** program, by running the following command:

```
restorecon -Rv /var/lib/mysql
```

It may also be necessary to repeat the command for other files and directories which have been restored.

Use the `man restorecon` command to get additional information about **restorecon**.

Restore through the command line

1. Start your terminal emulator and move to the Backup Manager installation directory

   ```
   cd /opt/MXB/bin
   ```

2. Initiate the recovery of your MySQL server

   ```
   ./ClientTool control.restore.start -datasource MySql -selection mysqldb
   ```

   Here are some options:

   - You can restore to the **current directory** (in-place restore) under certain circumstances. To perform a restore to an **intermediate directory**, specify the `-restore-to` parameter, for example `-restore-to /tmp`
   - You can specify the **backup session** that you want to restore (by default the most recent session is selected). This is done using the `-time` parameter - for example `-time "2016-09-02 14:44:39"`

   You can check the current status of the restore session using the `control.session.list` command.

3. **(if applicable)** If you recovered MySQL to an intermediate directory, you will need to **copy the recovered files** to the appropriate data directory for the recovered instance

   For example, on Linux:

   ```
   /var/lib/mysql
   ```

   For example, on Windows:

   ```
   C:\ProgramData\MySQL\MySQL Server 5.5\data
   ```

4. **(if applicable)** On Linux, original file locations and permissions cannot be determined, because Percona XtraBackup files are used and these do not contain the original file locations and permissions

   For example:

   ```
   chown -R mysql:mysql /var/lib/mysql
   ```

5. Restart the MySQL service to apply the changes

Important

To get details on a particular command (output structure, required arguments and optional arguments), enter the following string to your terminal emulator:

```
./ClientTool help -c <command>
```

Backup technology

Data backup in the Backup Manager is **session-based**. A session is a process during which a data selection on a client device is backed up to a remote server. Backup sessions result in the creation of virtual copies that can be retrieved at any time.

Because data tends to change, backup sessions usually run on a **repeated basis** (for instance, every day). You can start a new backup session manually or you can create a schedule for it.

> 1 data source = 1 backup session

There is a separate session for each data source. For example, if a backup selection has two data sources (Files and folders and System state), there will be two backup sessions.

Backup session structure

All backup sessions go through two stages: scanning and processing. The procedure varies slightly for **initial sessions** (performed on a device for the first time) and **subsequent sessions** (all other sessions after the initial one).

Structure of initial backup sessions

Stage 1: Scanning

At this stage, the Backup Manager makes the list of data to back up. In short, here is what it does:

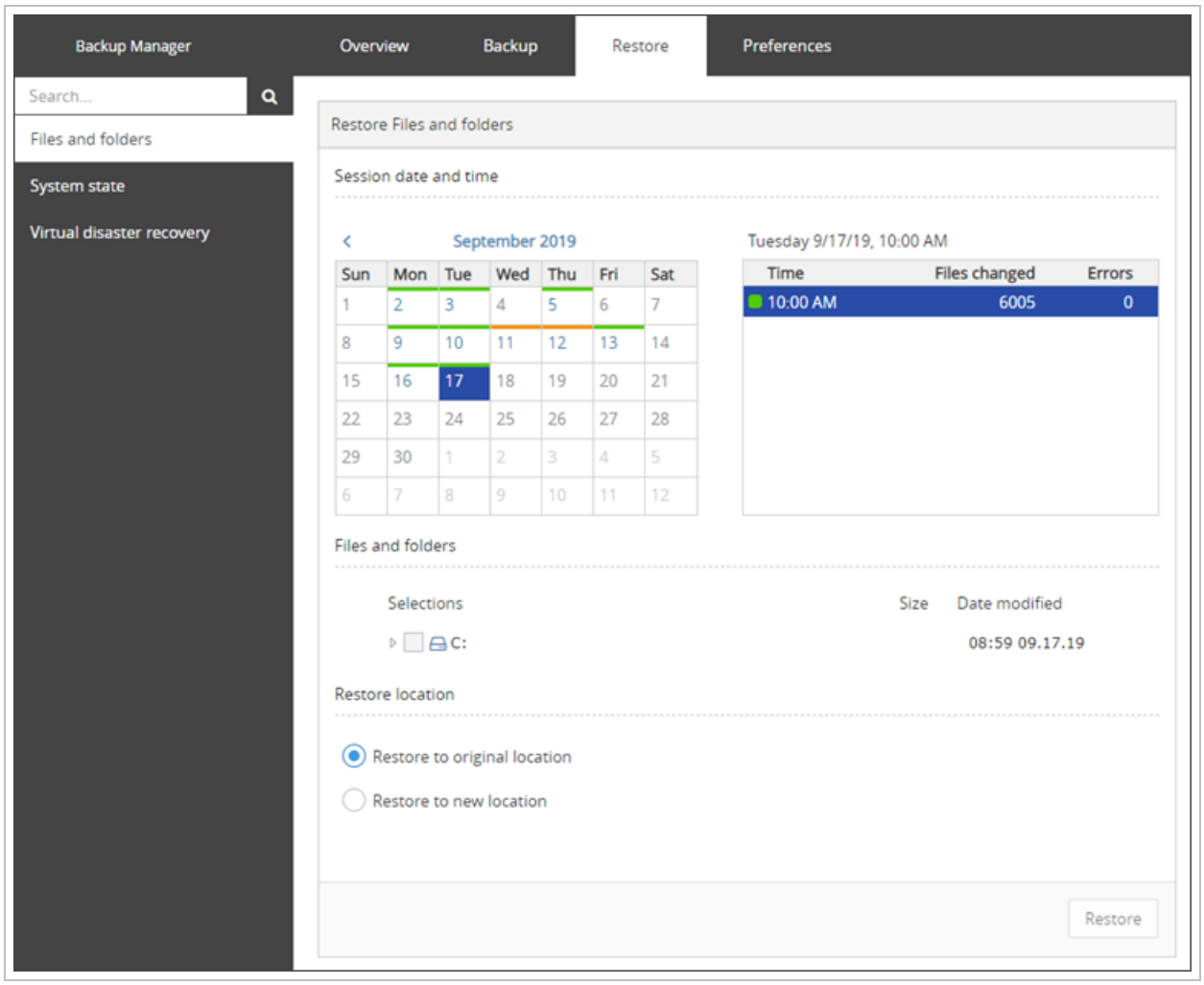
- Performs a system scan to locate the data selected for backup
- Puts the files in a queue

Stage 2: Processing

The Backup Manager takes the queued files one by one in the order of **priority** (user-defined) and **recentness** (defined by change dates) and handles them in the following way:

- Cuts them into smaller fragments known as **slices**
- Calculates a **hash** (a unique data fingerprint) for each slice. During further backups, the hash will be used to detect changes
- **Compresses** the slices to reduce their size (saves bandwidth and storage space)
- **Encrypts** the slices using the private security code/encryption key set during Backup Manager installation (the data will be inaccessible without the key)
- Combines multiple slices into **cabinets** to utilize network and storage resources more efficiently
- **Transfers** the cabinets to the Cloud. By default, 4 simultaneous connections are established. Their number can be customized using the `SynchronizationThreadCount` parameter in the advanced settings. The higher the number of connections, the faster your data will reach the storage. However, a high number of connections consumes more bandwidth and memory resources
- Registers all files and slices in a local database called the **Backup Register** and uploads the database to the Cloud

When the backup session is complete, the data becomes available for recovery. You can see a new entry in the calendar on the **Restore** tab.



Structure of further backup sessions (delta backup)

Stage 1: Scanning (only for non-accelerated backups)

The Backup Manager scans the system to find the data to back up and compares the results with those from the previous session. The comparison is drawn based on **file attributes** (names, change dates, size, access permissions and so on) stored in the Backup Register. If **at least one** attribute in a file has changed, the file is added to the queue for further processing.

> If a session is powered by the Backup Accelerator, the scanning stage is missing. The Backup Manager downloads the list of changes from the cloud and gets straight to processing.

Stage 2: Processing

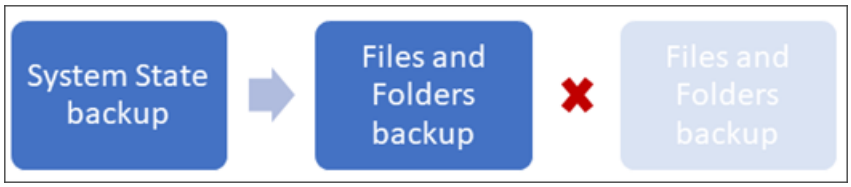
The Backup Manager slices the files in the order of priority and recentness and calculates hashes for the slices. Then the hashes are compared to the hashes from the previous backup session. New slices whose hashes do not have matches in the storage undergo the standard procedure. They are compressed, encrypted, combined into cabinets and delivered to the storage. The Backup Register is updated with new records after that.

Sequence of backup sessions

Backup sessions run **successively**. You can start a new session **after** the current one is complete (the **Run backup** button is unavailable while there is an active backup process).

Backup sessions can sometimes **overlap** (for example, if they were scheduled one shortly after another or if one session had been started manually just before a scheduled session was due). If this happens, the session that started first is completed normally. Further sessions that started while it was in progress are processed depending on their type.

- If the sessions belong to the **same data source**, the later sessions are **skipped**. The next backup takes place according to the active schedule (skipped sessions are not re-run)
- If the sessions belong to **different data sources**, the later sessions are put into a **queue**. They will be processed later, when the current session is complete
- If a **queue** contains a backup session for a certain data source, all newer sessions for that data source are **skipped**. Let's say, a System State backup is in progress. In the meanwhile, a Files and Folders backup is initiated. The Backup Manager adds Files and Folders to the queue. Then another Files and Folders backup is started on schedule which gets skipped. Users may get an impression that the Files and Folders backup got skipped without a reason, but that is because they cannot view the queue that already contains the data source



Practical implications

1. Backup Manager users **needn't make any preparations** for backup: move the files to a separate folder, compress them or check for duplicates
2. Data sent to storage is always **unique** in the sense that only changed blocks are transferred and only one copy of each change is submitted. This guarantees the use of bandwidth and storage space economically

3. If canceling a backup, the data already sent prior to the cancellation will stay in the cloud until it passes the retention period of the device. This data will not need to be sent again
4. When the Backup Manager searches for changes, it compares file properties first. Only if a property has changed, a content analysis is made. This drastically reduces the amount of time and processing required for change detection, especially when it comes to large data sets
5. To speed up backup sessions, you can enable the Backup Accelerator (Windows only) or increase the number of simultaneous connections

Enabling backups in Backup Manager

Two types of backups are available:

1. **Schedule-based** backups (run on a certain day/time basis)
2. **Frequency-based** backups (run at a specified interval)

Requirements

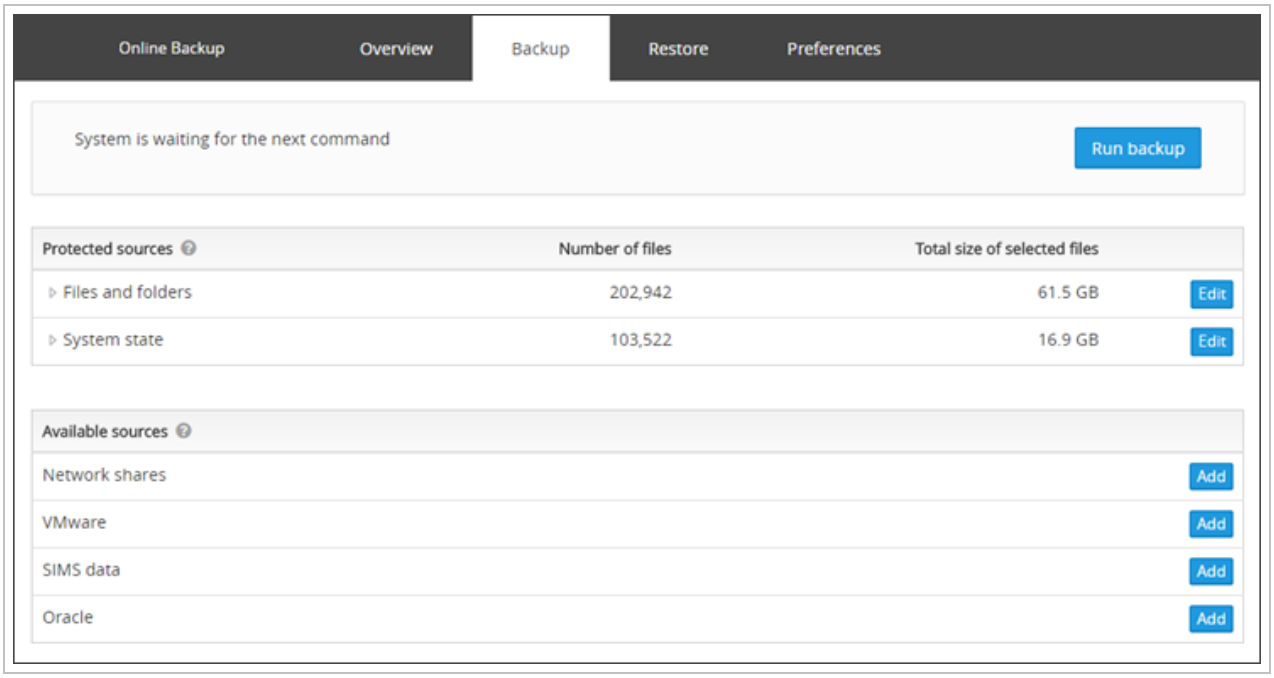
The computer must be online (turned on and must not enter the sleep mode) during backups. If a machine is offline, it will cause the backup to fail to start and will not begin until the machine is turned on or woken up.

If a backup is already running when the machine is turned off, the backup will be aborted. If the machine enters sleep mode while a backup is in progress, the backup will pause until the machine is woken up.

> Be aware that in order to successfully restore using the Virtual Disaster Recovery or Bare Metal Recovery methods, you must back up the full Files and Folders data source (the whole system disk `C:\` or any other depending on the configuration of your computer)

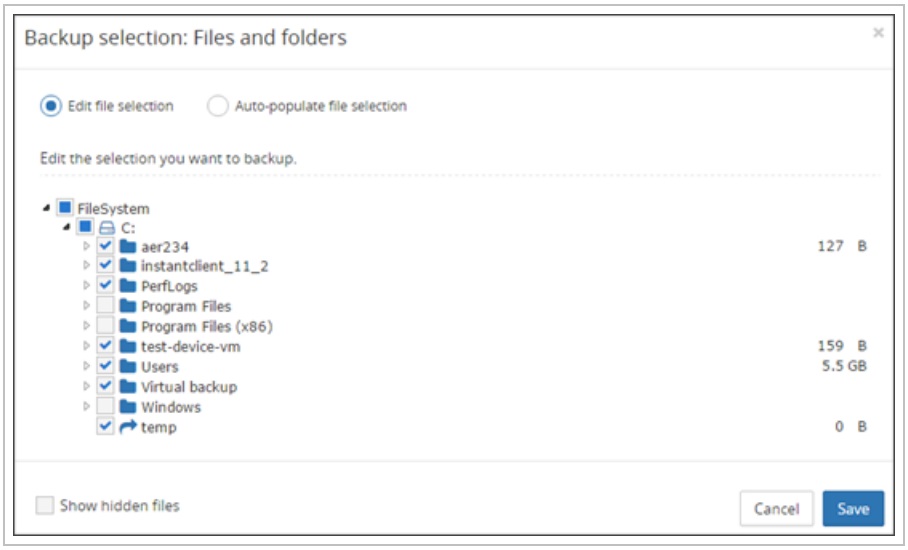
Configure backup selection

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Add** next to the data sources you want to back up



> The below steps detail adding **Files and Folders** for selection, but the process is similar for most data sources. Sources such as Network Shares and VMware require you to supply additional information, such as server details, paths, usernames and passwords.

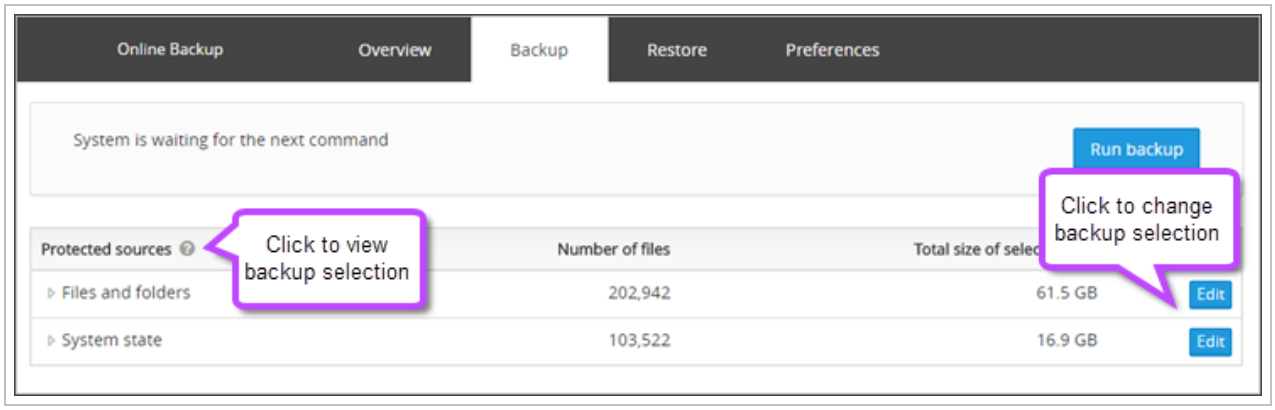
4. Select the files, folders, components (such as data bases, virtual disks, etc.) to back up. You can let the Backup Manager help you choose data for backup using the Automatic File Selection feature



5. Click **Save**

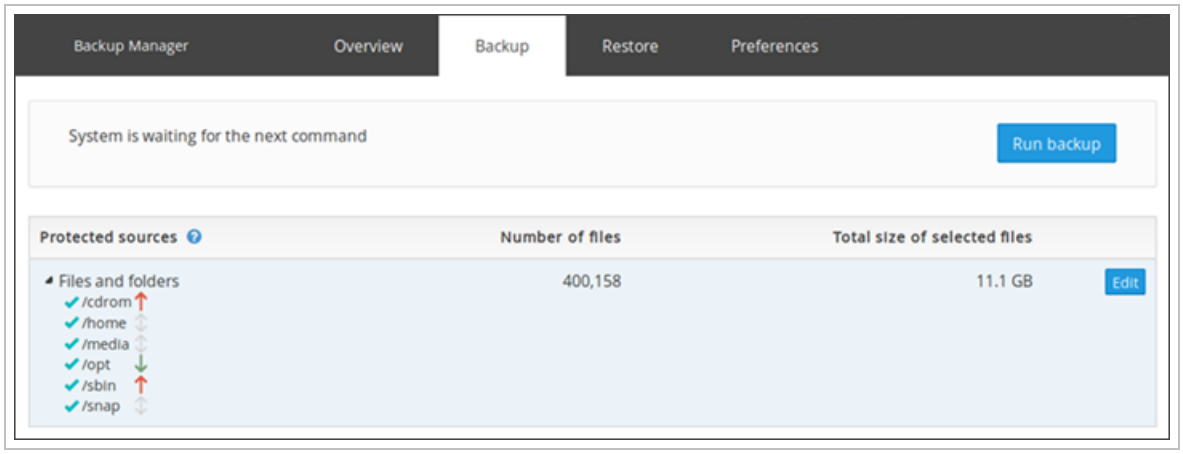
To make sure all necessary data has been included into your backup selection, click on the name of the data source. This will provide a list of the selection made.

Seeing a green tick followed by "\" means the whole data source is selected for backup.



> If you clear your backup selection after at least one backup has been completed, you will be offered to **remove all backup copies** of these files from the Cloud. This means the **entire backup history** of this data source will be deleted. **This action is irreversible.**

If you have selected only part of the disk, you have an option to set the priority of the files in the backup selection.



To do this:

1. Click on the name of the data source
2. Click the arrow to the right of the selection to choose the priority:
   - Click once to get a red up arrow - This indicates a high priority and will be backed up first
   - Click twice to get a green down arrow - This indicates a low priority and will be backed up last
   - Do not click or click to remove a priority to get a grey double-sided arrow - This indicates no priority set and will be backed up between the high and low priority jobs

> Data of the same priority will be completed in alphabetical order.

Starting a Backup

Start a one-time backup

You can initialize a backup manually at any time.

1. Launch the Backup Manager for the device
2. Open the **Backup** tab
3. Click **Run backup**

The length of the backup depends on the size of your backup selection, the data transfer speed and performance of your computer.

> The **Run backup** button will be unavailable until at least one data source is configured for backup. This can be done by following the Configure backup selection steps above.

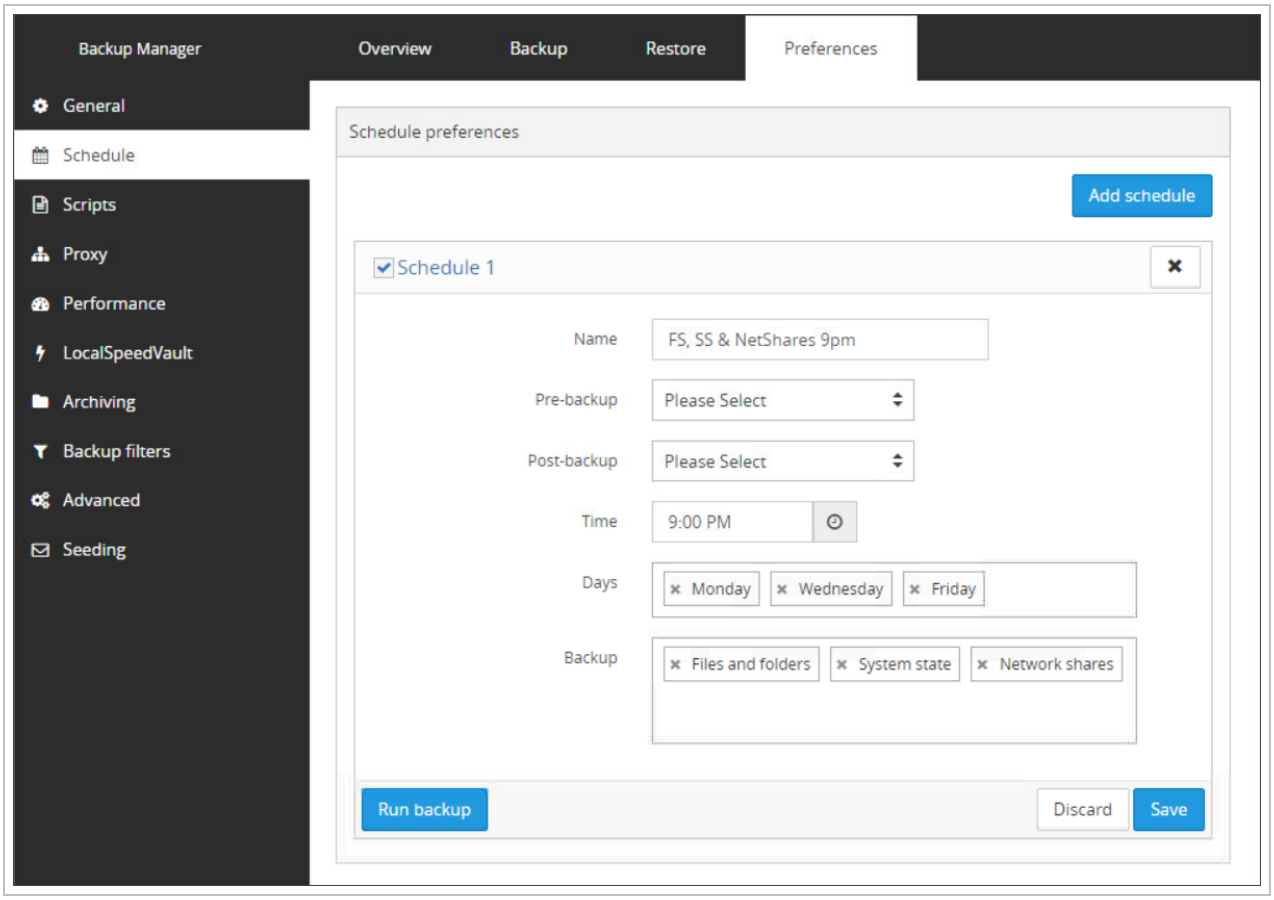
Configure schedule-based backups

The most convenient method of configuring backups is to set up a **backup schedule** which will automatically run the backups without requiring you to intervene.

You can create multiple schedules for each device, for example if you want Files and Folders to run at 9am but you want Files and Folders, System State and MySQL to run at 9pm.

To create a backup schedule:

1. Launch the Backup Manager for the device
2. Open the **Preferences** tab
3. Click **Schedule**
4. Select **Add Schedule**



5. Give the schedule a name - make this something relevant to the backup configured such as "FS, SS & MyS 9pm"
6. Optional - If you have created any scripts, these can be selected to run before the backup (Pre-backup) or after the backup (Post-backup) by selecting them from the given dropdowns.
7. Set the time for the backup to run
8. Choose the days on which you want the backup to run
9. Select the data sources to backup
10. Click **Save**

> If you want to back up a data source regularly, it **must** be configured for backup as well as selected in a schedule or a profile. This can be done by following the Configure backup selection steps above.

If you have multiple schedules listed in this page, you can enable or disable them by ticking the check box beside the name of the schedule. Disabling a schedule does not delete it, but will stop it from running until you manually enable it again.

To edit a schedule, you just need to expand the schedule in question, make the necessary changes and click **Save**.

To delete a schedule, simply click the **X** to the right of the schedule name, you will be prompted to confirm deletion of the schedule - click **Yes**.

> Please note, once a schedule has been deleted, it cannot be undeleted and would have to be recreated manually.

> If you have not configured the backup selection, the schedule will run, but as no data source configuration exists, nothing will be backed up.

Configure frequency-based backups

To enable frequency-based backups on a device, you need to create a **backup profile** with the required backup settings and apply the profile to the device.

See Backup Profiles in Management Console for detailed instructions on configuring profiles.

After the profile has been applied to the device, the new backup settings will be displayed under **Preferences > Schedule** in the Backup Manager. However, all editing is done through the profiles in the Management Console.

Backup options

There some options that you can consider for faster and efficient backups.

- Automatic file selection in Backup Manager
- Backup Accelerator for faster backups in Backup Manager

Automatic file selection in Backup Manager

Cove Data Protection (Cove) offers an **automatic file selection** feature. It is a quick and easy way to populate your backup selection for the "Files and Folders" data source. It also brings to focus important files that you might have forgotten about.

What the feature does

When you install the Backup Manager, it automatically detects files that you may want to protect against loss and offers you to add them to your backup selection. There are 3 groups of such files:

1. **Documents** (*.doc, *.docx, *.xsl, *.xslx)
2. **Images** (*.png, *.jpg, *.jpeg)
3. **Videos** (*.avi, *.mpg, *.mpeg, *.mkv)

You can change your initial choice of the file groups after the installation as well as refine your backup selection by checking/unchecking individual files and folders.

Feature availability

The automatic file selection feature can be activated on **Windows** devices:

- Windows 8 / 8.1
- Windows 10
- Windows 11
- Windows Server 2012 / 2012 R2 (limited[1])
- Windows Server 2016 (limited[2])

---

[1]New features such as Docker-based containers, Storage Spaces Direct and Shielded VMs are not.

[2]Only the features compatible with Windows Server 2012 R2 are supported.

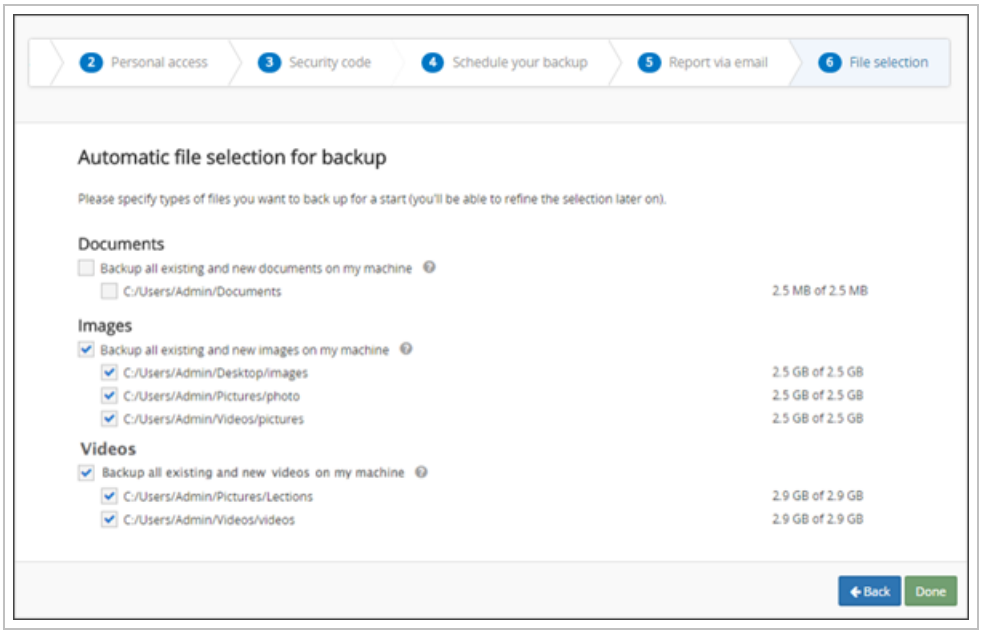
- Windows Server 2019 (limited[1])
- Windows Server 2022 (limited[2])

Instructions

Making an initial selection

You can start using the feature during installation. At the "File selection" step, the installation wizard displays major file categories detected on the current computer. Next to the name of the category you can see the total size of files in it.

Select the categories that you want to include into your backup selection. You will be able to view and edit the selection after the installation.



> The "Images" category appears if there is **at least one** folder with the total size of image files reaching **20 MB**. All its sub-folders are taken into account. Just the same is with "Videos". The minimum size limit keeps unneeded files such as application icons off your backup selection list.

Editing the selection

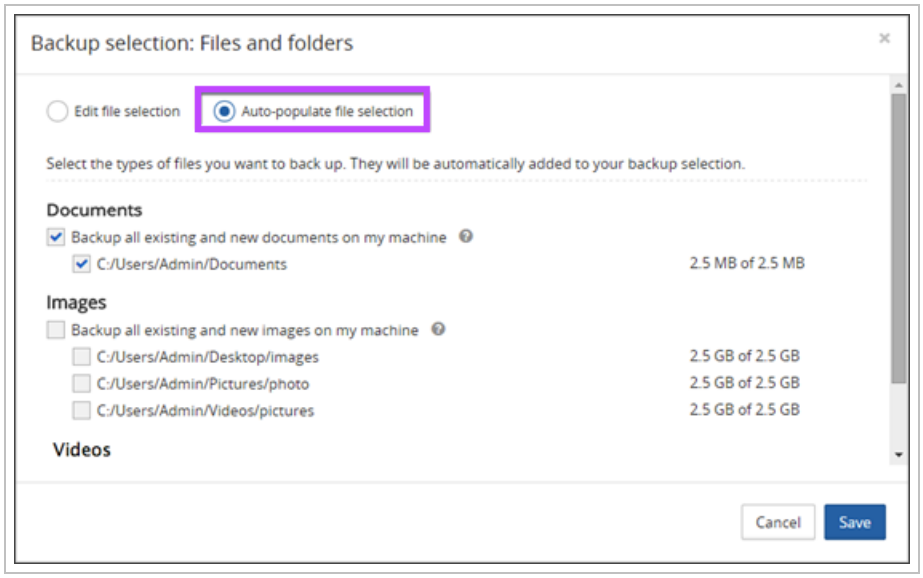
To edit the initial selection of the file categories for backup:

1. Launch the Backup Manager for the device
2. Navigate to the **Backup** tab
3. Click **Edit** next to the "Files and folders" data source

---

[1]Only the features compatible with Windows Server 2012 R2 are supported.
[2]Only the features compatible with Windows Server 2012 R2 are supported.

4. Switch from **Edit file selection** to **Auto-populate file selection**



Files from the selected categories are automatically added to your backup list (as well as the containing folders). Choose **Edit file selection** to view these files and folders and add more (if needed).

> If you are using exclusion filters **(Preferences > Backup filters)**, files matching your filtering conditions will not be backed up (even if they are included into your backup selection).

How the feature works

- The Backup Manager scans the **local hard drives** in search for valuable files. **Network shares** are not scanned
- The Backup Manager approaches valuable data **by the folder**. If it detects a folder with matching content, all files in that folder are selected
- The "Documents" category is populated based on **file extensions** only (no regard to file size). The "Images" and "Video" categories observe the **minimum size** limit of 20 MB per folder. If the total size of matching files in a folder and all if its subfolders is less than 20 MB, the folder does not appear under "Automatic file selection". You will be able to add it to your backup selection manually if you wish (the **Edit file selection** option)

- Some directories are automatically excluded from the automatic selection: "Windows", "Program Files", "Program Files (x86)" on 64-bit computers, and "ProgramData"
- Whenever you make changes to the automatic file selection categories, your backup list gets automatically updated. It does not work the other way round though. So editing your backup selection has no influence on the automatic selection categories. For example, if you select the "Images" category and then uncheck your D:\ volume, none of the images located on that volume will be backed up
- If a new file is added to a folder marked for backup, it is automatically included into your backup selection. Just the same is with sub-folders
- The Backup Manager scans your file system once a week (unless specified otherwise). This is done at a time when there are no active backup or recovery processes. To view the scanning results and integrate them into your backup selection, open the **Backup** tab, click **Edit** next to the "Files and folders" data source, and then choose **Auto-populate backup selection**. Click **Save** when you finish editing

Advanced settings (optional)

You can adjust how the feature works on your computer using through the advanced settings (view instructions).

Automatic file selection settings for configuration file

There are two advanced settings that may be configured for the Automatic file selection feature in the Backup Manager, which should be set or changed in the `config.ini` file.

Details on the file location of the configuration file can be found at: Config.ini location

Section	Parameter	Definition	Supported values
`[General]`	`AutomaticFileSelectionExaminingPeriodicity`	This is how often your system is scanned for new files that can be suggested for automatic selection.	Number (in seconds). Default value - 604800 (equals 7 days).
`[General]`	`AutomaticFileSelectionDirectoriesMaxDepth`	This is the maximum directory depth for scanning.	Number. The default value is 0 (no limit). Usually values from 3 to 7 are most appropriate, however this largely depends on your directory structure. For example, if you set the value to 5, the Backup Manager will not look deeper than the following subdirectory: `C:\Users\Admin\Documents\For_publishing\`.

Backup Accelerator for faster backups in Backup Manager

The Backup Accelerator is a feature in the Backup Manager that speeds up backups and increases RPO.

Enabling the Backup Accelerator

You can enable and disable the feature on devices through product settings. It is enabled by default in the "All-In" product.

Supported data sources

The Backup Accelerator works for files of **all types and sizes** belonging to the following data sources:

- Files and Folders
- System State
- Hyper-V
- Microsoft Exchange
- Microsoft SQL
- Microsoft SharePoint

The remaining data sources (VMware, Network Shares, Oracle and MySQL) are backed up without the involvement of the Backup Accelerator.

Requirements

Supported operating systems

The Backup Accelerator is a **Windows-only** feature. We support the following Windows versions:

- Windows 8 / 8.1
- Windows 10
- Windows 11
- Windows Server 2012 / 2012 R2 (limited[1])
- Windows Server 2016 (limited[2])
- Windows Server 2019 (limited[3])
- Windows Server 2022 (limited[4])

See the below links to additional required updates:

- Learn more about the 3033929 update (Technet article)
- Download the SHA-2 update

---

[1]New features such as Docker-based containers, Storage Spaces Direct and Shielded VMs are not.
[2]Only the features compatible with Windows Server 2012 R2 are supported.
[3]Only the features compatible with Windows Server 2012 R2 are supported.
[4]Only the features compatible with Windows Server 2012 R2 are supported.

Hardware requirements

- The Backup Accelerator processes all **local volumes** (both basic and dynamic) that have backup selections. **Network volumes** (including Cluster Shared Volumes) are not supported.
- Supported **file systems**: NTFS, ReFS and FAT32.

Limitations / Known issues

The Backup Accelerator does not track the following:

- Disk formatting
- VSS snapshot reverts
- Rolled back NTFS transactions
- Some memory-mapped files (delayed change detection may occur)

Also when a session is powered by the Backup Accelerator, existing backup quotas may be occasionally exceeded.

How the Backup Accelerator works

The Backup Accelerator is a **kernel mode driver** (a file system filter that monitors all file modification operations on selected volumes).

The Backup Manager uses information collected by the driver to increase backup performance by avoiding unnecessary scanning of the file system tree and reading the entire content of changed files. Instead, only files reported by the driver are processed and only modified file data is read from disks during backups.

Changes collected by the driver are reset if:

- The system is rebooted
- The backup selection is modified
- Backup filters are modified
- A backup session fails
- The Backup Service Controller is restarted
- The Backup Accelerator encounters an internal error and needs to be restarted
- An inconsistency in backup data is detected

In cases like these, the next backup session does not benefit from the Backup Accelerator technology and a full scanning is performed. When that full session is completed, the Backup Accelerator is re-activated.

Recovering data in Backup Manager

All data sources in Backup Manager are recovered according to a **general scheme**. Please check for additional requirements and settings for the data sources you use.

Critical Restore? We're not the judge of when a recovery is especially time critical–you are.

Critical Restore is our partner-driven fast escalation process. Just let us know on your initial support call, email, or chat message that a specific recovery is especially time sensitive, and we'll bring all hands on deck immediately to help you get your customer back up and running ASAP.

For more details please see the Critical Restore FAQ's.

Additional requirements and settings by data source

Data source	Additional requirements	Pre-recovery settings	Additional recovery settings
Files and folders	No	No	No
System state	Yes	For domain controllers only[1]	No
MS SQL databases	Yes	For master database recovery - stop the SQL Server service	No
VMware machines	Yes (for individual file recovery)	Power off the virtual machine if it is going to be overwritten	Server access settings for restore to a new location
Hyper-V machines	Yes (for individual file recovery)	Power off the virtual machine if it is going to be overwritten	No
MS Exchange databases	The original data stores must be available (for in-place restores)	No	No
MS Exchange items	Yes	Yes	Yes (optional)
Oracle databases	No	No	Post-recovery
MySQL databases	Yes, for in-place restores An in-place restore can only be performed only if the following is true: ▪ MySQL configuration is the same as during the backup ▪ All MySQL data is inside the datadir folder on Linux, MacOS and Windows. On Windows the `innodb_data_home_dir` and `innodb_log_group_home_dir` folders are also supported for in-place restores.	Stop the MySQL service	No

Instructions

The instructions below are relevant to the following data sources when restoring to any location on the same device as the backup was performed:

- Files and Folders
- System State

[1]Reboot the machine in Directory Services Restore Mode

- MS SQL
- VMware
- MS SharePoint
- Network Shares

For instructions on restoring Hyper-V data, see Individual File and Folder Recovery.

For instructions on restoring MS Exchange data, see MS Exchange recovery.

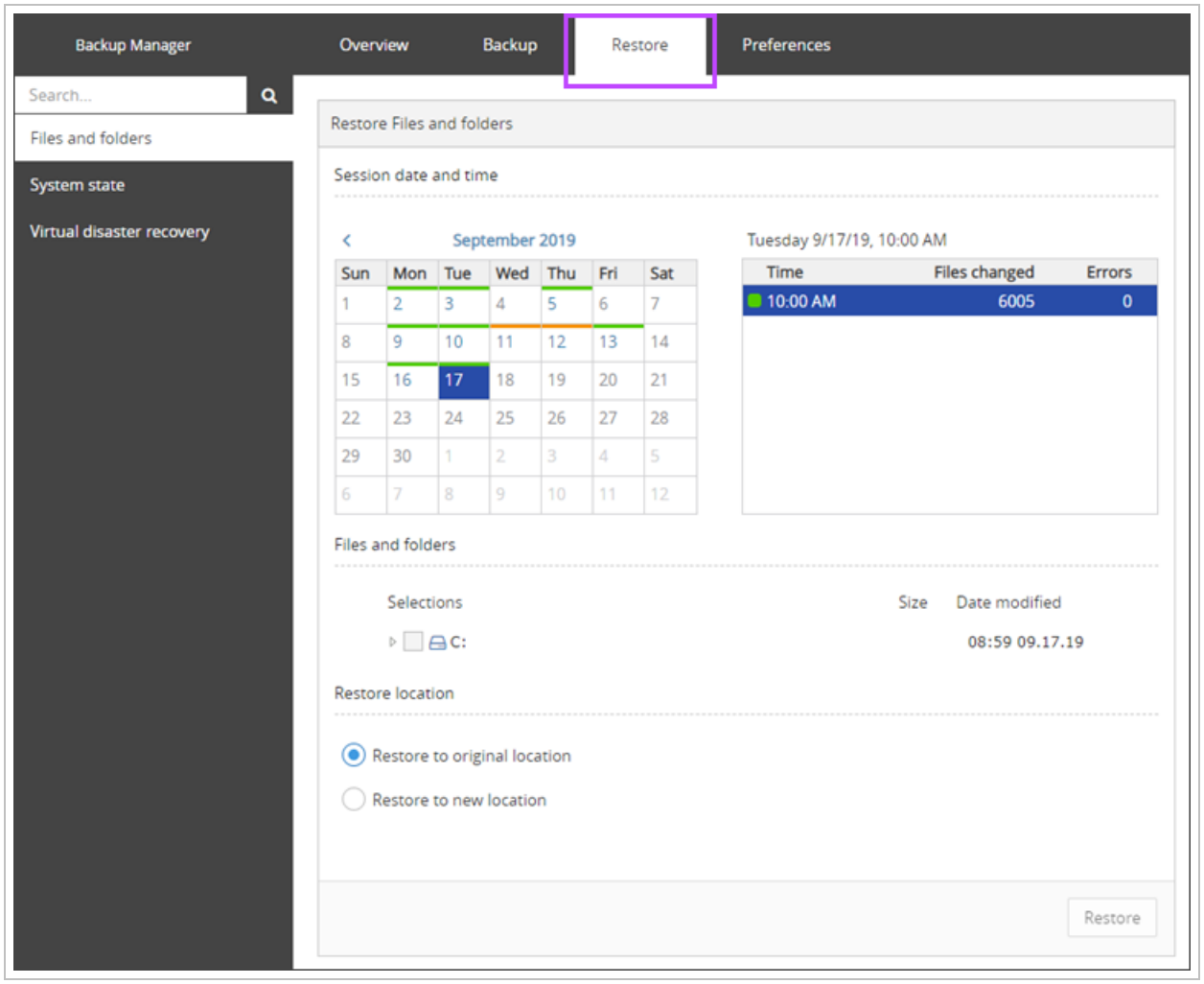
For instructions on restore MySQL databases, see How in-place restores work.

1. If you wish to restore data to a different machine, install the Backup Manager on the computer or virtual machine using **restore only** mode

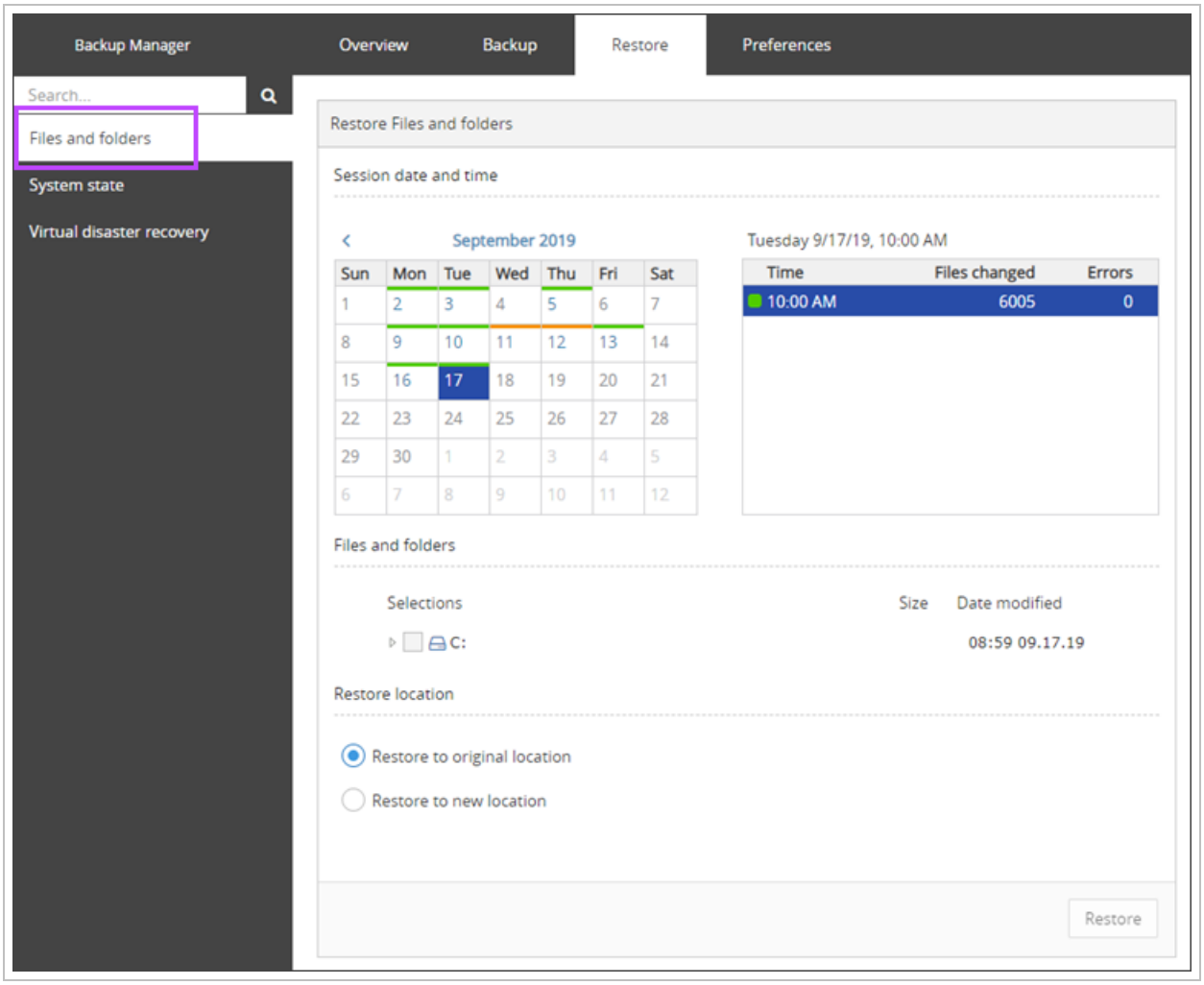
   If you are restoring date to a new device, this can be done by using Backup Manager Restore-Only Mode or our Recovery Console Guide tool.

2. Launch the Backup Manager for the device

3. Open the **Restore** tab

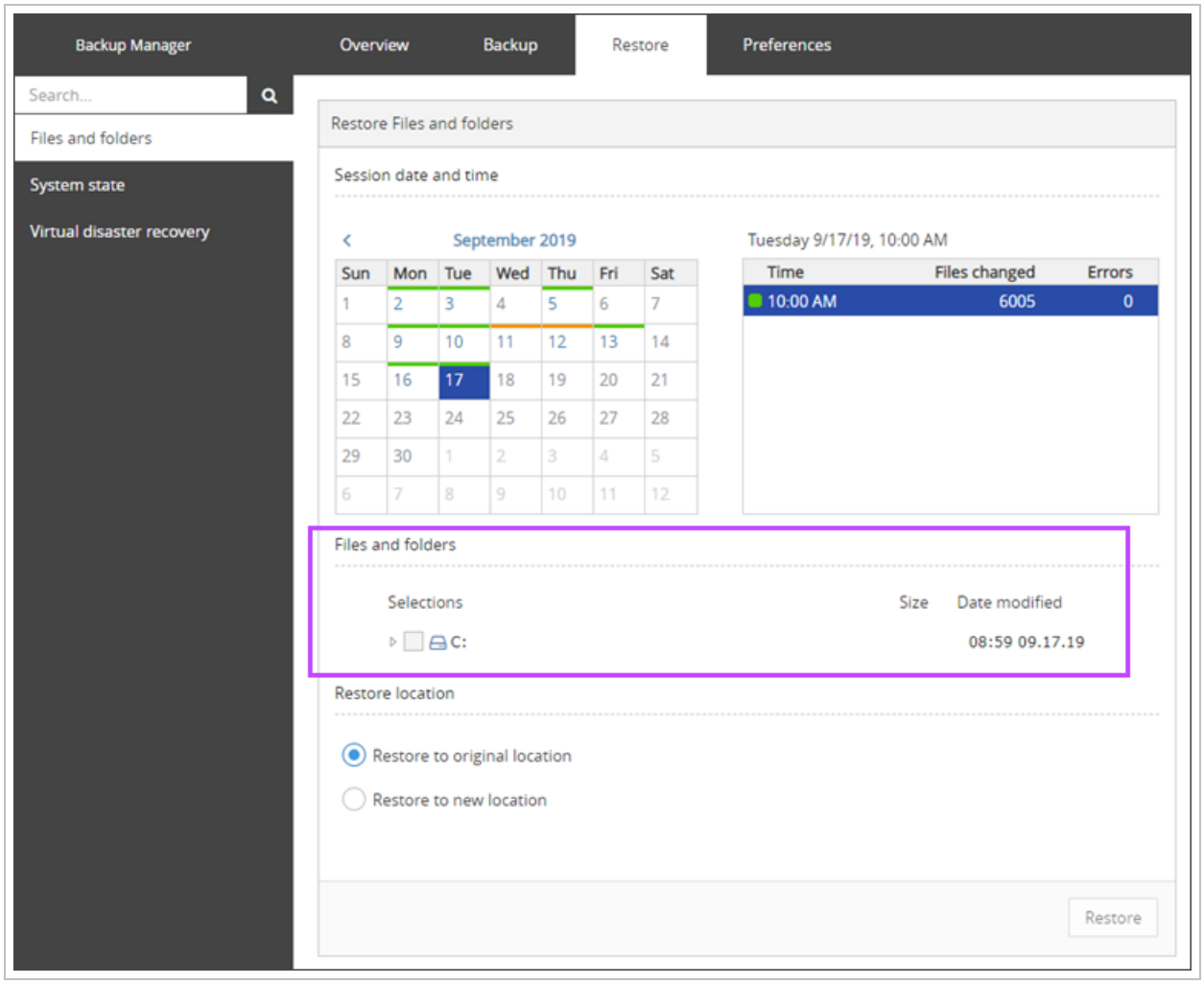


4. Select a data source from the vertical menu to the left. The selection includes all data sources that have been backed up at least once and for which data remains in retention on the current device

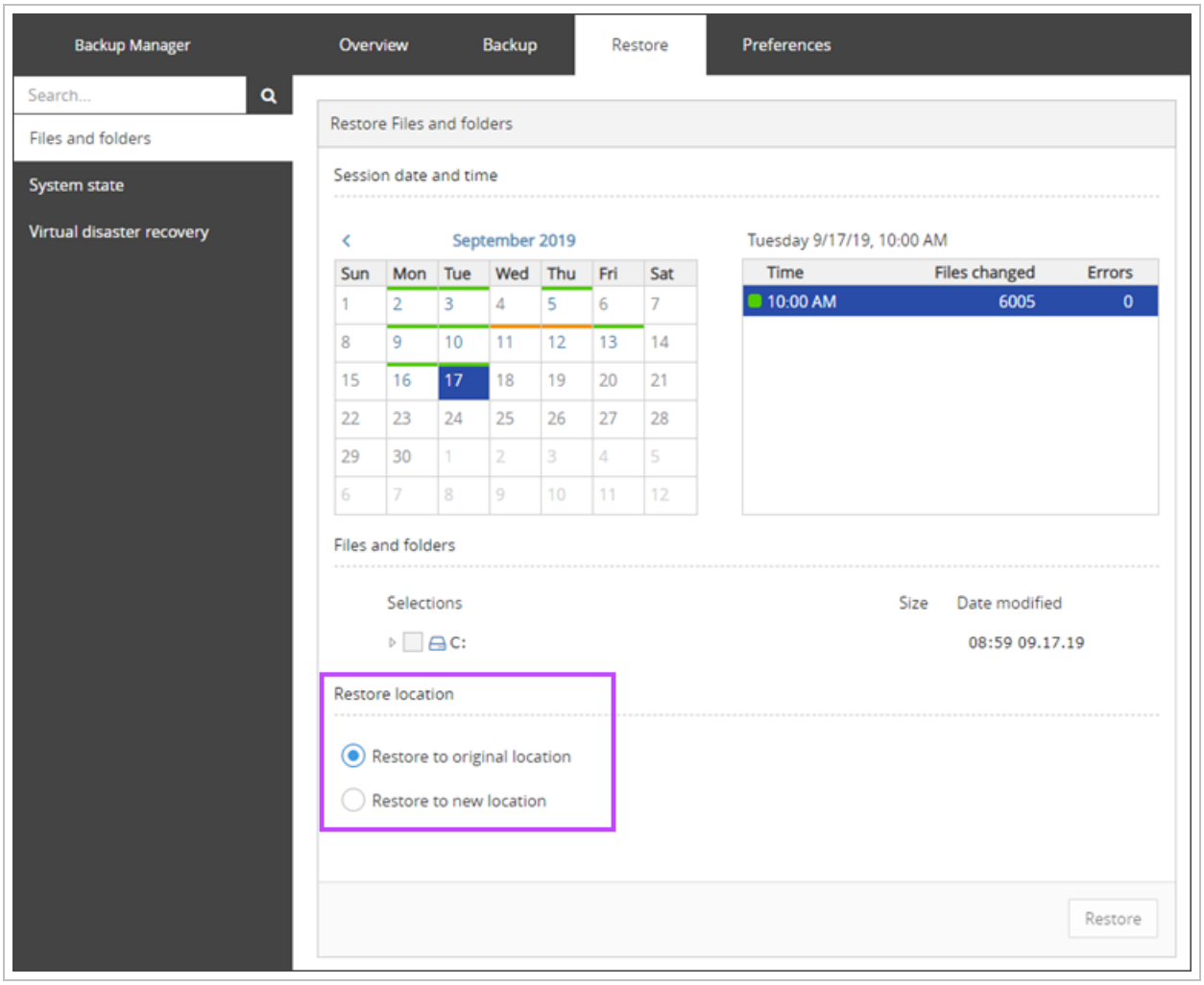


5. Select the backup session you want to restore using the date and time picker
   - **(A)** next to the name of a session means that the session is archived (more on backup session archiving)
   - **(L)** means that the session has been saved locally in the LocalSpeedVault and the data is not synchronized with the cloud yet

6. Select the data you want to restore. For some data sources like Files and folders you can expand the file tree and select individual files or directories. For other data sources only the root folder can be selected



7. Specify where to restore the selected data: to the original location or to a new one. Enter the target location, if applicable



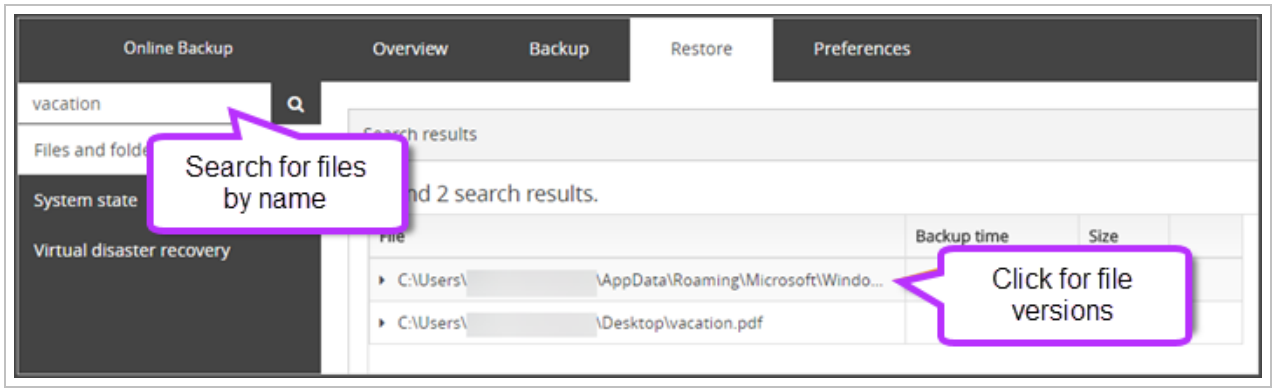
8. Click **Restore** and wait until the restore process is completed

> At this point, you can close Backup Manager in the browser while the recovery is in progress, it will continue in background

Settings

File search

If you want to restore a particular file, enter a complete or partial name into the Search field in the upper-left corner.



- The Search option does not accept wildcards or path names
- The search is not case sensitive
- When viewing the search results, you can select the most recent version of a file or expand the list of prior versions

Restore location

Two types of restores can be distinguished:

- **In-place restores** performed to the original location (the default option). This can be done if the original data is no longer there or if you want to overwrite it with a recovered version. If you choose this option, keep the **Restore to** field blank
- Restores to a **new location**. Specify a path to the target directory in the **Restore to** field

The Backup Manager installation folder is not subject to the in-place restore. This helps prevent the loss of settings, so you can be sure your backup data stays safe.

Generally, you can restore data to any of the following locations:

- Your hard drive
- A removable storage drive mapped as a fixed drive
- A network share (only for in-place restores). It must be available during the restore (it is not possible to restore data if the target computer has entered the sleeping mode or got disconnected from the local network). Also your user account must have read and write access to the target folder. E.g.

```
\\networksharename\folder
```

Or

```
\\192.0.1.1\folder
```

Skip files that have not changed

You can let Backup Manager skip content checks for files which properties have not changed since the selected backup session. This helps optimize data processing operations and reduces restore times.

Linux System Recovery

The **System State** data source cannot be backed up and restored for Linux devices using Cove Data Protection (Cove), meaning restoring a Linux system is different to recovery of a Windows device.

The following steps must be followed to restore a Linux system:

1. Reinstall the correct Linux distribution on the device
2. Download the Backup Manager installation file

   > This can be found from the Downloads page in Management Console, or from the Backup Downloads page on our website.

3. Install Backup Manager on the Linux device in **restore-only** mode:
   a. Run the installer by using the following command:

   ```
   # chmod +x mxb-linux-x86_64.run
   ```

   > We recommend that you grant the installer execute permissions using the above command

   > The installer can be run itself without permissions by using the following command:
   >
   > ```
   > # ./mxb-linux-x86_64.run
   > ```

   b. When the Backup Manager has opened in the browser, enter the device details:
      - Original device name

        > Found on the Device Properties > Settings tab in the Management Console

      - Installation key

        > Found on the Device Properties > Settings tab in the Management Console

      - Encryption Key (also known as Security Code or Passphrase)

        > If you do not know the Encryption Key or Security Code for a regularly installed device, you will need to retrieve this information before progressing. This can be done by converting the device to use passphrase-based encryption. See Convert devices to passphrase-based encryption for full details.

   c. Choose option *R* to install in **Restore-Only** mode
4. Launch the Backup Manager for the device
5. Restore the data you wish to recovery using the **Files and Folders** data source by following the Recovery Steps Instructions

Additional types of recovery in Backup Manager

We have several additional options for restoring data, see the options below for further information.

- Virtual disaster recovery guide
- Continuous restore in Backup Manager
- Seed restore in Backup Manager

Virtual disaster recovery guide

The Virtual Disaster Recovery feature lets you create a working mirror of your computer and run it in a virtual environment. The mirror can be kept up-to-date automatically through the Continuous Restore feature.

The feature is currently available on **Windows** devices. Please contact your service provider to add the Virtual Disaster Recovery to your service package (if it is not included yet).

You can perform virtual disaster recovery to the following **targets**:

- VMware VMDK (local)
- VMware ESXi (on a remote server)
- Hyper-V (local)
- Local VHD files (local, no Hyper-V installation required)

It is highly recommended to use an **isolated network** for tests. Performing virtual disaster recovery to a production environment can result in conflicts (for example, there can be 2 machines with the same IP addresses). Such conflicts lead to errors and data loss.

Please carefully check the Virtual Disaster Recovery Requirements for the correct recovery type before beginning with the Virtual Disaster Recovery Instructions.

Critical Restore? We're not the judge of when a recovery is especially time critical—you are.

Critical Restore is our partner-driven fast escalation process. Just let us know on your initial support call, email, or chat message that a specific recovery is especially time sensitive, and we'll bring all hands on deck immediately to help you get your customer back up and running ASAP.

For more details please see the Critical Restore FAQ's.

Virtual Disaster Recovery Requirements

Before you initiate Virtual Disaster Recovery (VDR), make sure both of the systems involved are supported and properly configured:

- **Source system** – This is the device that has been backed up with Backup Manager and needs to be recovered
- **Host system** – This is the device that the recovery software is installed on, where you want to restore the data to. It can be the same machine as the source system or a different one

You also need to have a note of the backup device's **Encryption key/Security code** or have access to the **Passphrase** before you begin.

Source system requirements

Supported Windows versions

The following Windows versions are supported for Virtual Disaster Recovery:

- Windows 8[1], 8.1, 10, 11 – Pro and Enterprise editions only (due to Microsoft licensing limitations)
- Windows Server 2012[2], 2012 R2, 2016, 2019 and 2022 – Standard and Data-center editions only (due to Microsoft licensing limitations)

Backup selection requirements

Make sure the following data in the source system is backed up:

1. The system state of your computer (the **System State** data source).
2. **The whole system disk** – `C:\` or another disk that has your operating system and that the operating system boots from (the **Files and Folders** data source).
3. Any other data that is important to you. Supported data sources: Files and Folders, MS Exchange, and MS SQL.

> It is possible to back up a system containing **dynamic disks**, though it should be noted that these are converted to basic disks during virtual disaster recovery.

> If a disk uses the **MBR** partition table, the total size of its volumes must not exceed **2TB**.

If in doubt concerning the selection of files, please perform a test restore or contact customer support for assistance.

Optional settings (for better restore speed)

If the data transfer speed through the Internet is not high enough, you can benefit from enabling the LocalSpeedVault in the source system.

Planning to perform recovery from another machine? Then consider placing the **LocalSpeedVault** folder on any of the following:

- A removable storage drive that you will be able to attach to the host machine.
- The host machine (if it is located on the local network).
- Another machine on the local network that is accessible from the host machine.

Host system requirements

Supported Windows versions

The following Windows versions are supported for Virtual Disaster Recovery:

---

[1] If the source machine is booted from a GPT disk (UEFI firmware), virtual disaster recovery must be performed from a recent version of Windows: Windows 8.1, Windows 10, Windows Server 2012 R2 or Windows Server 2016.
[2] If the source machine is booted from a GPT disk (UEFI firmware), virtual disaster recovery must be performed from a recent version of Windows: Windows 8.1, Windows 10, Windows Server 2012 R2 or Windows Server 2016.

- Windows 8[1], 8.1, 10, 11 – Pro and Enterprise editions only (due to Microsoft licensing limitations)
- Windows Server 2012[2], 2012 R2, 2016, 2019 and 2022 – Standard and Data-center editions only (due to Microsoft licensing limitations)

> The host system **must not be older** than the source system. For example, if you want to restore Windows 10, you must install your recovery software on Windows 10 or a newer version.

Device passphrases

To find the device name, passphrase etc. for automatically installed devices, please see Getting passphrases for automatically installed devices.

If you do not know the Encryption Key or Security Code for a regularly installed device, you will need to retrieve this information before progressing. This can be done by converting the device to use passphrase-based encryption. See Convert devices to passphrase-based encryption for full details.

Hyper-V & Local VHD

Cove Data Protection (Cove) has functionality for you to perform virtual disaster recoveries to Hyper-V targets. Hyper-V machines created for virtual disaster recovery purposes contain one or several **virtual disks** (their number equals the number of hard disks you have backed up). These virtual disks have the **VHD** or **VHDX** format. The format is determined by the version of Hyper-V and the system updates installed on your computer. Generally, VHDX disks are created on Hyper-V generation 3.0. VHD disks are created on Hyper-V 2.0.

If you do not have Hyper-V installed on the host machine, consider the "Local VHD file" target instead. It creates a **VHD** file that can be added to a virtual machine later.

Additional Required Software

The host system must have the following software installed:

1. Virtual disaster recovery software (the Backup Manager or the Recovery Console)
2. Hyper-V 2.0 or 3.0. **(Hyper-V Specific - not required for Local VHD file recovery)**

VMWare VMDK & VMWare ESXi

Cove's virtual disaster recovery feature lets you create a VMware machine in a local directory for VMDK and recover your system there.

You will find the following files in the target directory after recovery:

1. **VMX** - the primary configuration file, that can be opened with VMware Player/Workstation
2. **VMDK** - a virtual disk file, that stores the contents of the virtual machine's hard disk drive. The number of VMDK disks equals the number of hard drives in the source system

---

[1]If the source machine is booted from a GPT disk (UEFI firmware), virtual disaster recovery must be performed from a recent version of Windows: Windows 8.1, Windows 10, Windows Server 2012 R2 or Windows Server 2016.
[2]If the source machine is booted from a GPT disk (UEFI firmware), virtual disaster recovery must be performed from a recent version of Windows: Windows 8.1, Windows 10, Windows Server 2012 R2 or Windows Server 2016.

If you want to enable continuous recovery for multiple devices, consider using the **target vSphere/ESXi server** as your virtual disaster recovery host. Make sure you use the **same datacenter and storage** for the host machine and the target machine. This will give you **twofold or threefold speed increase** (confirmed by in-house tests).

Additional Required Software VMWare VMDK

The host machine must have **64-bit** virtual disaster recovery software installed (the Backup Manager or the Recovery Console).

Additional Required Software VMWare ESXi

1. VMware vSphere/VMware. All **paid 64-bit** versions are supported: 6.0, 6.5, 6.7, 7.0 and 8.0

   > Older versions of VMware may continue to work. However, as these have reached **End of Life** and are no longer supported by Microsoft, we can only offer limited support.

2. **64-bit** virtual disaster recovery software (the Backup Manager or the Recovery Console)

> **Free versions** of VMware ESXi hosts are **not supported**. However, we have two workaround options available for these versions:
>
> 1. Create a new virtual machine with required characteristics and perform bare metal recovery there (recommended as a faster option)
> 2. Perform virtual disaster recovery to a VMDK file. Use VMware vCenter Converter to convert the local VMDK file from the workstation format to the appropriate format and to attach it to the ESXi server

> For restore purposes, you **must** ensure the version of VMWare ESXi on the host device is the same or higher as is on the source device.

Once these requirements are met, carefully follow the Virtual Disaster Recovery Instructions to enable VDR for the appropriate target.

Virtual Disaster Recovery Instructions

You can perform virtual disaster recovery using either of these tools:

1. The Backup Manager - lets you recover data from one device to either the same source device or a new one
2. The Recovery Console - lets you recover data from multiple devices simultaneously to a new device

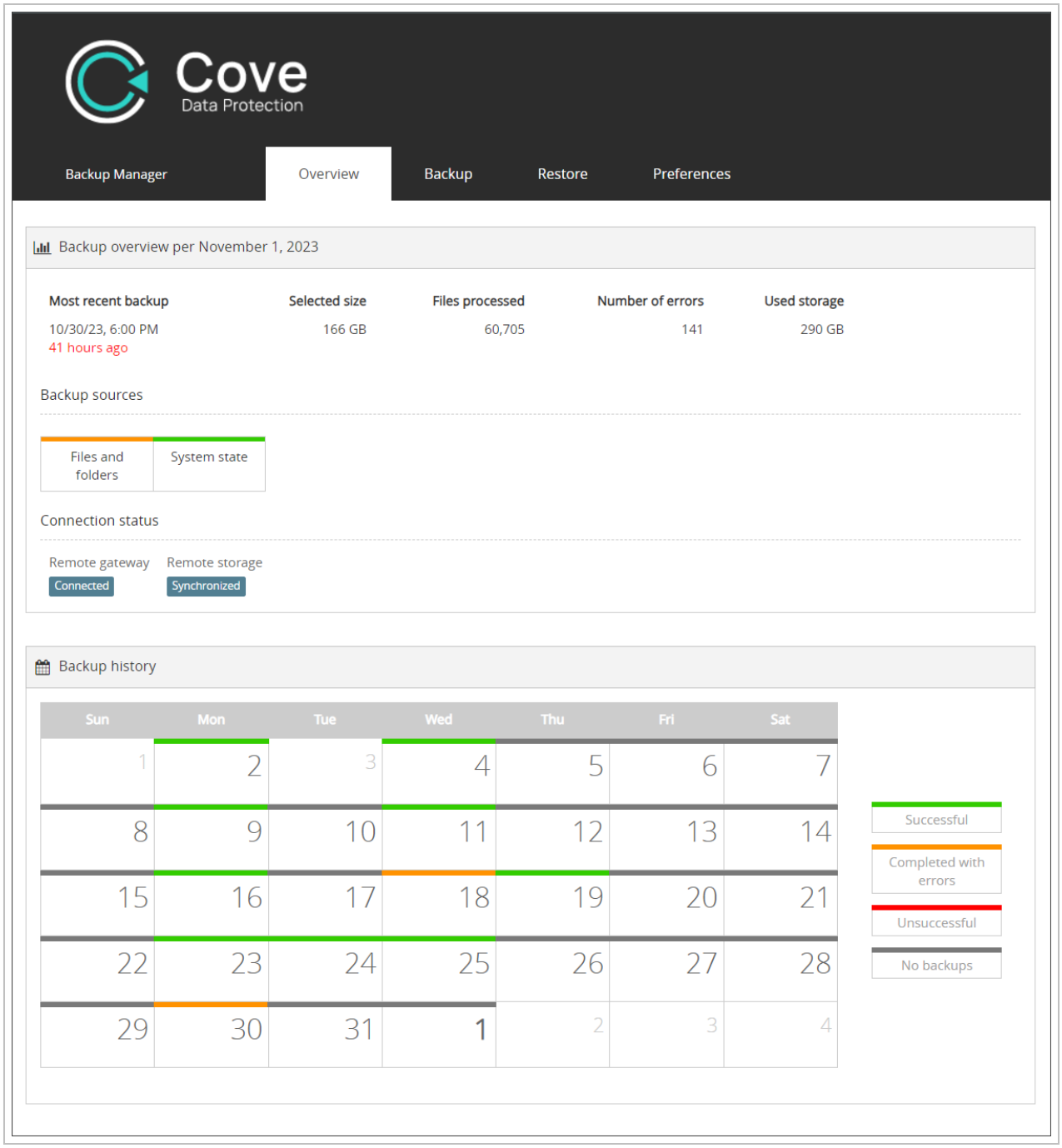
Both of the tools support one-time restores and Continuous Restore.

> Before beginning the Virtual Disaster Recovery, all Virtual Disaster Recovery Requirements **must** be met for the relevant recovery target.

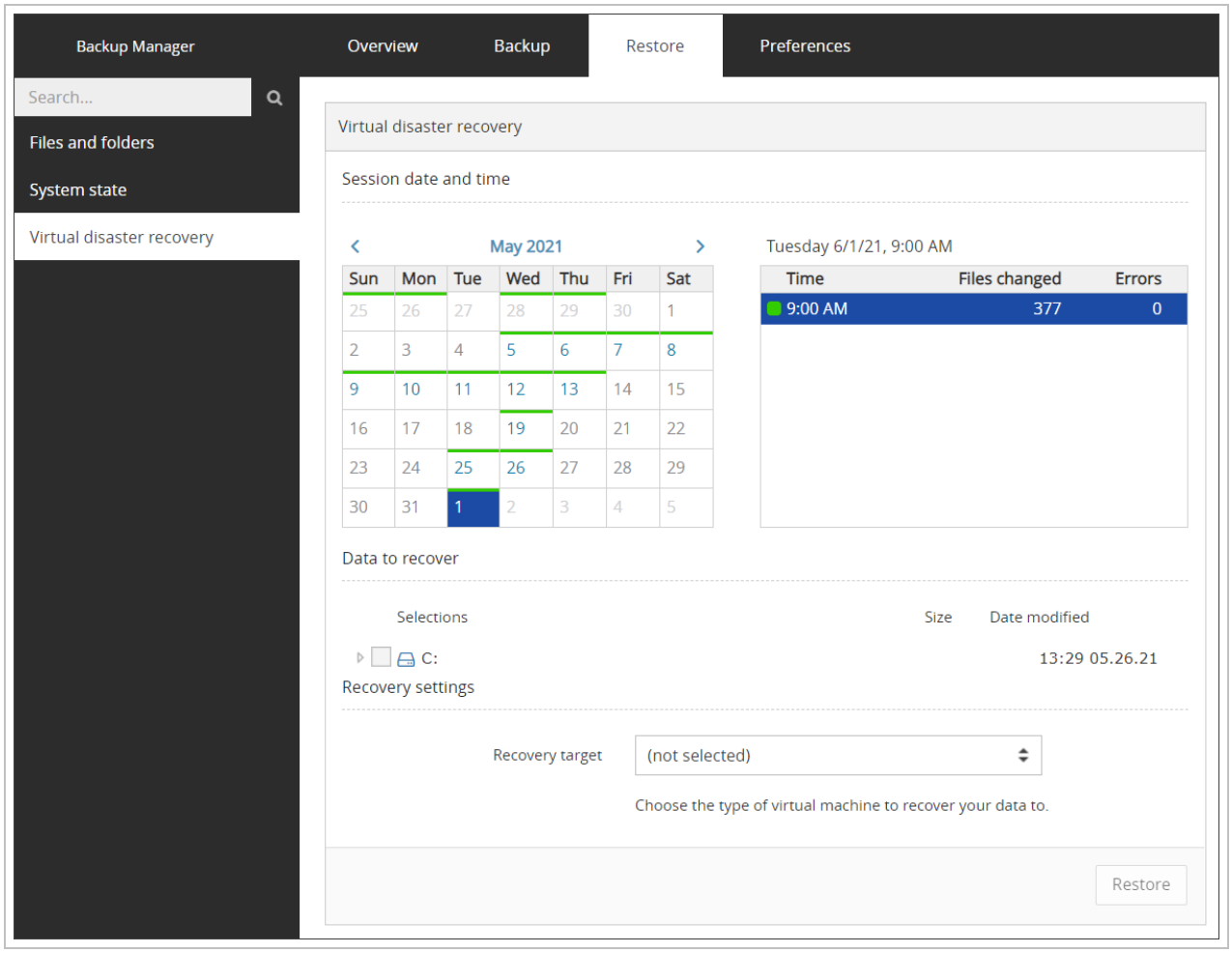
Backup Manager instructions

To perform virtual disaster recovery through the Backup Manager:

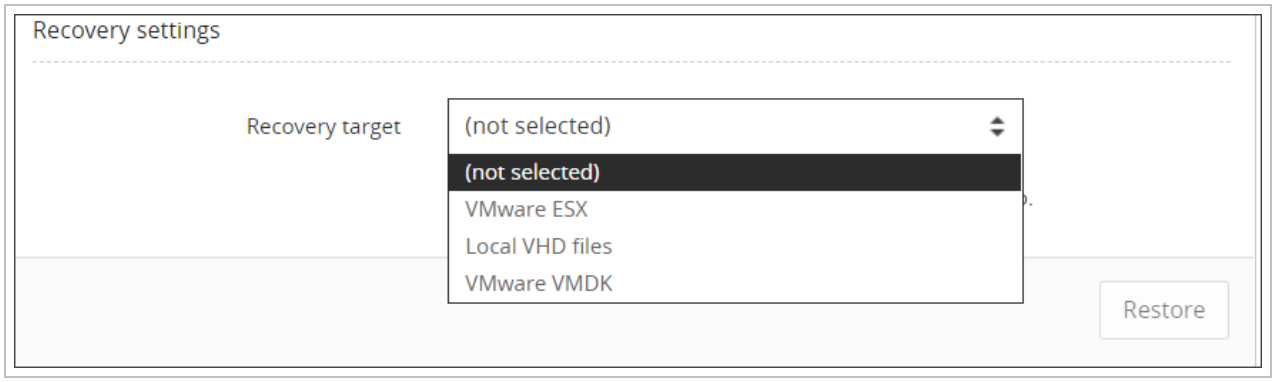
1. Launch the Backup Manager for the device



2. Navigate to the **Restore** tab
3. Click **Virtual Disaster Recovery** from the left-hand sources list



4. Using the calendar, find the session date and time you wish to restore from
5. Select the data to recover
6. In the **Recovery Target** dropdown, select the type of target you want to recover the data to

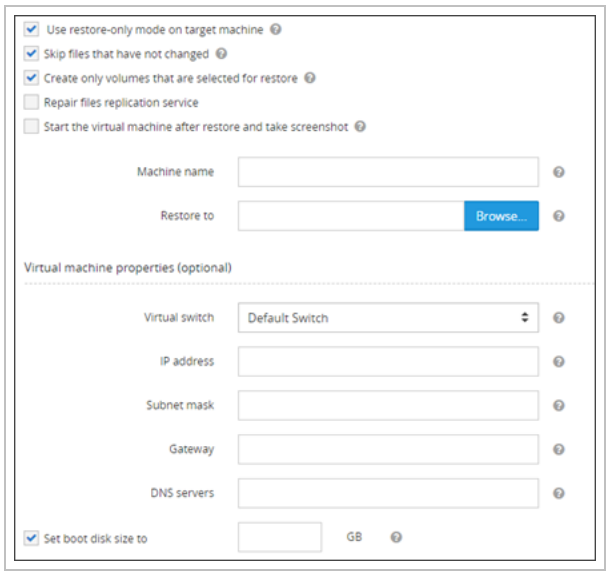


This list is adaptive, so will only show recovery targets that are available on the host device.

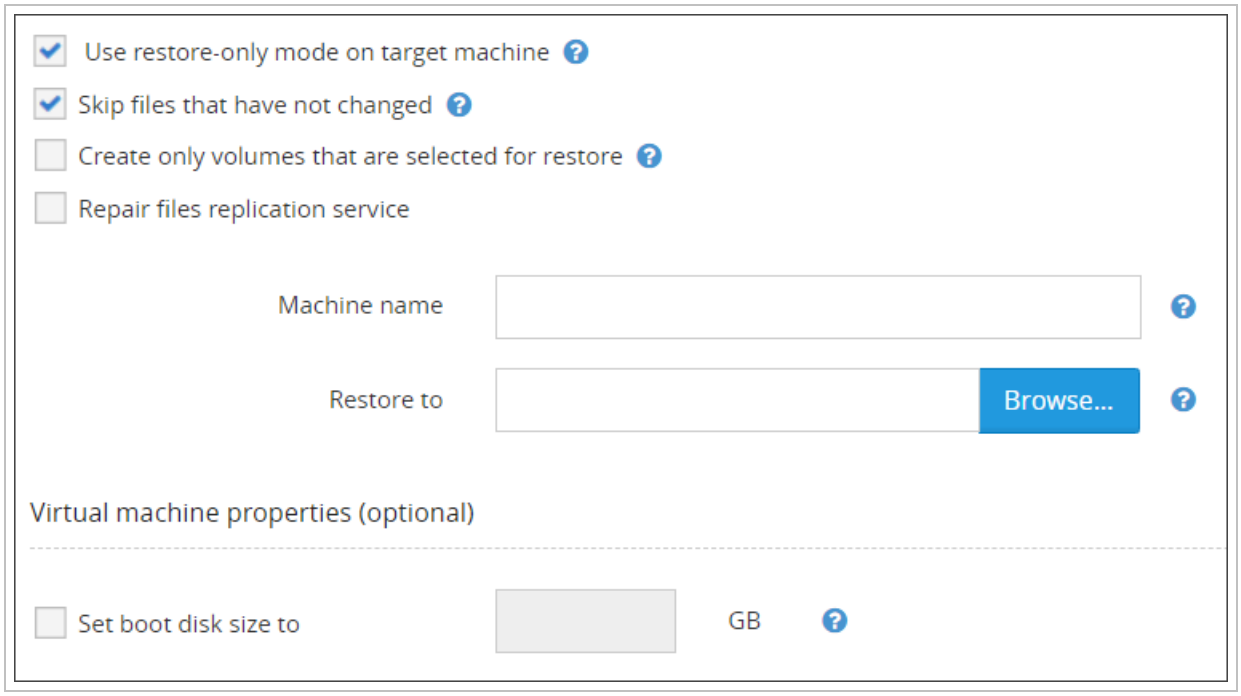
7. Fill out all settings fields for the target used before clicking **OK**

   See the Virtual Disaster Recovery Settings **page** for full details on required and optional settings for each recovery target:

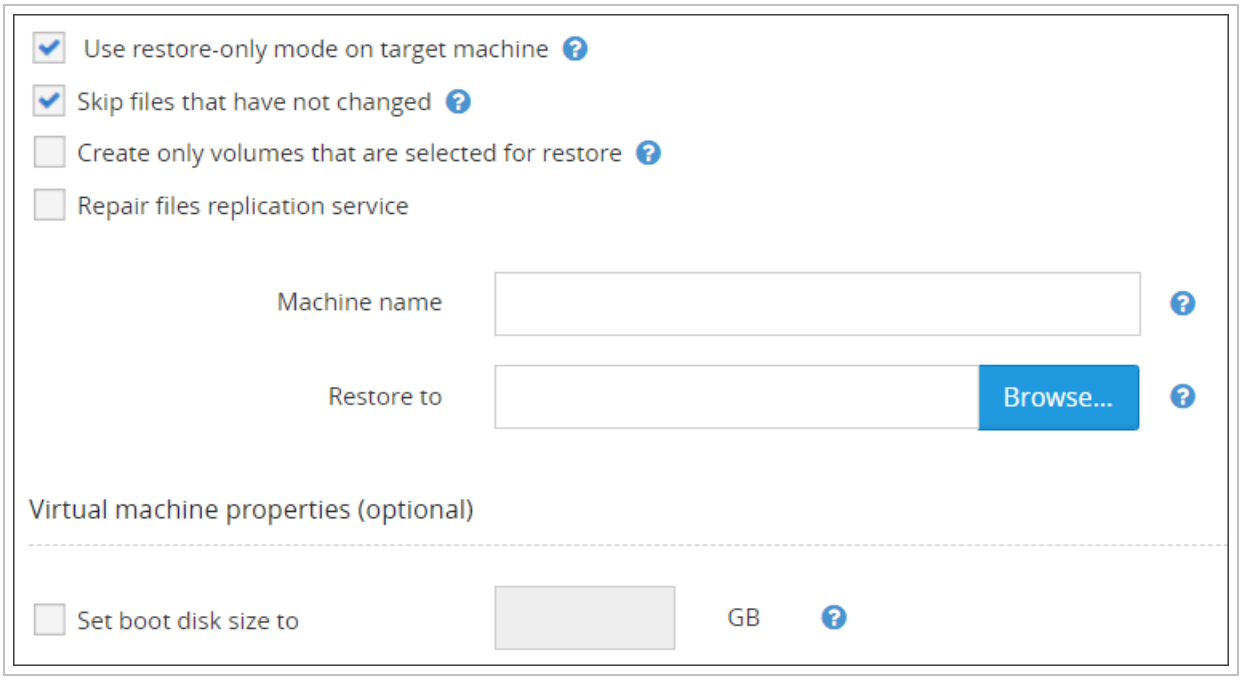
   Hyper-V:



   Local VHD files:



   VMWare VMDK:


Use restore-only mode on target machine
Skip files that have not changed
Create only volumes that are selected for restore
Repair files replication service
Machine name
Restore to
Browse...
Virtual machine properties (optional)
Set boot disk size to
GB

VMWare ESXi:

- [x] Use restore-only mode on target machine
- [x] Skip files that have not changed
- [ ] Create only volumes that are selected for restore
- [ ] Repair files replication service
- [ ] Start the virtual machine after restore and take screenshot

Access to remote ESX server

Server address

Username

Password Connect

Access to virtual machine

Machine name

Data center Select an Option

Host Select an Option

Storage Select an Option

Resource pool Select an Option

Virtual machine properties (optional)

IP address

Subnet mask

Gateway

DNS servers

- [ ] Set boot disk size to GB

8. Click **Restore** to start a recovery process

   Once the Virtual Disaster recovery begins, you will see a banner appear tracking the restore process in the Backup Manager.

> The length of time the recovery takes depends on the size of the system you are restoring, the data transfer speed, and the performance of your computer.

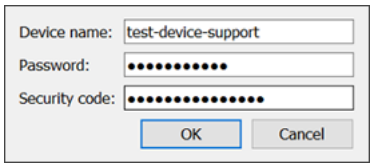
Recovery Console instructions from the most recent session

To perform virtual disaster recovery through the Recovery Console:

1. Start the Recovery Console on the host system
2. If the device already exists, move to step #3. If the device is not listed, you should add it first.

   ### To add a device:

   a. Click **Add**

   b. Fill in the device details:

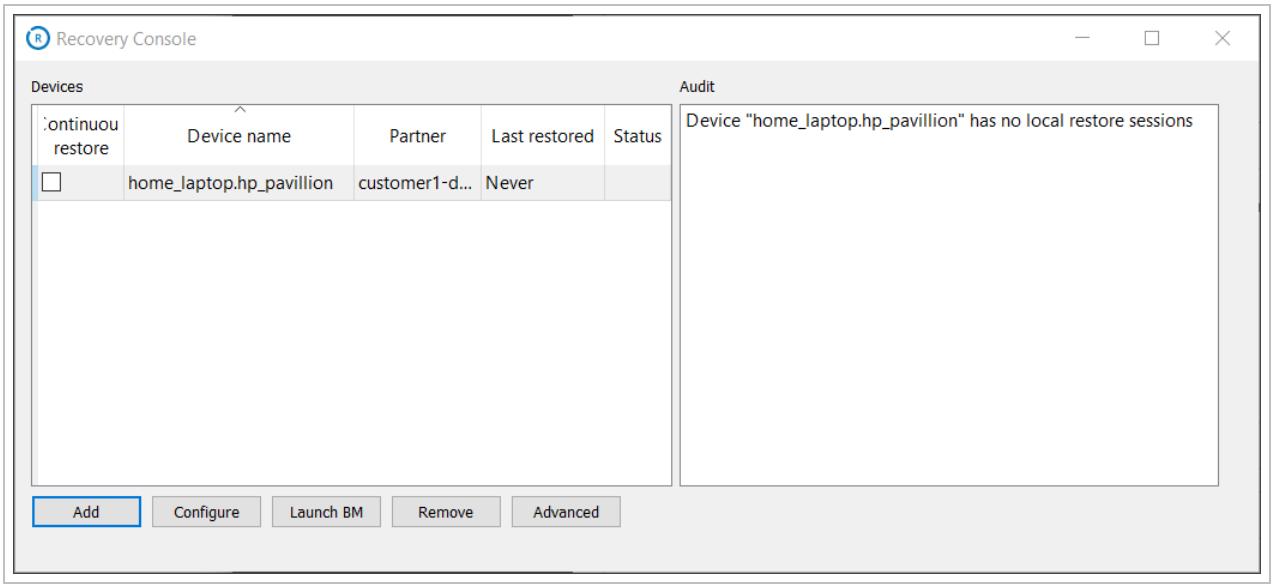
   - **Device name** - The device name as was given when Backup Manager was initially installed. This can be found on the Settings tab of the device in the Management Console.
   - **Password** - The device's Installation Key which can be found on the Settings tab of the device in the Management Console
   - **Security code** - This Is also known as the **Encryption Key** or **Passphrase** if the device was automatically installed or you have converted the device to use passphrase-based encryption.

     #### Device passphrases

     To find the device name, passphrase etc. for automatically installed devices, please see Getting passphrases for automatically installed devices.

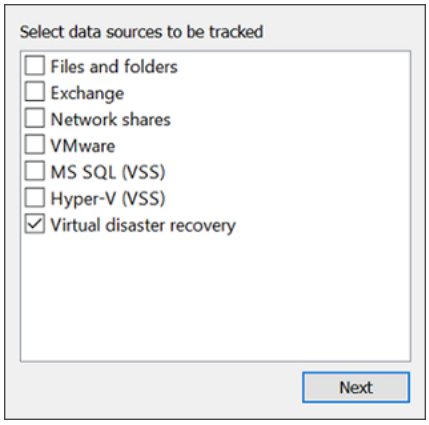
     If you do not know the Encryption Key or Security Code for a regularly installed device, you will need to retrieve this information before progressing. This can be done by converting the device to use passphrase-based encryption. See Convert devices to passphrase-based encryption for full details.

   c. Click **OK**



If the source device is already added but the Virtual Disaster Recovery source is not configured, select the device from the devices panel and then click **Configure**.

3. From the list of data sources, choose **Virtual disaster recovery**



4. From the **Restore target** list, choose the type of virtual machine you want to recover your system to

> The VDR **restore target** list is not adaptive, meaning it will show all recovery targets, even ones that are not available on the host device.

5. Fill out all settings fields for the target used

   See the Virtual Disaster Recovery Settings **page** for full details on required and optional settings for each recovery target. For example:

   Hyper-V:

Settings for device "home_laptop.hp_pavillion"

Virtual disaster recovery

Restore target HyperV

- [x] Use restore-only mode on target machine
- [x] Skip files that have not changed
- [x] Remove obsolete data from target computer
- [ ] Create only volumes that are selected for restore
- [ ] Change the FRS and DFSR services to authoritative
- [ ] Start the virtual machine after restore and take screenshot

Recover the data to a new virtual machine running on MS Hyper-V.

Restore tree

- [x] Virtual disaster recovery
  - [x] C:
  - [x] D:

HyperV role is not available on this machine: inplace HyperV restore is impossible

Access to virtual machine

Machine name

Location Browse

Virtual switch

Virtual machine properties (optional)

Boot disk size (GB)

IP address

Subnet mask

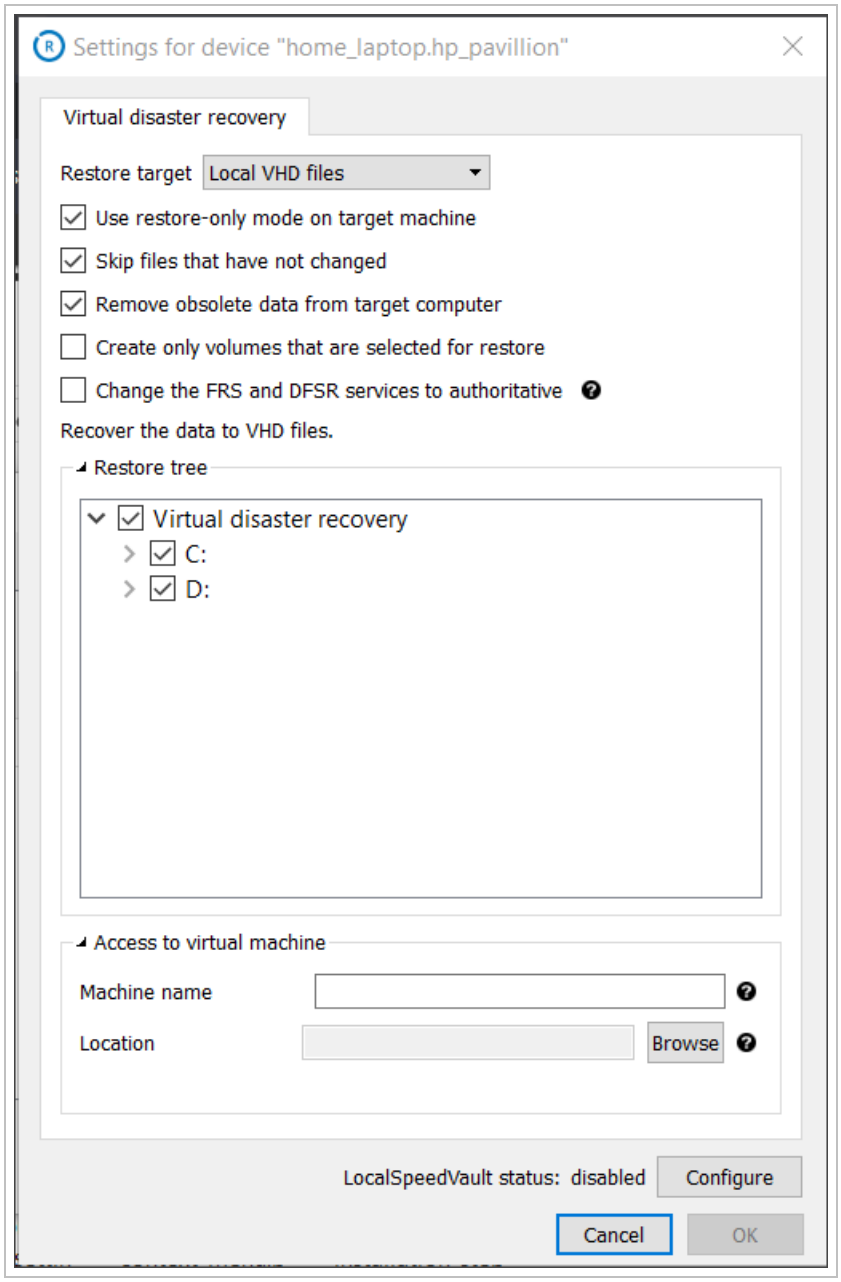
Gateway

DNS server

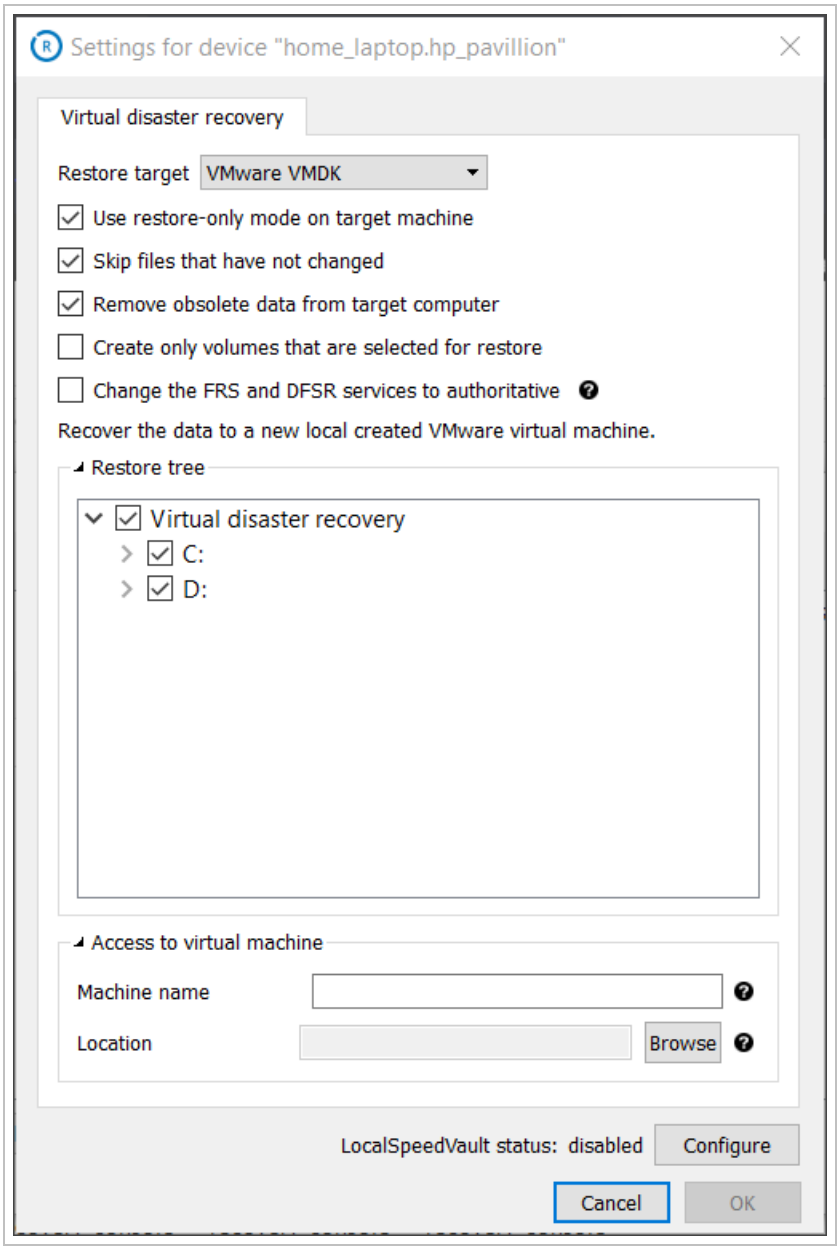
LocalSpeedVault status: disabled Configure

Cancel OK

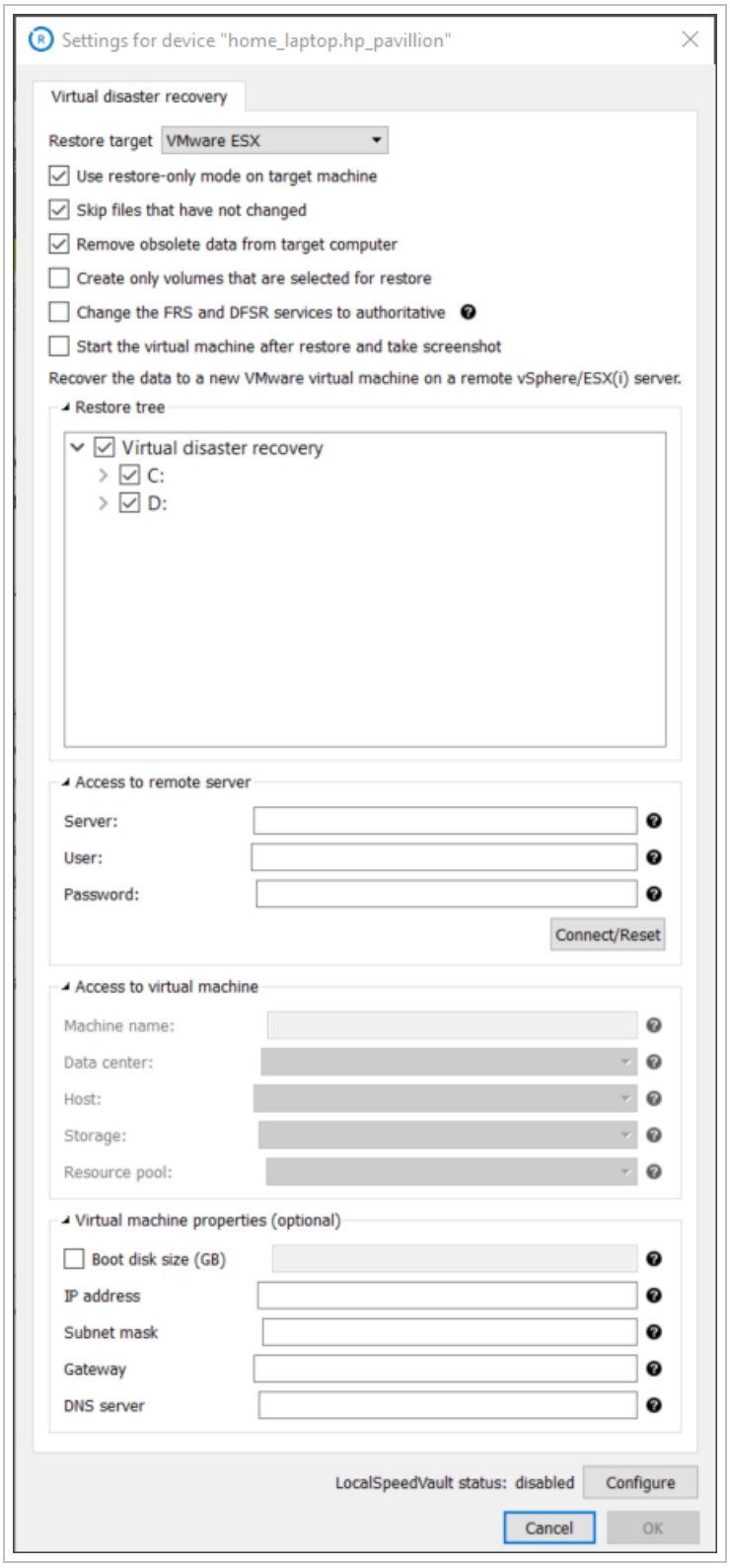
Local VHD files:



VMWare VMDK:


Settings for device "home_laptop.hp_pavillion"
Virtual disaster recovery
Restore target
VMware VMDK
Use restore-only mode on target machine
Skip files that have not changed
Remove obsolete data from target computer
Create only volumes that are selected for restore
Change the FRS and DFSR services to authoritative
Recover the data to a new local created VMware virtual machine.
Restore tree
Virtual disaster recovery
C:
D:
Access to virtual machine
Machine name
Location
Browse
LocalSpeedVault status: disabled
Configure
Cancel
OK

VMWare ESXi:


Settings for device "home_laptop.hp_pavillion"
Virtual disaster recovery
Restore target
VMware ESX
Use restore-only mode on target machine
Skip files that have not changed
Remove obsolete data from target computer
Create only volumes that are selected for restore
Change the FRS and DFSR services to authoritative
Start the virtual machine after restore and take screenshot
Recover the data to a new VMware virtual machine on a remote vSphere/ESX(i) server.
Restore tree
Virtual disaster recovery
C:
D:
Access to remote server
Server:
User:
Password:
Connect/Reset
Access to virtual machine
Machine name:
Data center:
Host:
Storage:
Resource pool:
Virtual machine properties (optional)
Boot disk size (GB)
IP address
Subnet mask
Gateway
DNS server
LocalSpeedVault status: disabled
Configure
Cancel
OK

6. Click **OK**

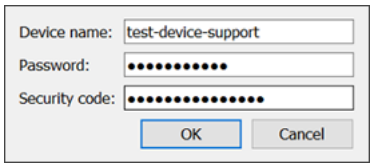
The Recovery Console will offer you to start data recovery for the device. Click **Yes** to continue or click **No** to add the device without recovering data (you will be able to do it any time later using the **Continuous restore** checkbox).

The length of time the recovery takes depends on the size of the system you are restoring, the data transfer speed, and the performance of your computer.

Recovery Console instructions from a specific session date or time

To perform virtual disaster recovery from a specific date or time session through the Recovery Console:

1. Start the Recovery Console on the host system.
2. If the device already exists, move to step #3. If the device is not listed, you should add it first.
   ### To add a device:
   a. Click **Add**

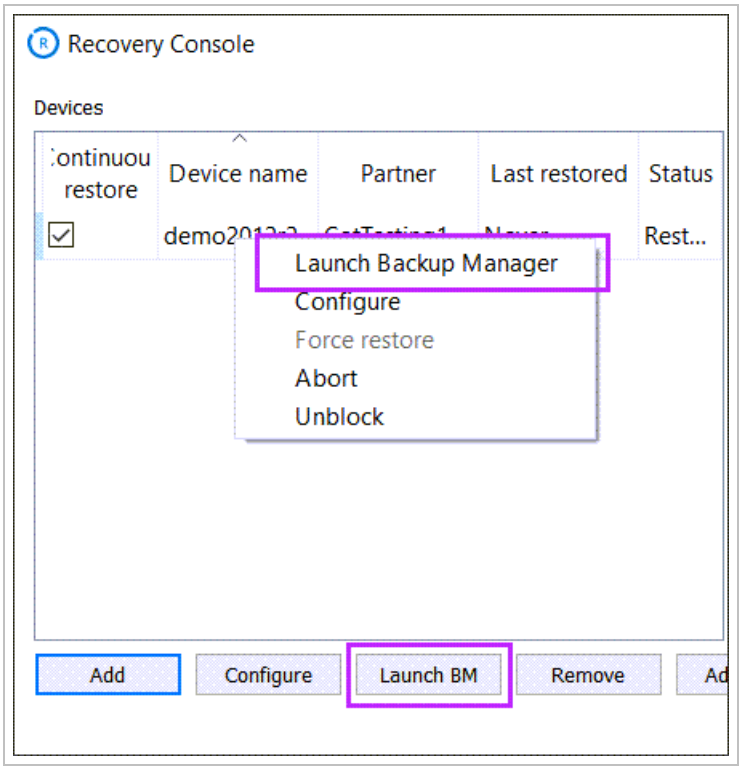
   b. Fill in the device details:
      - **Device name** - The device name as was given when Backup Manager was initially installed. This can be found on the Settings tab of the device in the Management Console.
      - **Password** - The device's Installation Key which can be found on the Settings tab of the device in the Management Console
      - **Security code** - This Is also known as the **Encryption Key** or **Passphrase** if the device was automatically installed or you have converted the device to use passphrase-based encryption.

        #### Device passphrases

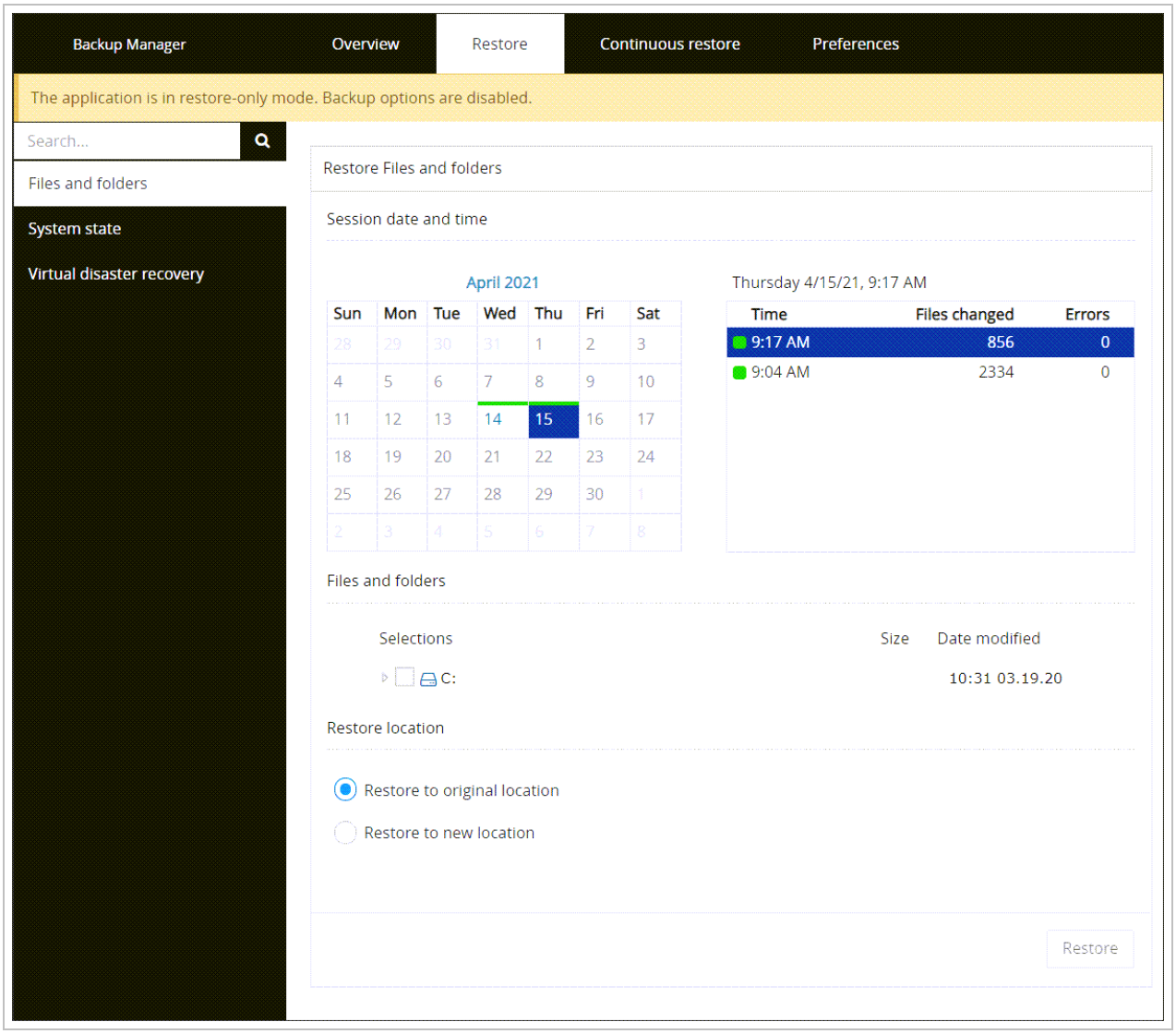
        To find the device name, passphrase etc. for automatically installed devices, please see Getting passphrases for automatically installed devices.

        If you do not know the Encryption Key or Security Code for a regularly installed device, you will need to retrieve this information before progressing. This can be done by converting the device to use passphrase-based encryption. See Convert devices to passphrase-based encryption for full details.

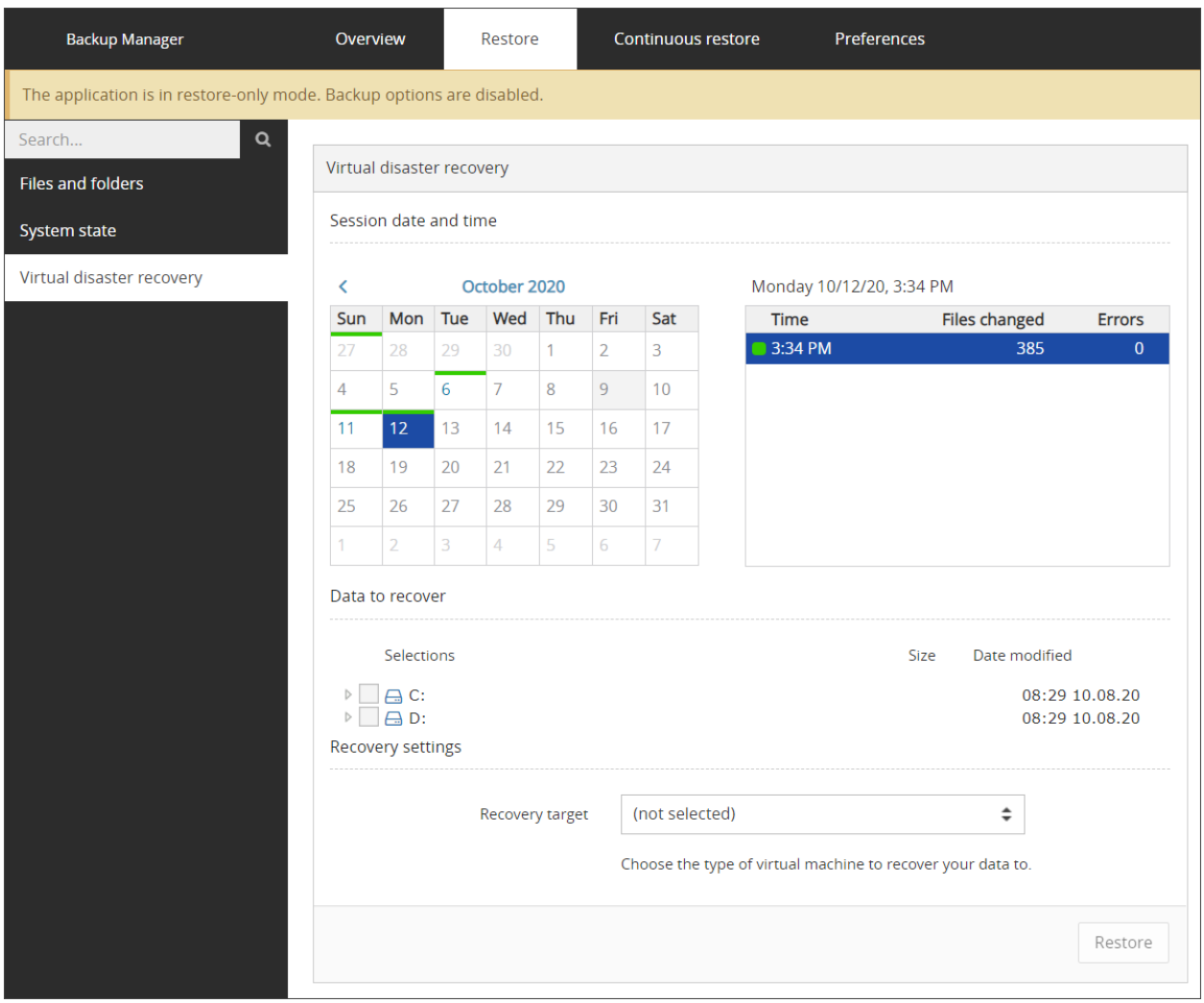
   c. Click **OK**
3. Highlight the device you wish to do the Virtual Disaster Recovery for and either click the **Launch BM** button or right-click and select **Launch Backup Manager**



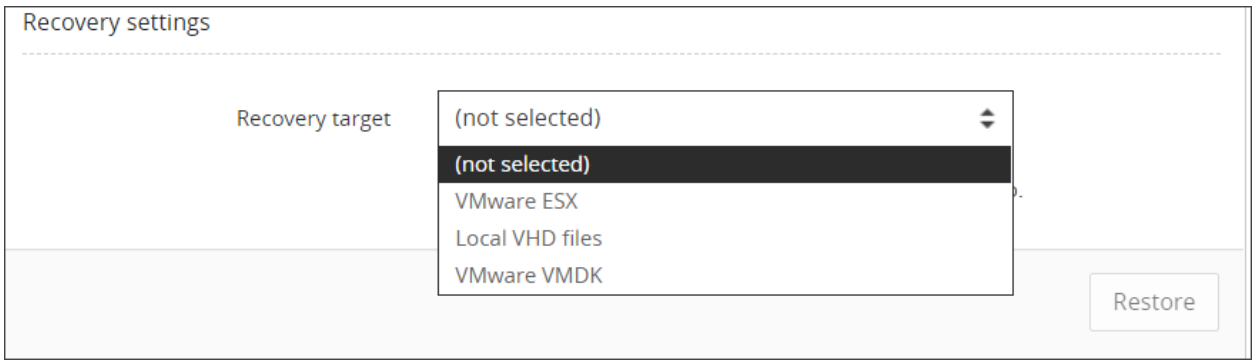
4. The device's Backup Manager will open in your browser in **Restore Only** mode, displaying a banner stating so



5. Navigate to the **Restore** tab
6. Click **Virtual Disaster Recovery** from the left hand sources list



7. Using the calendar, find the session date and time you wish to restore from
8. Select the data to recover
9. In the **Recovery Target** dropdown, select the type of target you want to recover the data to

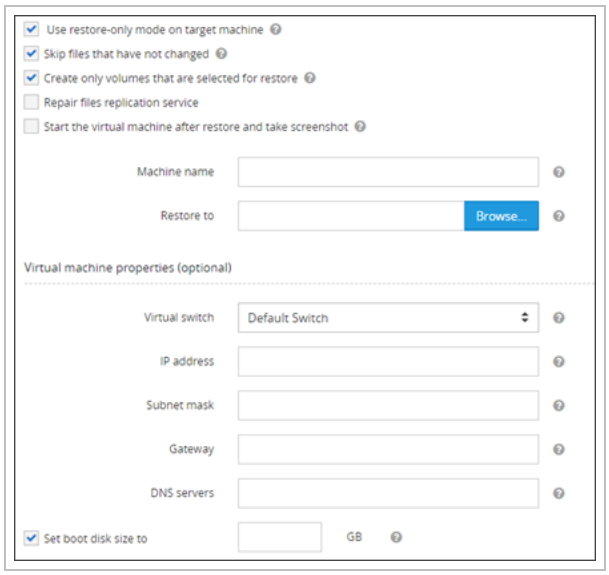


This list is adaptive, so will only show recovery targets that are available on the host device.

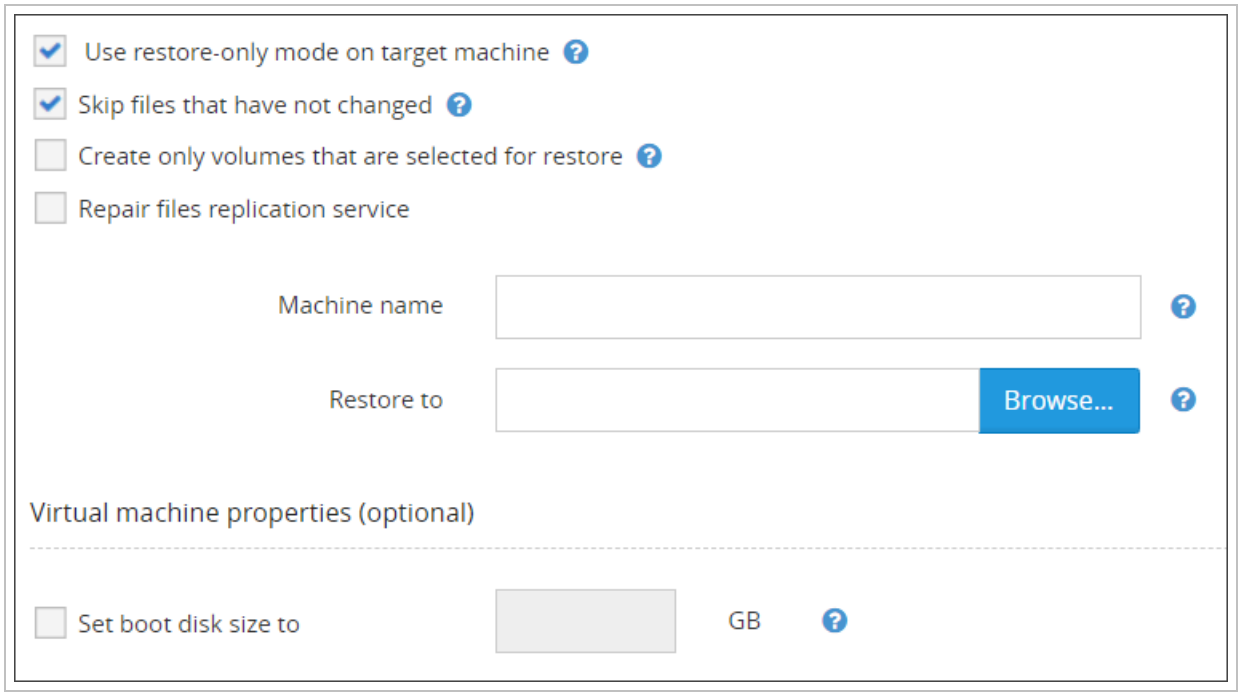
10. Fill out all settings fields for the target used

See the Virtual Disaster Recovery Settings **page** for full details on required and optional settings for each recovery target:

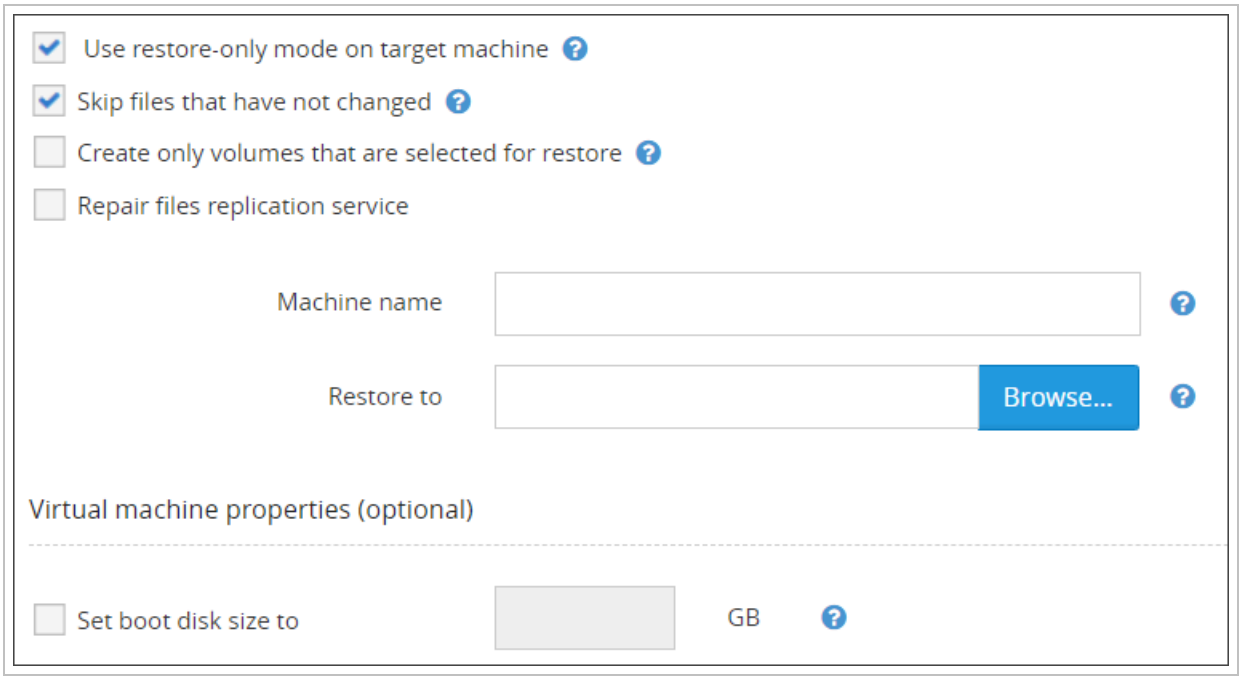
Hyper-V:



Local VHD files:



VMWare VMDK:


Use restore-only mode on target machine
Skip files that have not changed
Create only volumes that are selected for restore
Repair files replication service
Machine name
Restore to
Browse...
Virtual machine properties (optional)
Set boot disk size to
GB

VMWare ESXi:

- [x] Use restore-only mode on target machine
- [x] Skip files that have not changed
- [ ] Create only volumes that are selected for restore
- [ ] Repair files replication service
- [ ] Start the virtual machine after restore and take screenshot

Access to remote ESX server

Server address

Username

Password Connect

Access to virtual machine

Machine name

Data center Select an Option

Host Select an Option

Storage Select an Option

Resource pool Select an Option

Virtual machine properties (optional)

IP address

Subnet mask

Gateway

DNS servers

- [ ] Set boot disk size to GB

11. Click **Restore** to start a recovery process

    Once the Virtual Disaster recovery begins, you will see a banner appear tracking the restore process in the Backup Manager.

> The length of time the recovery takes depends on the size of the system you are restoring, the data transfer speed, and the performance of your computer.

Virtual disaster Recovery for Linux

> Support for Virtual Disaster Recovery on **Linux devices** has ceased.

Virtual Disaster Recovery Settings

Settings for a successful Virtual Disaster Recovery (VDR) will depend on the recovery target used.

Hyper-V, Local VHD, VMWare VMDK

The Hyper-V, Local VDH and VMWare VMDK recovery targets all share the same two required settings:

- **Machine name** - A name that you want to assign to the target virtual machine. If you keep the field blank, it will be automatically populated with the name of your backup device
- **Restore to** - Specify a path to the directory where your new virtual machine will be created

These recovery targets share the following optional settings:

- **Set boot disk size to ...** - Use this setting to customize the size to the system disk created on the virtual machine (by default, the new disk is the same size as the original)

  > If the disk contains several partitions, you cannot reduce the original size by more than the amount of free space on the last partition. For example, if the total size of the disk is 100 GB and the last partition has 10 GB of free space, you can set the value to 90 or more.

- **Use restore-only mode on target machine** - This setting helps prevent unwanted backups from running on the recovered virtual machine
- **Skip files that have not changed** - This setting can be used to optimize data recovery operations and increases recovery speed. It applies to subsequent restore sessions not the initial restore session in which the whole amount of data is transferred
- **Create only volumes that are selected for restore** - When this setting is on, the target virtual machine will contain only those disks that have data selected for recovery. When off, and no data from a disk is selected for recovery, the virtual disk is created without any data

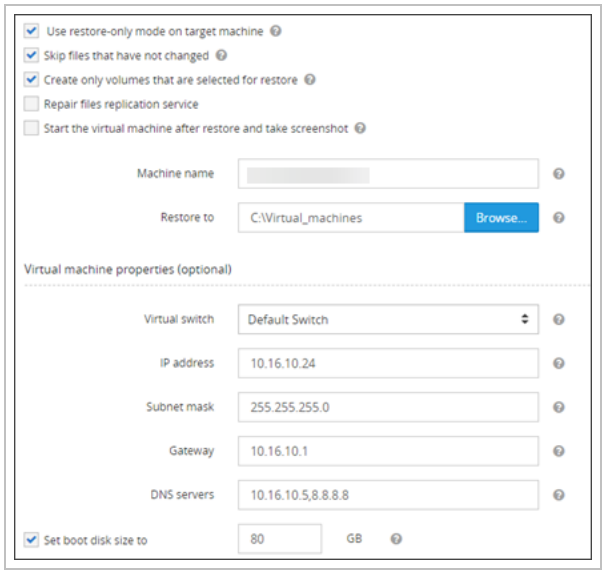
  > The setting is ignored if the disk you have excluded from recovery contains critical data. Such a thing can happen if your recovery selection includes MS Exchange or MS SQL and some files belonging to these data sources are located on the excluded disk. In this case the disk is created and populated with the files required by MS Exchange and MS SQL.

- **Repair files replication service** - If you are restoring Active Directory with multiple domain controllers, you should change the FRS and DFSR services to authoritative in the domain controller that will be started in the first place. Avoid marking several FRS/DFSR services as authoritative in the production environment as it can result in data loss. When the feature is on, the FRS and DFSR services are started on the target VM in the authoritative mode. The NETLOGON and SYSVOL shares become available, so the Active Directory and DNS services become functional again

  More information about FRS/DFSR is available in the Microsoft Knowledge Base. Article IDs: KB2218556, kbinfo KB290762.

Additional Hyper-V Optional Settings

The Hyper-V recovery target has several additional optional settings to allow for more customization:



- **Virtual machine properties** - You can assign **custom properties** to the new virtual machine:
  - **Virtual switch** - choose the Hyper-V network adapter that will be used by your new virtual machine. The selection of available adapters is detected automatically
  - **DNS servers** - assign the list of custom DNS servers (separated by comma)

    Example: `8.8.8.8` or `8.8.8.8,7.7.7.7`
  - **IP address** - assign a custom IP address to the virtual machine
  - **Subnet mask** - assign a custom subnet mask to the virtual machine
  - **Gateway** - assign a custom gateway to the virtual machine

- **Start the virtual machine after restore and take screenshot** - If the option is enabled, the new virtual machine is booted up after recovery and a confirmation screenshot is created. The results of virtual disaster recovery sessions together with screenshots of the booted systems come in email notifications (a special notification rule has to be activated by the service provider or system administrator)

  The screenshots are also available in the Management Console (see the "Virtual Disaster Recovery data session verification details (restore)" column in the **Device Management** module)

Important: Use the feature carefully if there is another virtual machine in the local network offering the same services (for example, the Active Directory) as it can result in a conflict with subsequent data loss.

VMWare ESXi

The VMWare EXSi recovery target has different required and optional settings to the others:

- [x] Use restore-only mode on target machine
- [x] Skip files that have not changed
- [ ] Create only volumes that are selected for restore
- [ ] Repair files replication service
- [ ] Start the virtual machine after restore and take screenshot

Access to remote ESX server

Server address: server-address.here

Username: username1

Password: ••••••••• Connect

These settings will not become available until you connect to the server

Machine name: test-lab-b2

Data center: Select an Option

Host: Select an Option

Storage: Select an Option

Resource pool: Select an Option

Virtual machine properties (optional)

IP address:

Subnet mask:

Gateway:

DNS servers:

- [ ] Set boot disk size to GB

Required settings

There are two sections of the VMWare EXSi setup which require configuration:

1. **Access to remote ESXi server** – Enter your vSphere/ESXi server access credentials to let the recovery software access the server and create a virtual machine there
   - **Server Address** - The address to the vSphere/ESXi server
   - **Username** - The administrator login username
   - **Password** - The administrator login password
2. **Access to virtual machine** – You must assign a name to the new virtual machine. The rest of the settings are retrieved automatically after a connection to the server is established. Where options are available, you will be able to choose a suitable one from a dropdown list

Optional settings

The VMWare ESXi recovery target has the following optional settings which may be configured:

- **Set boot disk size to ...** - Use this setting to customize the size to the system disk created on the virtual machine (by default, the new disk is the same size as the original)

  > If the disk contains several partitions, you cannot reduce the original size by more than the amount of free space on the last partition. For example, if the total size of the disk is 100 GB and the last partition has 10 GB of free space, you can set the value to 90 or more.

- **Use restore-only mode on target machine** - This setting helps prevent unwanted backups from running on the recovered virtual machine
- **Skip files that have not changed** - This setting can be used to optimize data recovery operations and increases recovery speed. It applies to subsequent restore sessions not the initial restore session in which the whole amount of data is transferred
- **Create only volumes that are selected for restore** - When this setting is on, the target virtual machine will contain only those disks that have data selected for recovery. When off, and no data from a disk is selected for recovery, the virtual disk is created without any data

  > The setting is ignored if the disk you have excluded from recovery contains critical data. Such a thing can happen if your recovery selection includes MS Exchange or MS SQL and some files belonging to these data sources are located on the excluded disk. In this case the disk is created and populated with the files required by MS Exchange and MS SQL.

- **Repair files replication service** - If you are restoring Active Directory with multiple domain controllers, you should change the FRS and DFSR services to authoritative in the domain controller that will be started in the first place. Avoid marking several FRS/DFSR services as authoritative in the production environment as it can result in data loss. When the feature is on, the FRS and DFSR services are started on the target VM in the authoritative mode. The NETLOGON and SYSVOL shares become available, so the Active Directory and DNS services become functional again

  > More information about FRS/DFSR is available in the Microsoft Knowledge Base. Article IDs: KB2218556, kbinfo KB290762.

- **Start the virtual machine after restore and take screenshot** - If the option is enabled, the new virtual machine is booted up after recovery and a confirmation screenshot is created. The results of virtual disaster recovery sessions together with screenshots of the booted systems come in email notifications (a special notification rule has to be activated by the service provider or system administrator)

  > The screenshots are also available in the Management Console (see the "Virtual Disaster Recovery data session verification details (restore)" column in the **Device Management** module)

  > Important: Use the feature carefully if there is another virtual machine in the local network offering the same services (for example, the Active Directory) as it can result in a conflict with subsequent data loss.

Continuous Restore for Virtual Disaster Recovery

Virtual Disaster Recoveries can be performed **on request** or set it to the **Continuous Restore** mode where data recovery is synchronous with backups performed in the source system.

Requirements

> The Continuous Restore requires a dedicated computer or virtual machine that must not be used for other purposes (learn more).

Device passphrases

To find the device name, passphrase etc. for automatically installed devices, please see Getting passphrases for automatically installed devices.

If you do not know the Encryption Key or Security Code for a regularly installed device, you will need to retrieve this information before progressing. This can be done by converting the device to use passphrase-based encryption. See Convert devices to passphrase-based encryption for full details.

Enabling the Continuous Restore mode

Continuous Restore can be enabled either in Recovery Console or by installing Backup Manager in restore-only mode. Information on configuring this from Backup Manager can be found here: Continuous restore in Backup Manager.

Recovery Console instructions

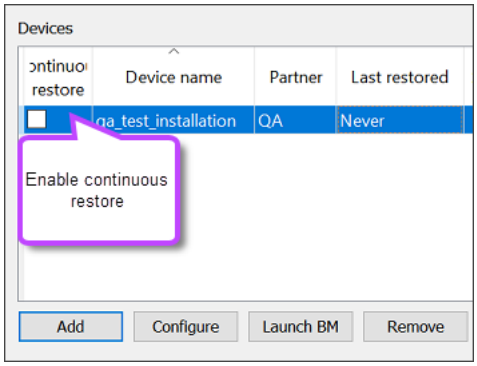
> This can be found from the Downloads page in Management Console, or from the Backup Downloads page on our website.

The Continuous Restore mode[1] is the predefined option in the Recovery Console. You can manage the setting for each device through the **Continuous Restore** checkbox to the left of each device name.

---

[1]Repeated data recovery to a computer or virtual machine that is specifically allocated for that purpose. The recovery is synchronous with backups performed in the source system.

1. Add the device to the Recovery Console following these steps
2. Once the device has been added and configured correctly, tick **Continuous Restore** which can be found to the left of the device name in the Devices panel



3. The Virtual Disaster Recovery will now begin running in Continuous Restore mode. If you need to amend any settings, this can be done by launching Backup Manager for the device and changing settings from **Continuous restore > Virtual disaster recovery**

> If you click 'Launch BM' before configuring continuous restore as above, you will find the content of the tab is greyed out and you cannot make any changes. Enable continuous restore first before launching the Backup Manager client.

Using virtual machines in-between restore sessions

The target virtual machine **is not supposed to be in use** while the Continuous Restore mode is active. If your recovery software detects that the virtual machine was started in-between restore sessions, further restores **are blocked** and a warning message appears. This is done to prevent possible data loss.

Unblocking the Continuous Restore

There are several ways to **unblock the Continuous Restore process:**

1. Click the **Unblock** button in the warning message
2. In Backup Manager, go to **Continuous restore > Virtual disaster recovery** and then click **Restore**. This will initiate a quick delta restore that will overwrite the changes at the target location (if any)
3. In the Recovery Console, right-click the device and choose **Unblock** from the context menu

After this is done, the continuous restore process will be fully functional again.

> If the virtual machine may contain changes that you want to keep, please make a copy of it before you unblock the Continuous Restore mode.

Disabling virtual machine checks

The recovery software checks if the virtual machine has been in use before each virtual disaster recovery session. If you are sure no important data is added to the virtual machine, you can **disable these checks** and have the previous version overwritten without warning messages. To do it, add `VdrRestorePolicyForceOverwrite=1` to the `[General]` section of the configuration file belonging to your recovery software.

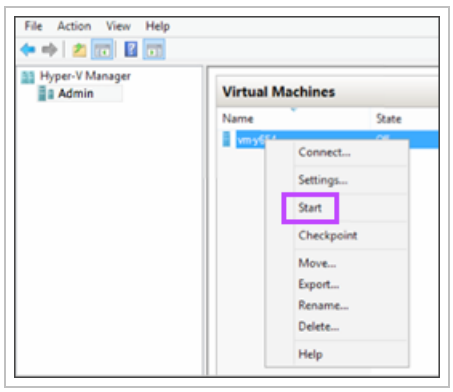
- Backup Manager instructions
- Recovery Console instructions

> The setting applies to **all** backup devices installed on the current computer (one device for the Backup Manager or multiple devices for the Recovery Console).

Hyper-V Post Virtual Disaster Recovery

Once you have completed the Virtual Disaster Recovery Instructions and the recovery process has completed for the Hyper-V Virtual Disaster Recovery, you can boot the virtual machine.

1. Open the Hyper-V Manager
2. Right-click on the new virtual machine (its name will coincide with the name you gave it during configuration, or that of the backup device if no name was given)
3. Choose **Start** from the context menu



VMWare VMDK Post Virtual Disaster Recovery

The **VMWare VMDK files** created by the Virtual Disaster Recovery have the "VMWare workstation 8" format. Such files cannot be copied to the ESXi.

Before these can be used, they must be converted to an appropriate format using a VMWare Converter.

Please see the VMWare documentation for details.

Continuous restore in Backup Manager

Backup Manager users can recover data on request or enable **automatic recovery** (Continuous Restore).

The Continuous Restore requires an additional computer (or a virtual machine) on which the same backup device is installed in restore-only mode or where Recovery Console is installed.

> For more information on configuring the continuous restore from Recovery Console, this can be found here.

> The computer or virtual machine used as the restore location **cannot** be used for other purposes.

The Backup Manager automatically synchronizes with the source computer. If any changes are detected between the source backup and current restored version, a restore takes place: this way the additional computer always has the **most current version** that mirrors the data on the source computer.

Feature availability

The Continuous Restore feature can be used on all backup devices.

> Due to the nature of the **System State** data source, it needs to be restored to a different computer (not the one on which Continuous Restore is set up). Otherwise all files and settings would get overwritten and it would not be possible to continue the auto recovery.

Limitations

There is a particular case of Continuous Restore that has some usage limitations. This is **system state restore to a virtual machine** (Virtual Disaster Recovery). The target virtual machine is not supposed to be in use while the Continuous Restore mode is active. If the Backup Manager (or the Recovery Console) detects that the virtual machine was started in-between restore sessions, further restores will be blocked and you will get an error message. This is done to prevent possible data loss.

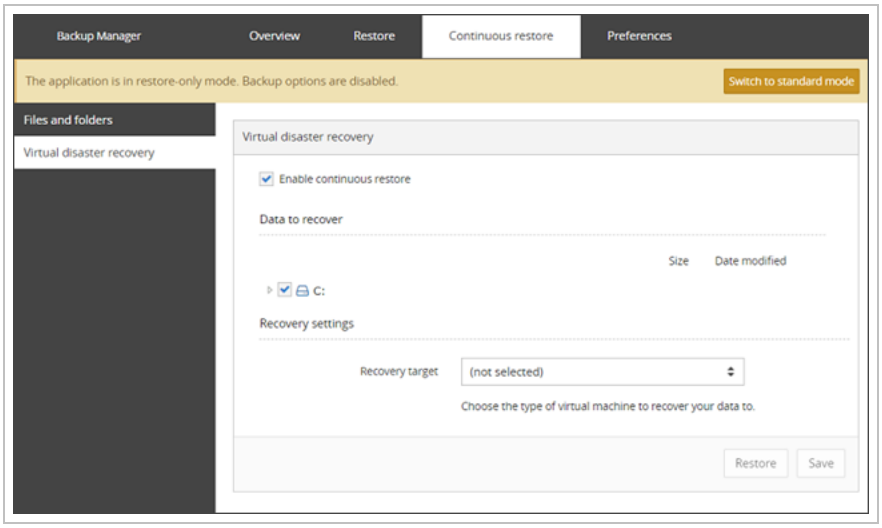
Unblock the Continuous Restore process

1. Make a copy of the virtual machine that is currently available at the target location. Skip the step if the VM was accessed for test purposes and no important changes were made
2. Run an additional restore manually to the same location. This will be a quick delta restore that will overwrite the changes at the target location (if any)

After this, the continuous restore process will be fully functional again.

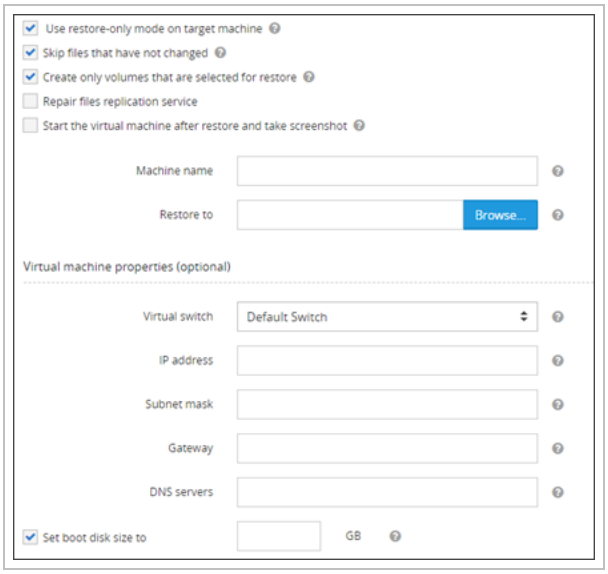
Enabling the Continuous Restore

1. Install Backup Manager in restore-only mode or if it is already installed, launch the Backup Manager from the device
2. Open Backup Manager
3. Go to the **Continuous restore** tab
4. Select **Virtual disaster recovery** from the data sources tab on the left hand side
5. Click **Enable continuous restore**
6. Select a recovery target

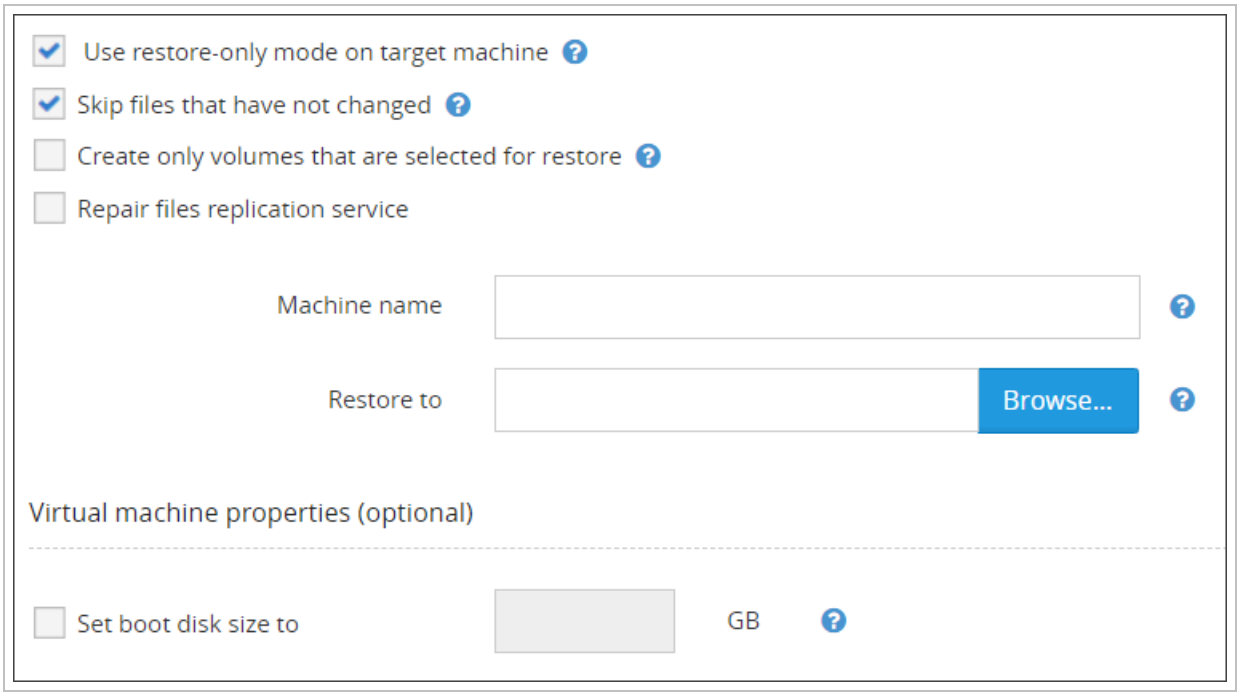


7. Fill out all settings fields for the target used before clicking **OK**. See the Virtual Disaster Recovery Settings for full details on required and optional settings for each recovery target. For example:

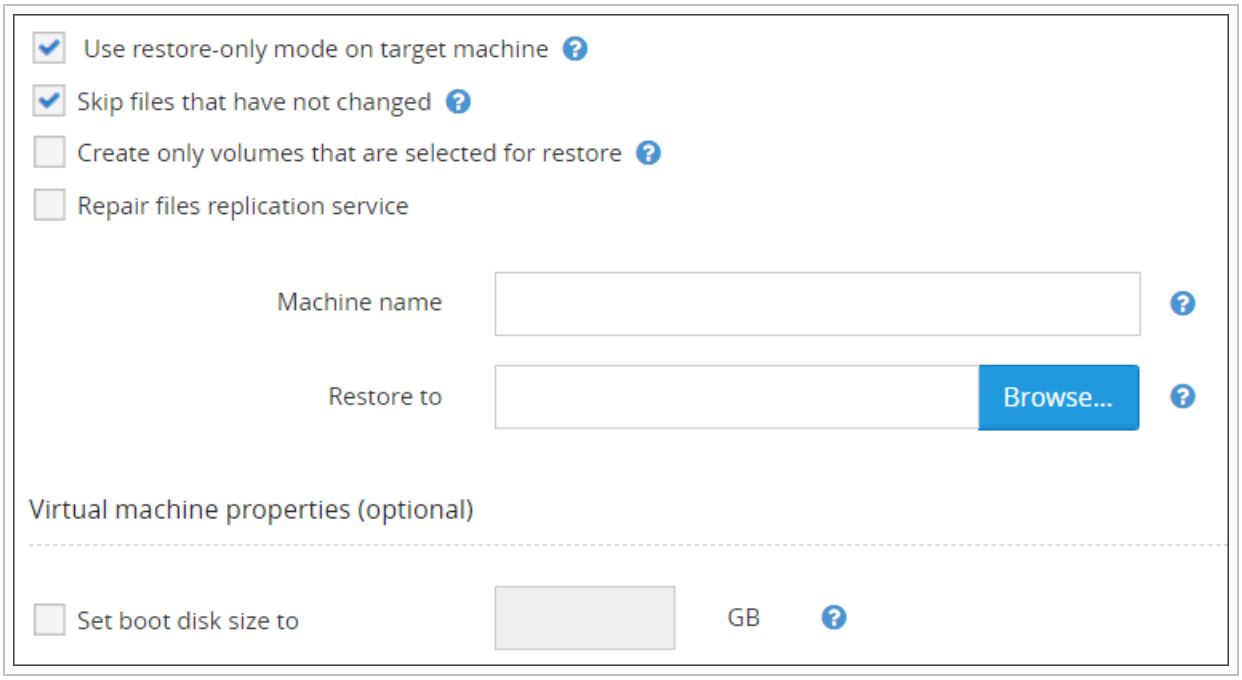
   Hyper-V:



   Local VHD files:



VMWare VMDK:



VMWare ESXi:

- [x] Use restore-only mode on target machine
- [x] Skip files that have not changed
- [ ] Create only volumes that are selected for restore
- [ ] Repair files replication service
- [ ] Start the virtual machine after restore and take screenshot

Access to remote ESX server

Server address

Username

Password Connect

Access to virtual machine

Machine name

Data center Select an Option

Host Select an Option

Storage Select an Option

Resource pool Select an Option

Virtual machine properties (optional)

IP address

Subnet mask

Gateway

DNS servers

- [ ] Set boot disk size to GB

8. Click **Restore** to start a recovery process

To disable the continuous recovery process, go back to the **Continuous restore** tab and deselect the **Enable continuous restore** checkbox.

Customization options

When the Continuous Restore feature is on, the Backup Manager connects to the Cloud every 30 minutes and checks for updates. This time interval can be customized through the configuration file (in seconds).

```
[General]
SessionsUpdatePeriodicityForReadOnlyModeInSeconds=900
```

When configuring the continuous recovery process, you can enable the **Remove obsolete data from target computer** option. If this is enabled, the software will free some disk space on the target machine by deleting files that have been deleted from the source computer.

Continuous Restore for multiple devices

If you have multiple devices to enable continuous restore for, consider using the Recovery Console instead of the Backup Manager. This tool allows you to add a number of devices to run continuous restores.

Seed restore in Backup Manager

Seed restore is a reverse seeding process to download data from the cloud in bulk for use in a local restore. This is useful if the Internet connection on the target computer isn't fast enough or if uploading data from the Internet is undesirable (for example, due to security reasons).

> Seed restore is a **self-service** operation. It can be performed without the involvement of service providers.

Definitions

- A **host computer** - the computer on which a seed restore is initiated
- A **target computer** - the computer to which the data will be restored
- A **removable drive** - a storage device for the transfer of recovery data to the target computer

Requirements

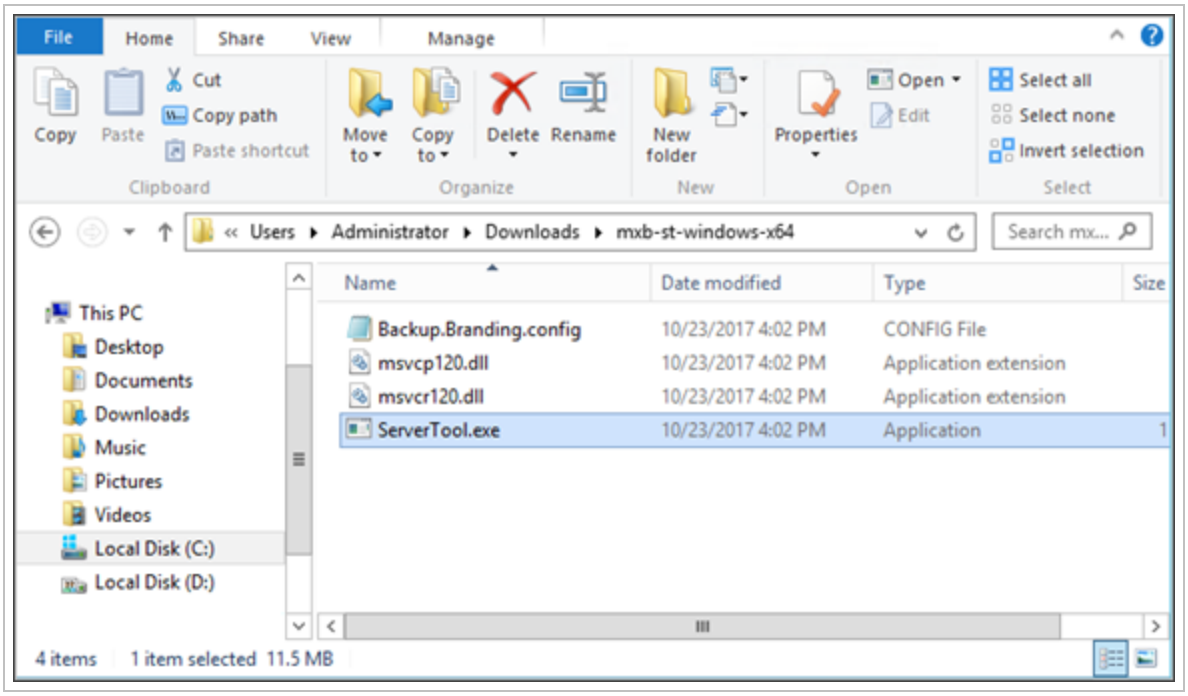
1. The **host computer** must run on Windows and must have a high-speed Internet connection
2. The **target computer** can run on Windows, macOS or Linux. It must have the Backup Manager installed with the same device name and installation key that was used for backup
3. The **removable drive** must have a sufficient amount of free space for recovery data

> During the seed restore **all backup sessions** available in the cloud are copied to the removable drive (therefore the free space requirement).

Instructions

Step 1: Get the Server Tool

1. On the host computer, download the **Server Tool** utility. Version 17.10 or later is required (it contains important fixes). You can get an installer from the Downloads page in the Management Console or from the Additional downloads section of the N-able Backup Downloads page
2. Unpack the archive you have downloaded



Step 2: Create a recovery folder

1. Connect the removable drive to the host computer
2. On the removable drive, create a folder where recovery data will be downloaded to, for example `D:\OfflineRestore`

Step 3: Download backup data to the recovery folder

1. Start the Command Prompt
2. Go to the folder where the Server Tool is located, for example:

```
cd "C:\Users\Administrator\Downloads\mxb-st-windows-x64"
```

3. Run the `seed.download` command. Here is an example:

```
ServerTool.exe seed.download -account sony-vaio-frontdesk -password 123456 -
path
D:\OfflineRestore
```

Values containing spaces must be submitted in straight double quotes.

Required parameters

Parameter	Definition	Supported values
`-account`	The name of the backup device recovery is performed for	Text
`-password`	The installation key for access to the backup device	Text
`-path`	The path to the recovery folder on the removable drive	Path

Optional parameters

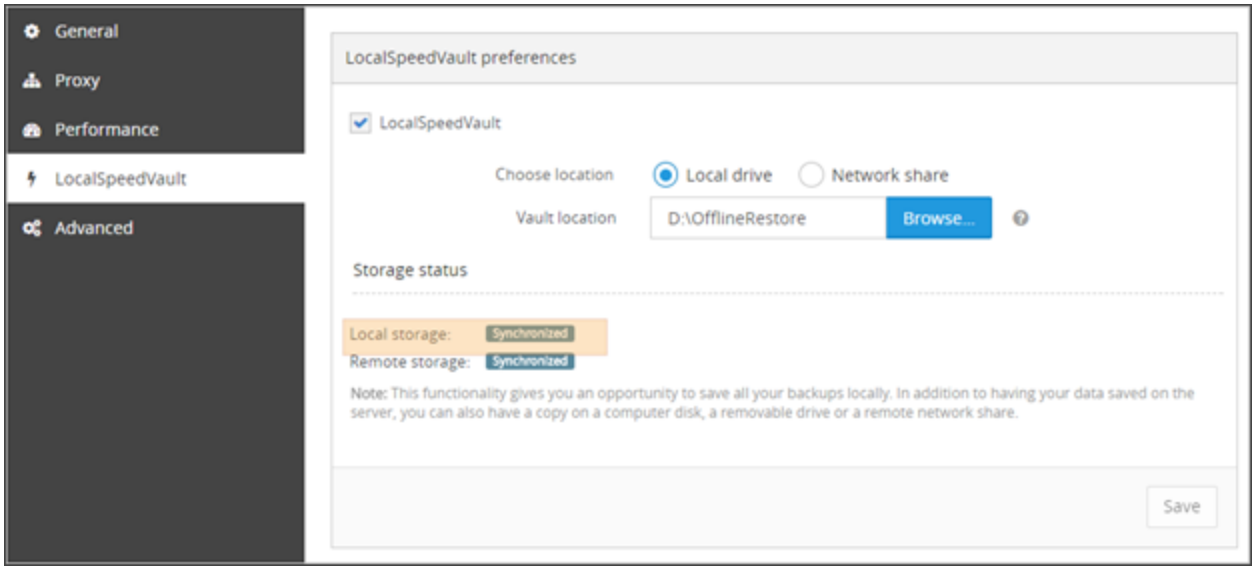
Parameter	Definition	Supported values
`-retry-count`	The number of attempts to connect to the remote server (if the initial attempt fails).	A whole number (set to 5 by default). Recommended range: 1 to 5
`-thread-count`	The number of simultaneous download threads	A whole number (set to 1 by default). 4 is recommended.

For security reasons, the backup data downloaded to the removable drive is **encrypted**. To make it accessible, add it to the backup device that was used for its creation (see the next step for details).

Step 4: Recover the data to target computer

1. When the download is completed, eject the removable drive and connect it to the target computer
2. In the Backup Manager, go to **Preferences > LocalSpeedVault**. Enable the feature and set **Vault location** to the recovery folder on the removable drive, for example `D:\OfflineRestore`

3. When the local storage synchronization status changes to "Synchronized", open the **Restore** tab and perform recovery



Preferences for Backup Manager

The **Preferences** page in Backup Manager contains several tabs which are used in configuring the backup device.

What's inside:

General

Language

The Backup Manager can be used in any of these 9 languages:

- English
- Dutch
- Russian
- German
- Spanish
- French
- Portuguese
- Norwegian
- Italian

Backup Dashboard Settings

Send a report regarding the status of the **backup** to the email address(es) entered into the **Send To** field.

> Separate multiple recipient email addresses with a semicolon, e.g. `user1@company1.com;admin@company1.com`

Using the **Frequency** dropdown, set how often to send the report to the provided addresses:

- Daily
- Every Wednesday and Saturday
- Saturday
- Never

Restore Dashboard Settings

Send a report regarding the status of the **restore** to the email address(es) entered into the **Send To** field.

> Separate multiple recipient email addresses with a semicolon, e.g. `user1@company1.com;admin@company1.com`

Using the **Frequency** dropdown, set how often to send the report to the provided addresses:

- Daily
- Every Wednesday and Saturday
- Saturday
- Never

Remote Connections

Enable or disable remote connections to the device by either selecting or deselecting this setting.

Save

You must make sure to save any changes you make before moving away from this page.

Schedule

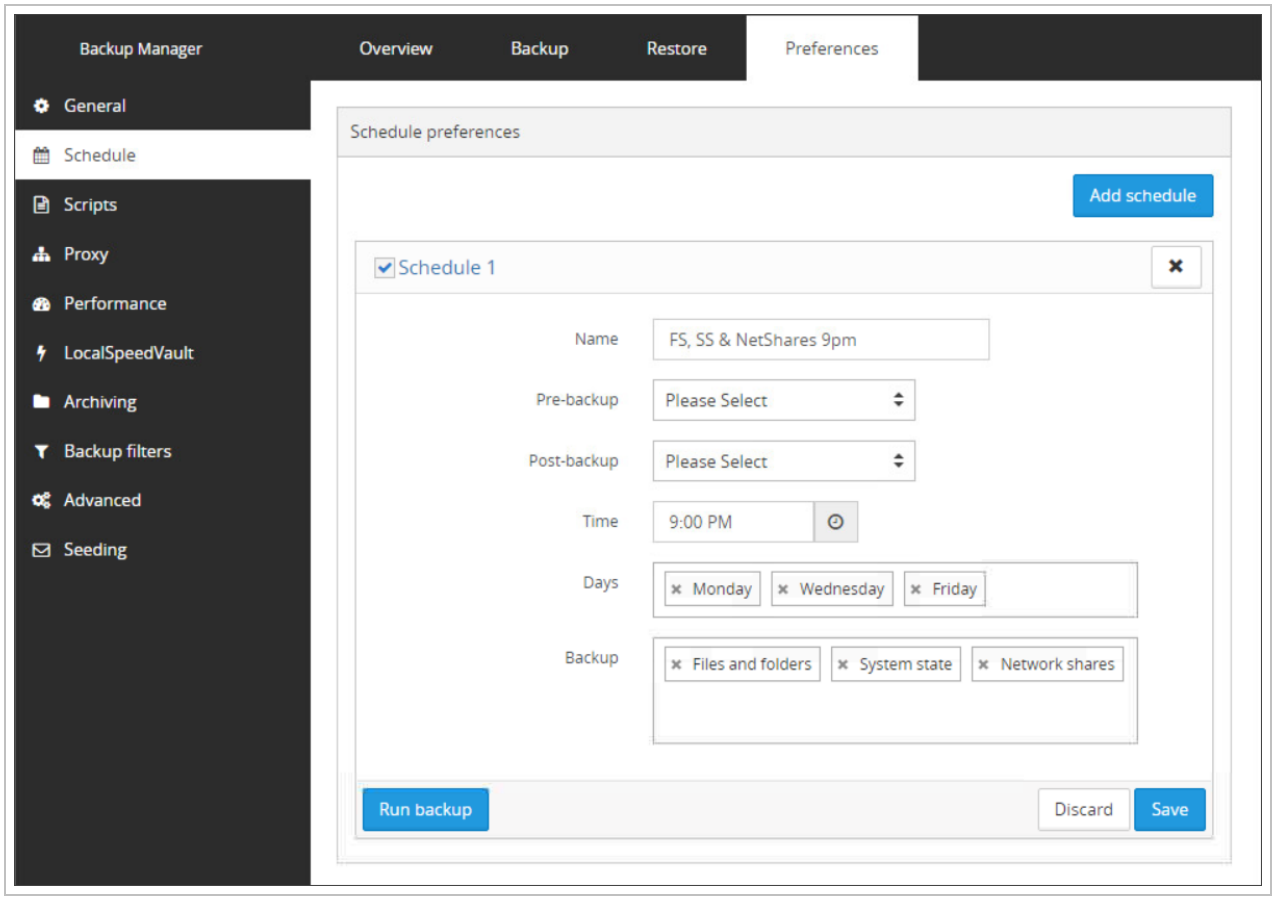
The most convenient method of configuring backups is to set up a **backup schedule** which will automatically run the backups without requiring you to intervene.

You can create multiple schedules for each device, for example if you want Files and Folders to run at 9am but you want Files and Folders, System State and MySQL to run at 9pm.

Create Schedule

To create a backup schedule:

1. Launch the Backup Manager for the device
2. Open the **Preferences** tab
3. Click **Schedule**
4. Select **Add Schedule**



5. Give the schedule a name - make this something relevant to the backup configured such as "FS, SS & MyS 9pm"
6. Optional - If you have created any scripts, these can be selected to run before the backup (Pre-backup) or after the backup (Post-backup) by selecting them from the given dropdowns.
7. Set the time for the backup to run
8. Choose the days on which you want the backup to run
9. Select the data sources to backup
10. Click **Save**

> If you want to back up a data source regularly, it **must** be configured for backup as well as selected in a schedule or a profile. This can be done by following the Schedule steps above.

> If you have not configured the backup selection, the schedule will run, but as no data source configuration exists, nothing will be backed up.

Disable Schedule

If you have multiple schedules listed in this page, you can enable or disable them by ticking the check box beside the name of the schedule. Disabling a schedule does not delete it, but will stop it from running until you manually enable it again.

Edit Schedule

To edit a schedule, you just need to expand the schedule in question, make the necessary changes and click **Save**.

Delete Schedule

To delete a schedule, simply click the **X** to the right of the schedule name, you will be prompted to confirm deletion of the schedule - click **Yes**.

> Please note, once a schedule has been deleted, it cannot be undeleted and would have to be recreated manually.

Save

You must make sure to save any changes you make before moving away from this page.

Scripts in Backup Manager

You can set up Backup Manager client to perform certain actions before or after backups. This is done with the help of scripts. You can use any command line commands as scripts in Backup Manager.

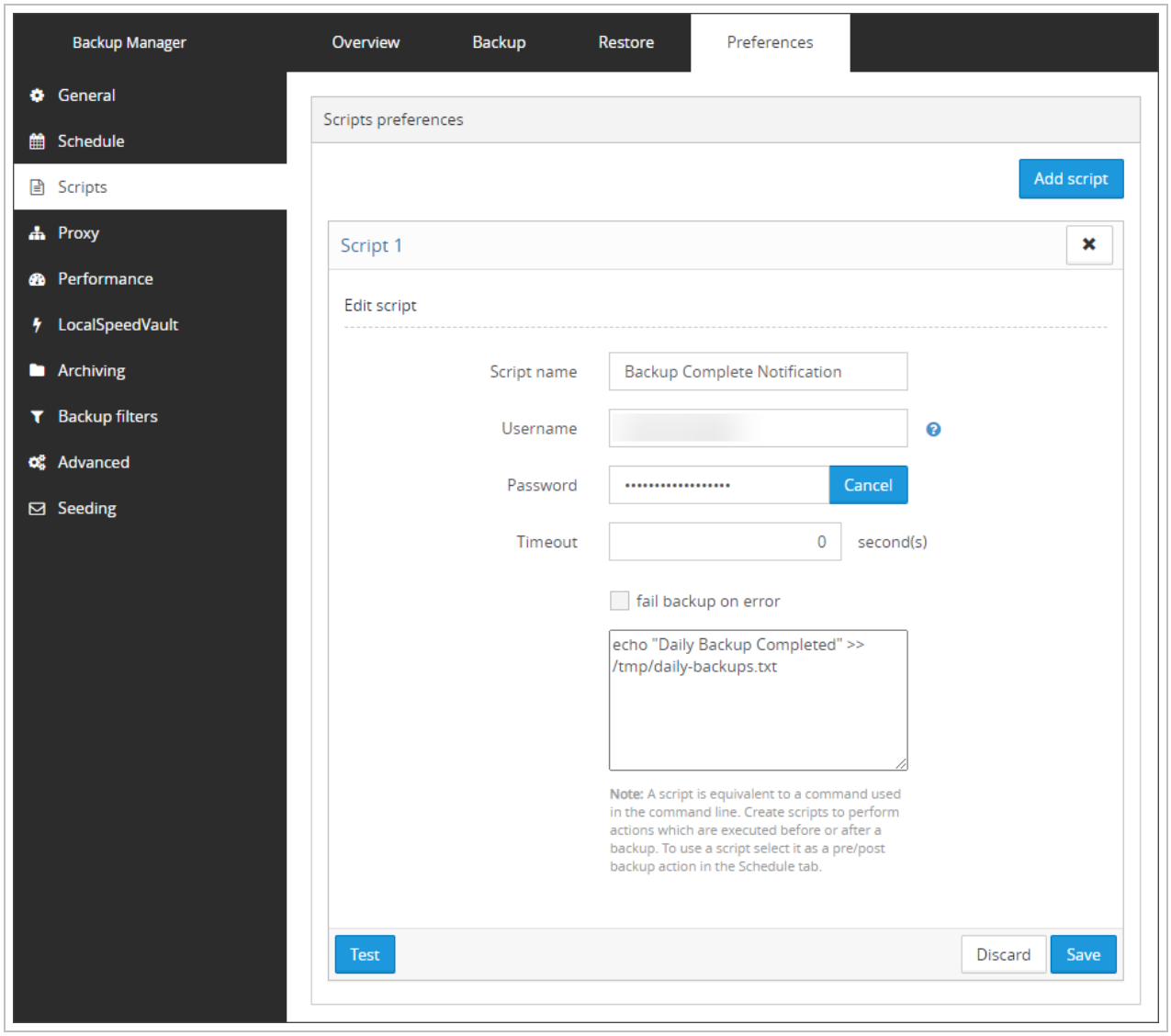
> The scripts tab is only available when opening the backup manager locally on the device.

Adding scripts

Before you can add the script to run as part of the schedule, you must first create the script in the Backup Manager client.

1. Launch the Backup Manager for the device
2. Click **Preferences > Scripts**

3. Click **Add script**



4. Configure the settings:
   - **Script name** - Name the script something that will be recognizable when adding the script to the schedule, e.g. Backup Completed Notification
   - **Username** - The username for a user with sufficient permissions to run scripts on the local system
   - **Password** - The password for the username with sufficient permissions to run scripts on the local system
   - **Timeout** - enter a time limit (in seconds) after which the script will be stopped
   - **Fail backup on error** - Check this box to fail the backup, or stop the backup from running if the script returns an error

     > If a **pre-backup script** is important, enabling the **fail backup on error** setting will stop the following backup from running

   - **Script body** - In the remaining text box, provide the script content
5. *(optional)* Click **Test** to make sure the script has been entered correctly
6. Click **Save**

Available settings for scripts

- Scripts run under the **LocalSystem** account that Backup Manager normally operates under. If your script requires some special permissions, you should provide an alternative username and password. The account you specify must be from the **administrative group**. Different username formats are supported: `username`, `username@domain` and `domain\username`
- The **Group** field on Linux and macOS devices requires the name of the group

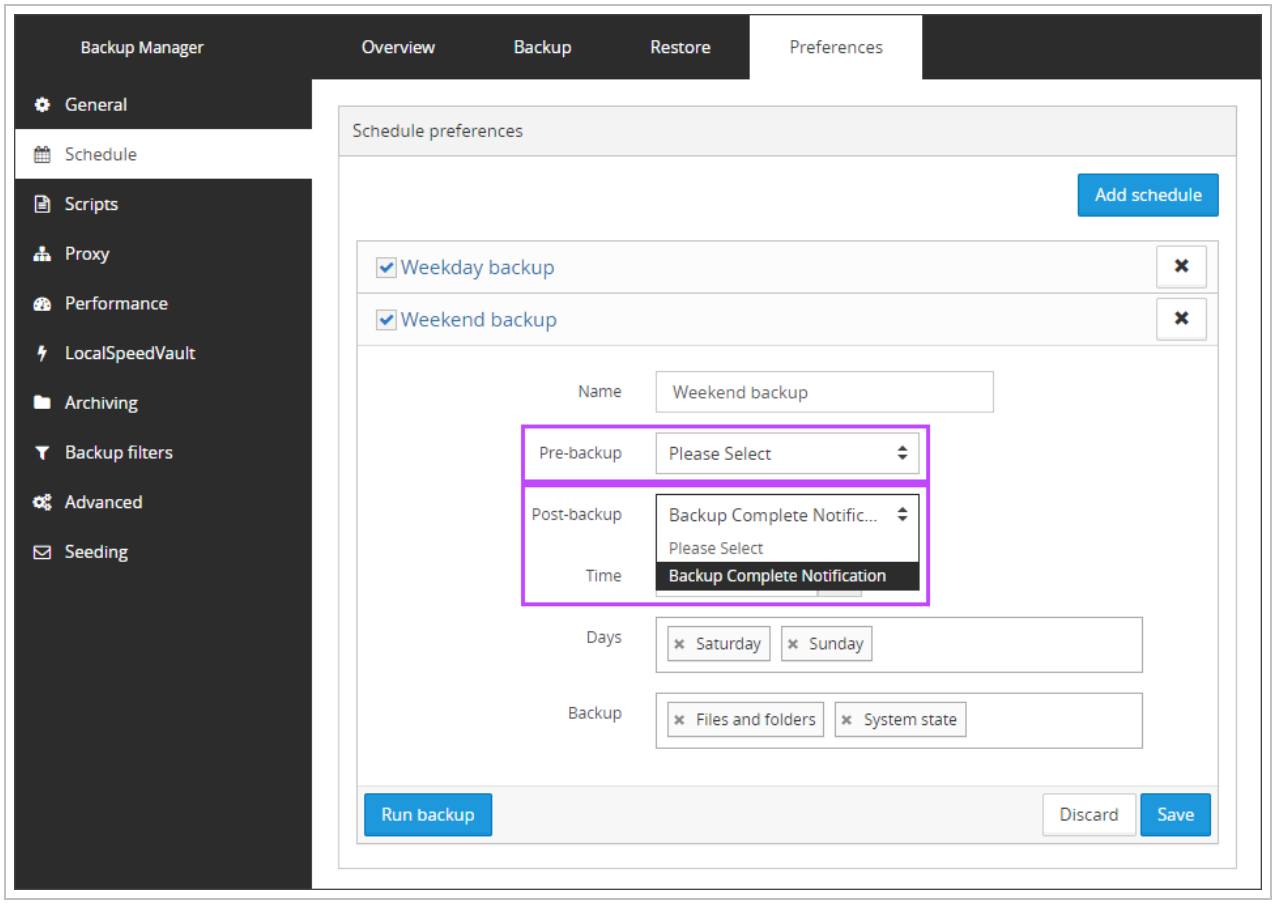
Applying scripts

The scripts you have added become available for selection in the backup schedule settings **(Preferences > Schedule)**. You can add a script to an existing backup schedule or create a new schedule for this purpose.

Once added to the schedule, these scripts run once per backup source. For example, where a schedule contains both *Files & Folders* and *System State* backup sources, a schedule's pre-backup script runs before each backup takes place.

1. Launch the Backup Manager for the device
2. Click **Preferences > Schedule**
3. Expand an existing schedule, or click **Add Schedule** to create a new one

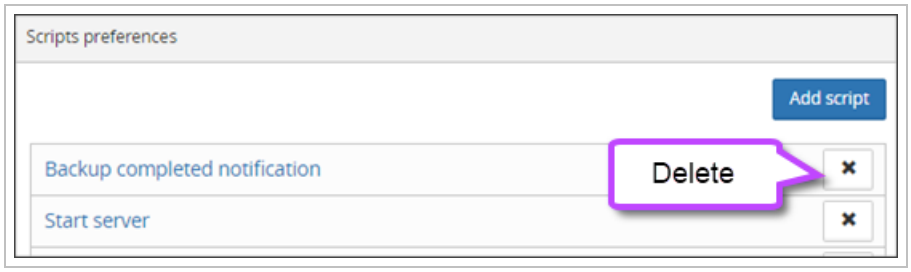
4. If adding a script to an existing schedule, select the script from the **Pre-backup** or **Post-backup** dropdown boxes. If creating a new schedule, follow these instructions to create a new schedule



5. Click **Save**

Removing scripts

To remove a script that you no longer need, remove it from any schedules, then navigate to the Scripts tab and delete it using the cross icon next to its name.



Note for Linux users

The syntax for Linux machines is the same as for usual bash scripts. Here is an example:

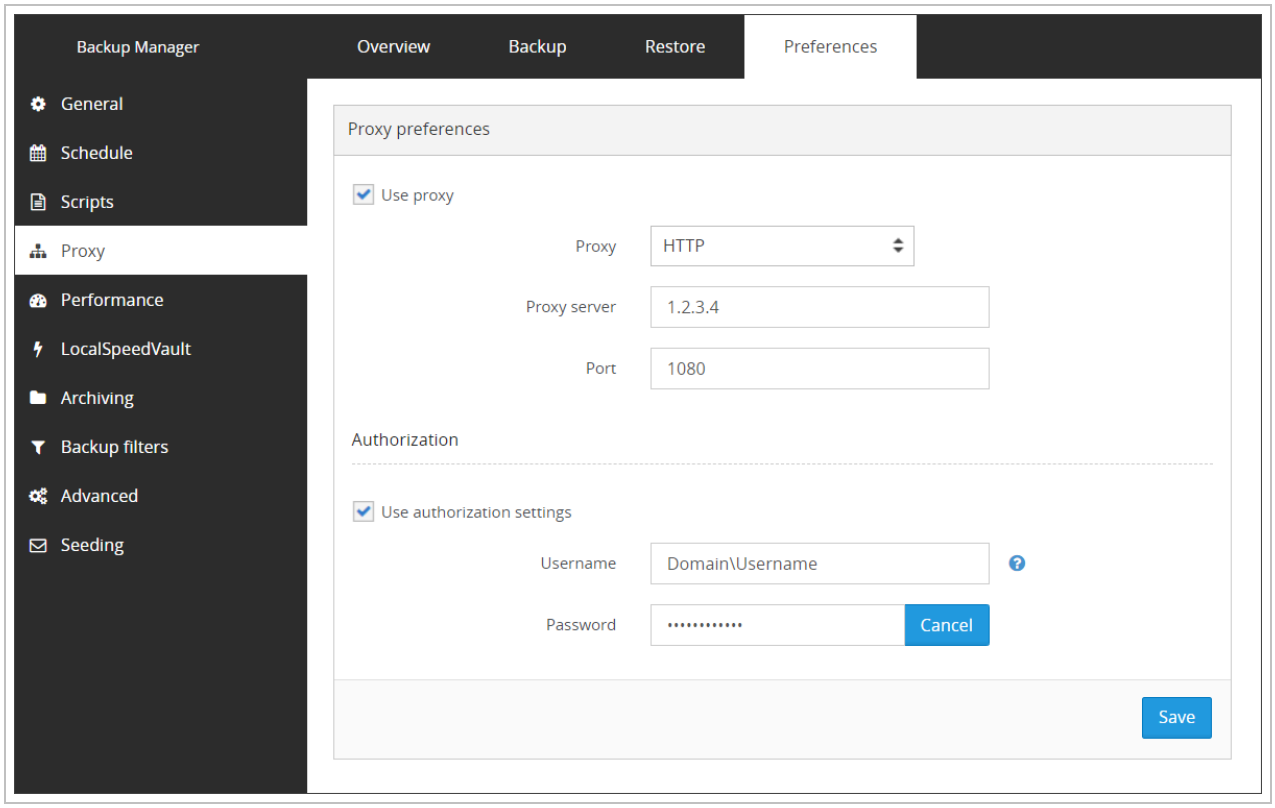
```
#!/bin/sh
echo "Daily backup completed" >> /tmp/daily-backups.txt
exit 0
```

Save

You must make sure to save any changes you make before moving away from this page.

Proxy

You may configure the Backup Manager to use a **Proxy** from this tab.



Enable Proxy

1. Enable **Use Proxy** by placing a check in the box
2. Provide the proxy details:
    - **Proxy** - select from one of the following proxy types:
        - HTTP
        - SOCKS4
        - SOCKS5
    - **Proxy Server** - provide the proxy address
    - **Port** - Enter the port to use, the default is 1080
3. **Save** the changes

Authorization

Once the proxy is enabled, the **Authorization** section becomes available. To use these:

1. Enable **Use authorization settings** by placing a check in the box
2. Provide authorization details:
    - **Username** - Enter a username with sufficient credentials to access the proxy server e.g. `domain\username` or `username`
    - **Password** - Enter the password for the user
3. **Save** the changes

Save

You must make sure to save any changes you make before moving away from this page.

Performance

By default, Backup Manager does not use any kind of bandwidth throttling or restriction, meaning that if a backup is set to run during regular working hours, or begins over night and continues into normal working hours, Cove Data Protection (Cove) will not throttle bandwidth by default. This can, however, be set manually by enabling bandwidth limiting and restricting the maximum upload and download speed during backups and the times in which backups are permitted to start.

Reasons to enable Bandwidth Limiting

This can be useful if the device:

- Is used heavily during certain hours
- Has other programs installed which require exclusive access to databases or files
- Has a slow internet connection

Feature availability

The bandwidth throttling feature is supported on Windows, macOS and Linux devices.

Set Bandwidth Limiting

There are two ways to configure bandwidth limitation, one through the Backup Manager client as detailed below and the other by using the **set bandwidth** remote command.

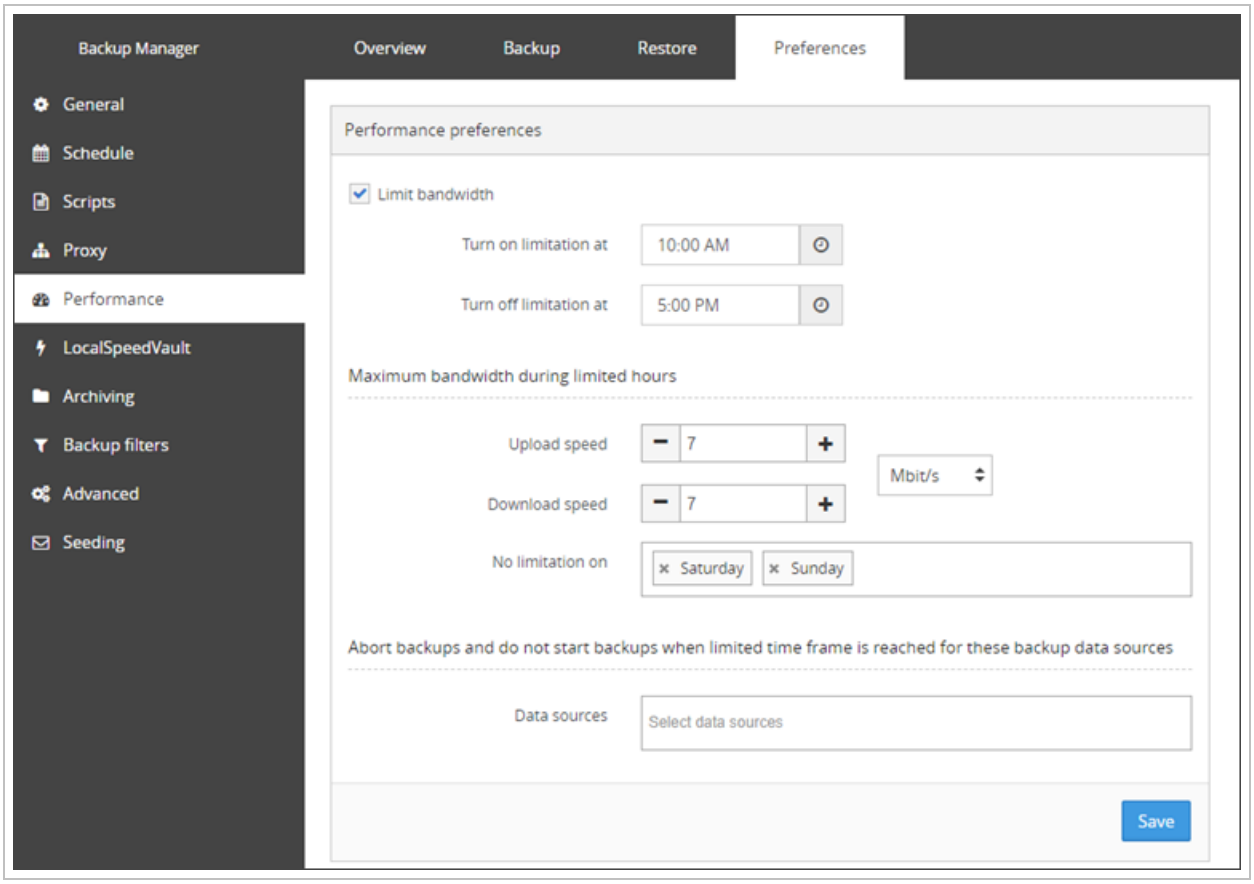
1. Launch the Backup Manager for the device
2. Go to **Preferences > Performance**
3. Select **Limit bandwidth** checkbox
4. Specify times for the limitation to start and end
5. Specify the maximum bandwidth during the specified times

   These can be in Kbit/s or Mbit/s.

6. Add the days in which you *do not* want any limitation
7. Specify any data sources you wish to abort or not start a backup for when the time frame provided above is reached

   This feature is not available if the device is using a profile.

8. **Save** the changes you have made



Save

You must make sure to save any changes you make before moving away from this page.

LocalSpeedVault (a local storage directory in Backup Manager)

By default, the Backup Manager saves your backups remotely in the cloud or at a private data center (depending on your terms of service). You can enable the LocalSpeedVault (a local storage directory) to have an **additional copy** on your own computer or in your local network. Doing this helps speed up the backup process.

Overview

Reasons to enable the LocalSpeedVault

When the LocalSpeedVault is on, scheduled backups **run** secondary to the cloud backup, thus speeding up the backup process. Also restoring data to a local folder becomes faster and does not depend on your Internet connection.

How it works

When a LocalSpeedVault is enabled on a device and a backup runs, the data is sent to both the LocalSpeedVault and the cloud or private storage location. As the LSV is on the local network, this part of the backup completes faster. Once this has completed and synchronized, the LSV begins pushing the backup data to the cloud or private storage as well.

This effectively means that the backup to the cloud or private storage is being sent twice at the same time and so completes faster.

During a restore, data is automatically downloaded from the LocalSpeedVault first to the local device. If the LocalSpeedVault is not available or not synchronized, the restore data will be pulled from the cloud or private storage location. This takes place automatically and cannot be reconfigured.

> If the LocalSpeedVault becomes full, backups will still continue to the cloud, or your private storage nodes.

Feature availability

The feature is supported on Windows, macOS and Linux devices.

What can be used as the LocalSpeedVault

You can create a LocalSpeedVault directory on a local disk, a removable disk or in a local network. All kinds of network resources are suitable: workstations, file servers or network-attached storage (NAS) devices.

Network Shares can be used as a storage location for Linux and macOS devices by mounting them, then browsing to the Network Share location.

Requirements

Size Requirements

Whether you are using a local drive or a network resource, there must be a **sufficient amount** of **free space**.

Your backup data will take up the same amount of disk space as on the remote server, so we recommend that the LocalSpeedVault should be two or three times that of the **used storage**, e.g.:

Initial Backup	Incremental Backup	Total Used Storage	LocalSpeedVault size
200GB data backed up initially	50GB worth of changes backed up incrementally throughout the day	450GB of data stored	1TB - 1.5TB recommended

For Local Drives

If the LocalSpeedVault directory is on a local drive, it must meet the following requirements:

1. It must be **open to the LocalSystem account** (this is the account that the Backup Manager usually performs backups under)

   > Read and write permissions are required

For Network Resources

If the LocalSpeedVault directory is in your local network, it must meet the following requirements:

1. The local network must use the **SMB protocol** for file sharing
2. The network resource must be **accessible** during backups (it must not go into the sleep mode or get disconnected from the network)
3. The network resource must be **open** (available without authorization), which is not recommended due to security reasons, or – preferably – it must have an account that **coincides with the account** on the client machine where the Backup Manager is installed (the same username and password). This can be an Active Directory account
4. If the computers in your local network are united into domains, the network resource must belong to the **same domain** as the client machine (otherwise there may be cross-domain authentication issues on Windows)

The network resource can be integrated with **Active Directory** or **connected to a workgroup**.

Security recommendations for network resources

Recommendations for network resources integrated with Active Directory

If you manage the local network using Active Directory, the accounts from the client machines are suitable for access to the network resource (**pass-through authentication**). You can differentiate access to the network resource with the help of **groups**.

Recommendations for network resources connected to a workgroup

If the network resource is connected to a workgroup, we recommend creating a **separate user account** for backup purposes on each client machine where the Backup Manager is installed. The same account must be created on the network resource (this is necessary for access to the network resource).

- Use a **unique** username and password for each client machine
- Do not use administrative logins/passwords
- Limit access to the defined LocalSpeedVault share for all other users and groups

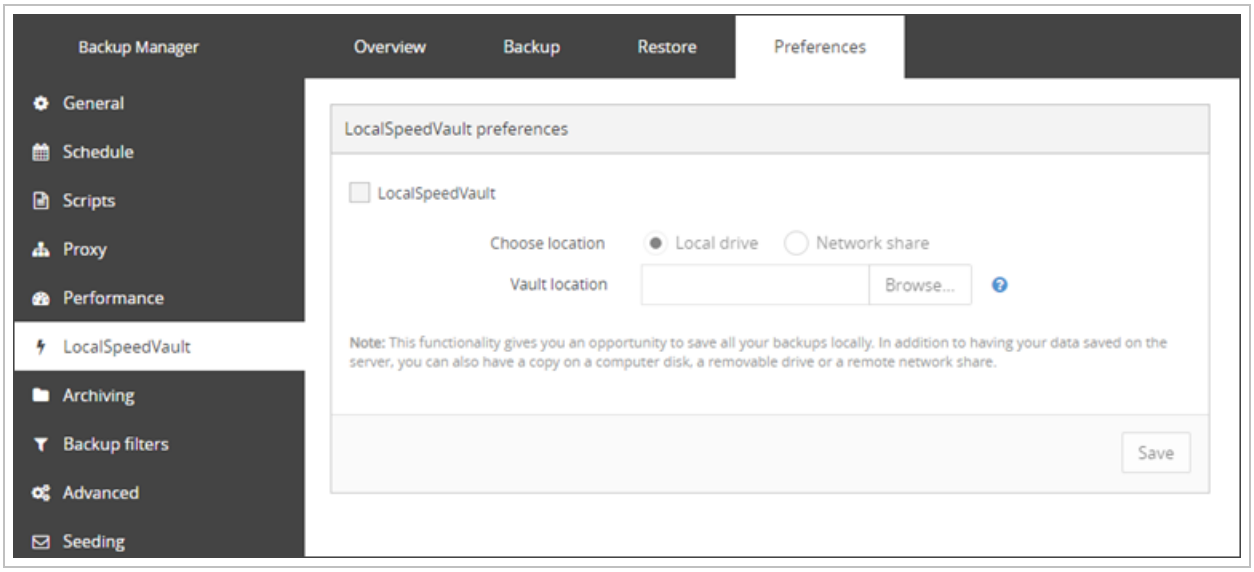
Enabling the LocalSpeedVault

Windows

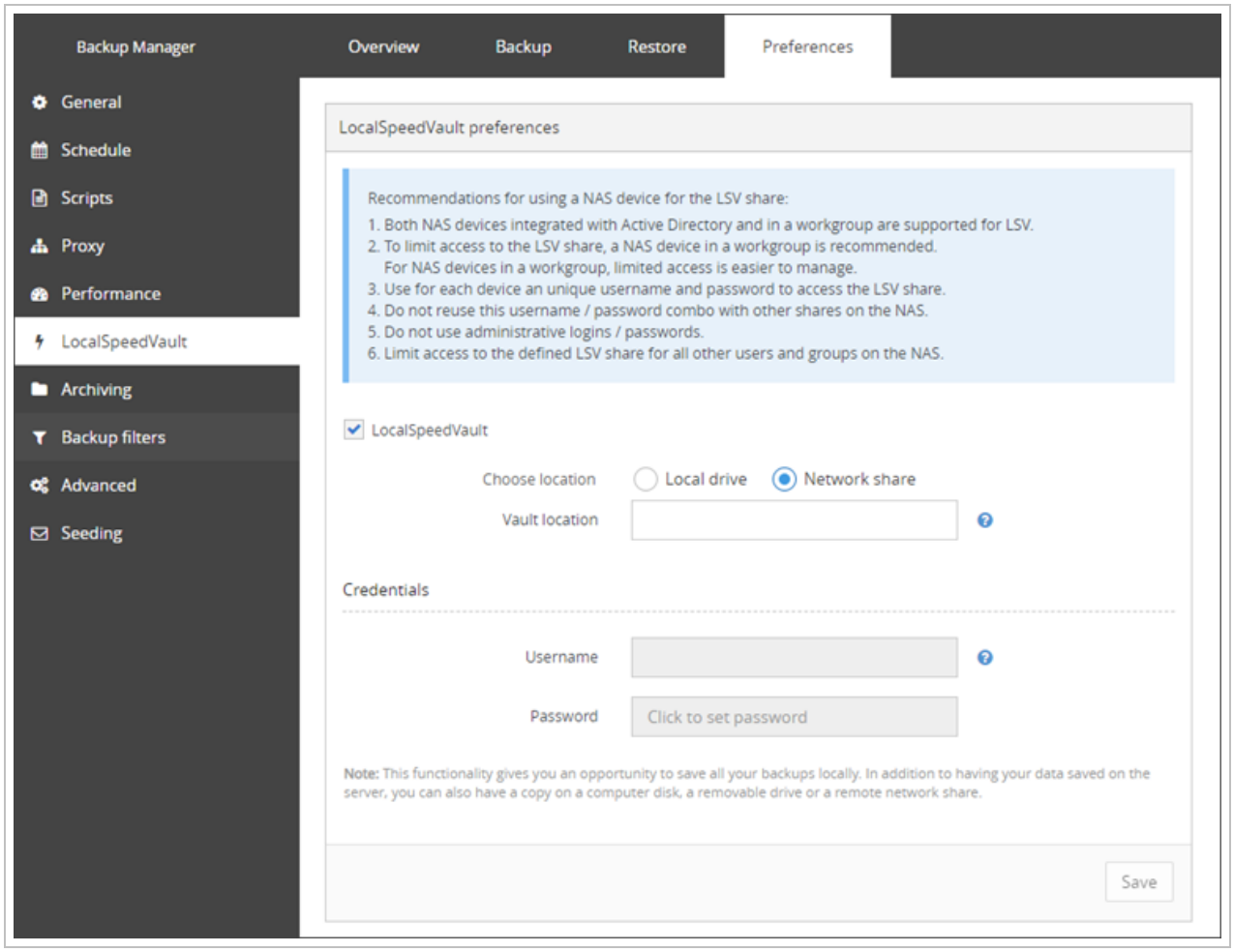
To enable the LocalSpeedVault, do the following:

Go to **Preferences > LocalSpeedVault**

1. Select the **LocalSpeedVault** checkbox
2. Specify the location of the directory allocated for the LocalSpeedVault. This can be an existing or a new directory (the Backup Manager will create it for you automatically if it is not there yet)



3. If the directory is on a network share, enter your access credentials for that network share



4. Save the changes you have made

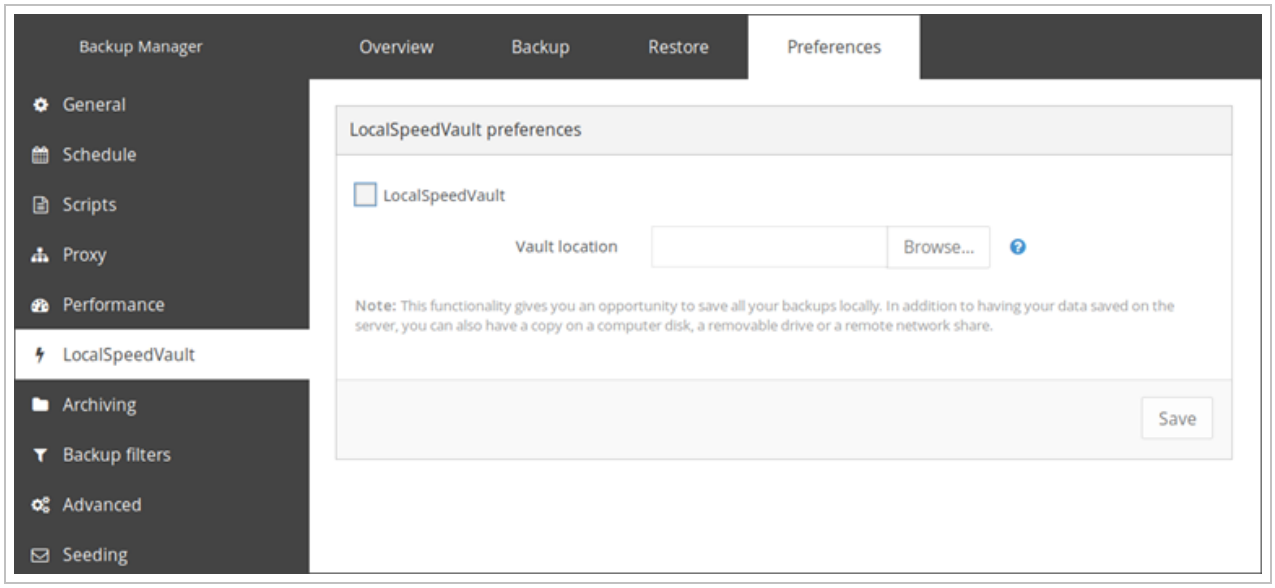
macOS & Linux

To enable the LocalSpeedVault, do the following:

1. Go to **Preferences > LocalSpeedVault**
2. Select the **LocalSpeedVault** checkbox
3. Specify the location of the directory allocated for the LocalSpeedVault

> If the directory is on a network share, you must mount it on the device then select the network share location using the browse option for Vault Location.

4. Save the changes you have made



Monitoring LocalSpeedVault

See the Synchronized page for full details.

Save

You must make sure to save any changes you make before moving away from this page.

Monitoring the LocalSpeedVault

During a backup process, data is sent to the cloud and the LocalSpeedVault. If either of the two storage locations is temporary unavailable, it is updated later when the connection is re-established.

Synchronization statuses

To check whether the local and remote storage locations have all necessary data, open the **Overview** tab in the Backup Manager or go to **Preferences > LocalSpeedVault**.

LocalSpeedVault statuses can also be included in Management Console dashboards by adding the **LSV Status** column.

- Scheduled reports can be generated based on a view that contains the **LSV Status** column (Scheduled Reports in Management Console)

You can also enable **custom notifications** to receive emails regarding LSV status:

- Information on one-time notifications based on a certain LocalSpeedVault status can be found here.

There are three statuses altogether:

- Synchronized
- Synchronizing
- Failed

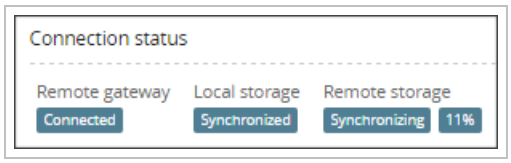
Synchronized

The **Synchronized** status means that both the LocalSpeedVault storage location and the Remote storage location (Cloud storage) have the same backed up data, and so, are both up-to-date.

Synchronizing

The **Synchronizing** status will be followed by a percentage (%), and means that either the LocalSpeedVault storage location or the Remote storage location (Cloud storage) are currently in the process of getting the backed up data from the other storage location.

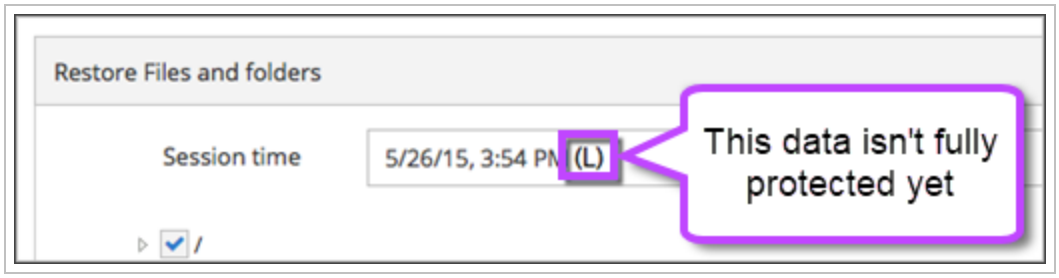
E.g. In the below image, you can see that the Local Storage (LocalSpeedVault) shows as Synchronized, while the Remote Storage is Synchronizing with a percentage of 11%.



This means that your recent backup(s) has been saved locally and is being copied to the remote server at that time. The data is not fully protected until the synchronization is completed for both Local and Remote storage locations.

> While the synchronization is in progress, it is **crucial** to keep the LocalSpeedVault working and to avoid making changes to its settings. Otherwise the sessions that have been backed up to the LocalSpeedVault can be lost.

> You can identify backup sessions which have not been successfully synchronized to the Remote storage location by viewing the Backup Session in the session list. If a session is marked with "L", this means it is available on the Local storage **only**.



Failed

The **Failed** status means that synchronization to one or both of the storage locations has failed and there is a risk of data loss.

Synchronization is automatically **disabled** after the LocalSpeedVault has stayed in the "Failed" state for 14 days (learn more). The Backup Manager invalidates the data that has not fully synchronized with the cloud and tries to back it up again during the next session.

> A notification will appear in the Backup Manager interface and an email alert is sent out in that case.

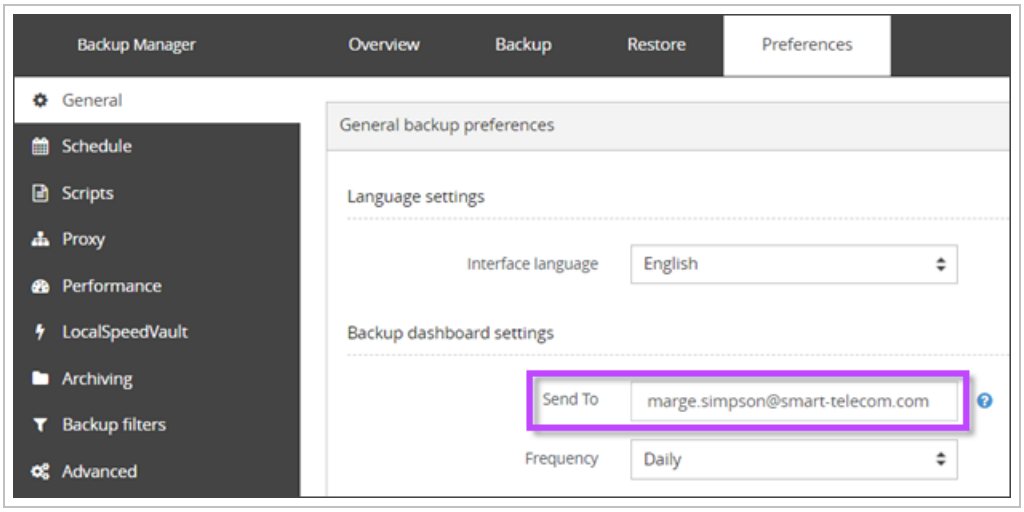
The default 14-day period can be customized for each backup device through the Backup Manager configuration file by adding the following parameter to the `[General]` section:

- `LocalSpeedVaultUnavailabilityTimeoutInDays = NN`
  - Where `NN` is replaced with the number of days

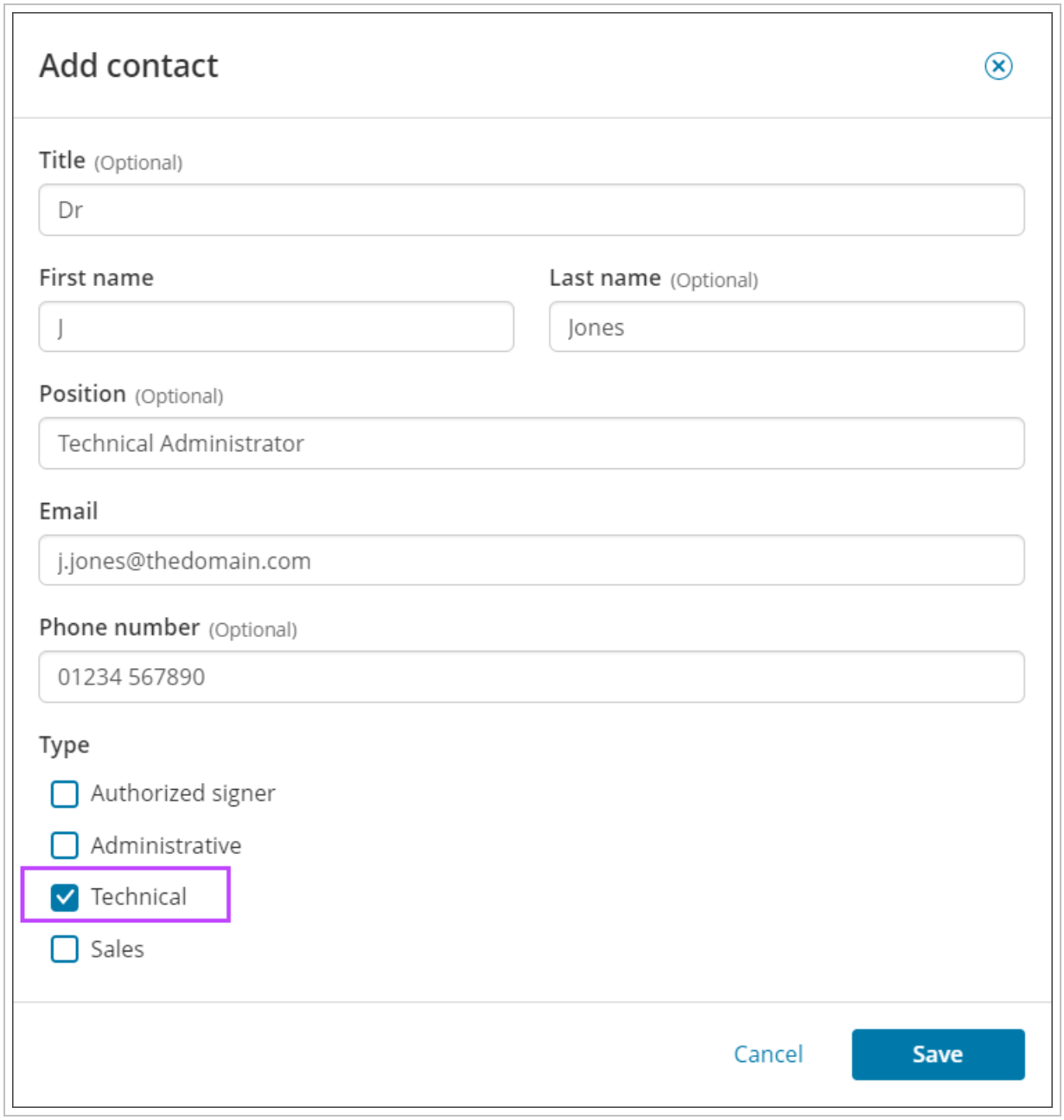
Email alerts on LocalSpeedVault synchronization statuses

Alerts on LocalSpeedVault failures are sent to the following emails:

- The email address specified for backup Dashboards. In the Backup Manager, this can be found under **Preferences > General > Backup Dashboard Settings**



- The technical contact person from the company the device belongs to. You can add such a contact person through the Management Console by navigating to **Management > Customers**, edit the company, open the **Contacts** tab and click **Add Contact**



Synchronizations errors

There are a number of reasons the Synchronization may have issues. Below are some common issues and how to resolve these:

Access is denied

If you have received an **Access Is Denied** error, check the following:

1. Check your local access credentials for the LocalSpeedVault storage location
2. Make sure the Backup Manager client has **read and write** access to the LocalSpeedVault directory
   - If the LocalSpeedVault is on a local drive, check the LocalSystem user account
   - If the LocalSpeedVault is on a shared network resource, check the specified network user account

Path is invalid

If the error received states that the **path is invalid**, check the specified LocalSpeedVault storage path and make sure the LocalSpeedVault directory is correct and available.

It might have been moved or deleted.

Not enough space

If the LocalSpeedVault directory is full and cannot receive any new data, the notification will state **Not Enough Space**.

To fix this you can:

1. Add more space to the directory (if your infrastructure allows it) by following local workstation instructions
2. Copy the previously stored files to another directory with a sufficient amount of space, then update the LocalSpeedVault path in the Backup Manager to the new, larger storage location
3. Disable the LocalSpeedVault and continue with the cloud storage only

   > If you choose this option, make sure the remote storage is synchronized with the LocalSpeedVault **before** disabling it, or you may risk loss of data.

4. Clean up unneeded Archive sessions from the LocalSpeedVault. This can be done in the same way as removing Archiving sessions from the Remote location, following the steps found here

Archiving backup sessions in Backup Manager

As you regularly back up your data using the Backup Manager, a series of backup sessions accumulate in the Cloud (your remote storage location), and on the LocalSpeedVault if this is used. After a certain period, older sessions are cleaned to free up storage space on both the remote and local storage locations. The duration of this retention period is measured in number of days to keep backup sessions for (depending on your Product settings).

If needed, you can keep selected backup sessions in the storage after their retention period expires using the **Archiving** feature. Such sessions will not be deleted (unless you choose to do so manually).

> Using Archiving will *increase* the storage space used.

If data is removed from the backup selection, any future backups will not include this information, but all versions of this data stored in an **Archive** session will not be affected and so will be kept until a clean is done of the archive sessions.

If LocalSpeedVault is used while Archiving is enabled, the used storage of both the Remote storage location (the Cloud) and the Local storage location (LocalSpeedVault) will increase.

Enable Archiving

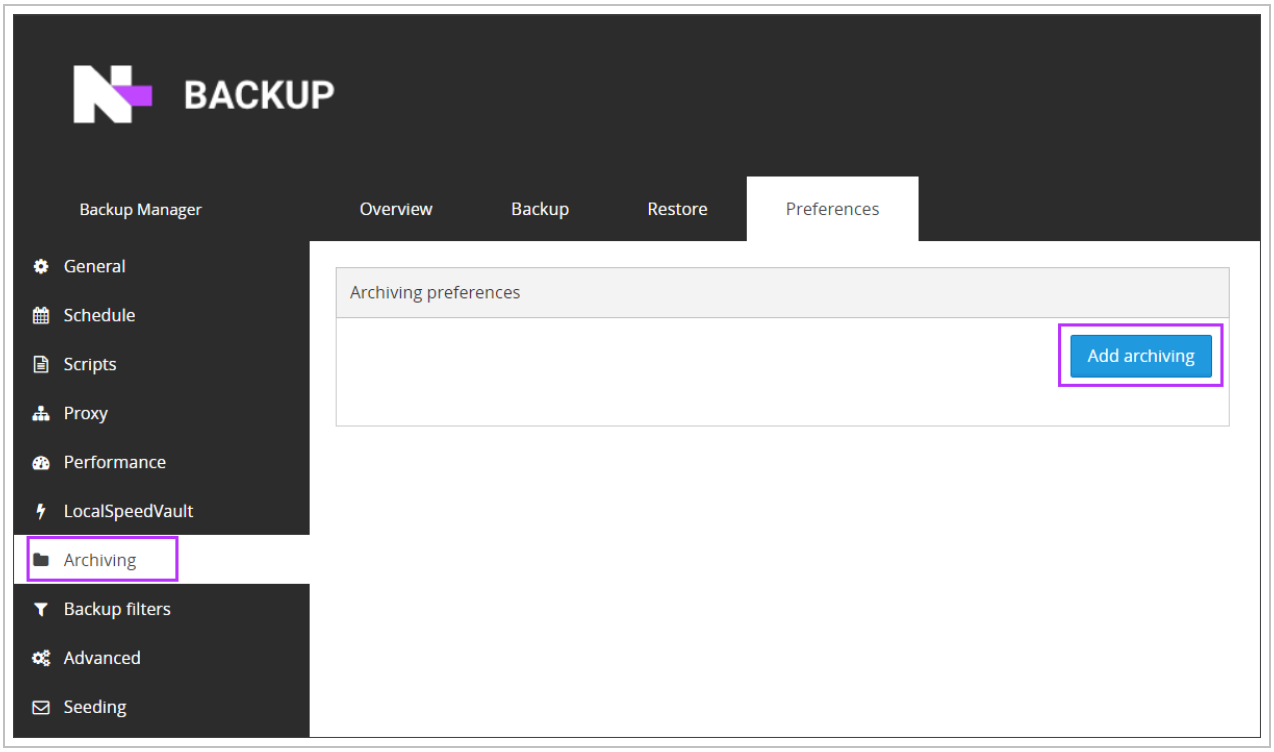
To archive a backup session, you need to enable archiving on the devices Backup Manager client. The task will apply to the next backup session to start after the archive time.

> Previously completed backup sessions cannot be archived.

- The archive task can be an individual or repetitive task
- There can be only one archiving task for each data source per day

> It is not possible to archive data belonging to the same data source several times a day

1. Open the Backup Manager client for the device you wish to configure archiving on
2. Navigate to the **Preferences**tab
3. Go to **Archiving** on the left hand menu
4. Click **Add Archiving**

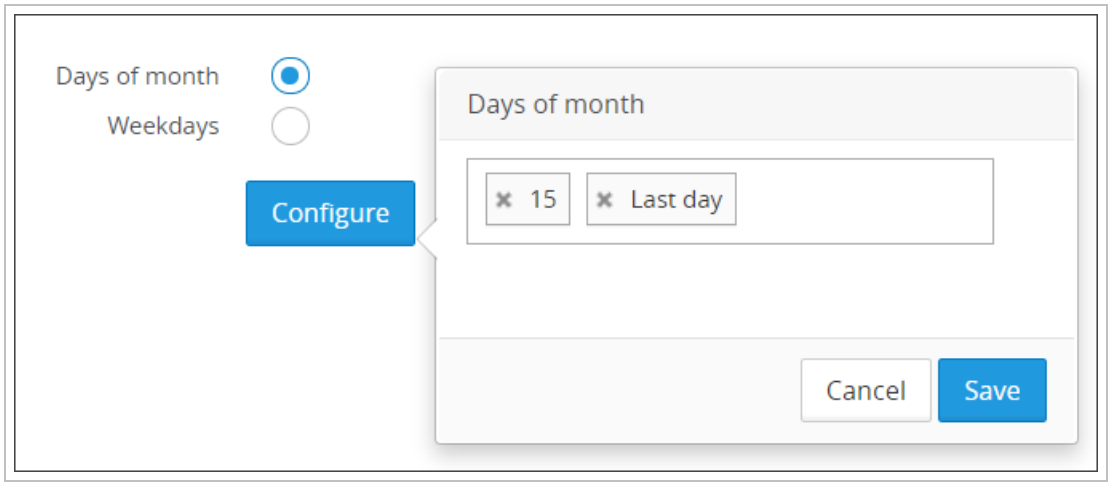


5. Give your archive a name relevant to the frequency of the archive such as "End-of-month archiving" or "Bi-Weekly archiving"
6. Set a time for the archive

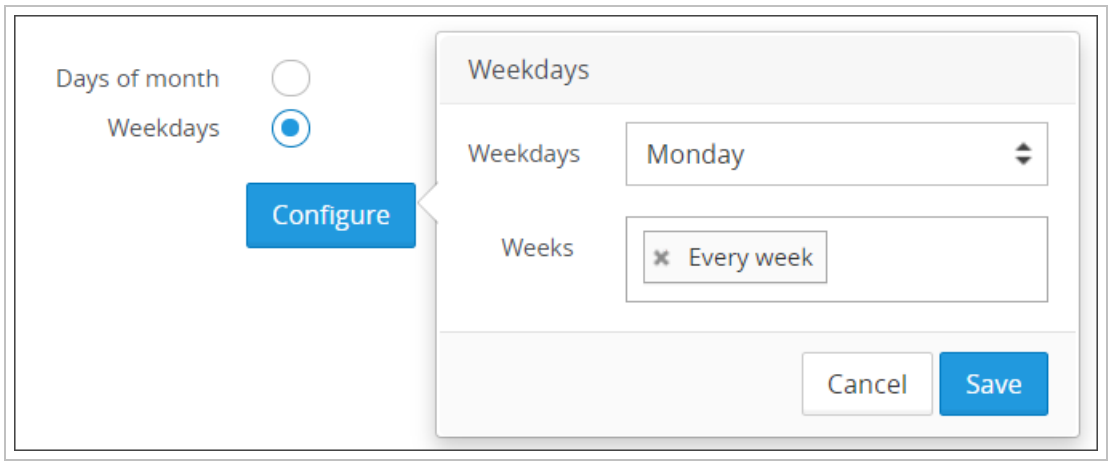
> This **does not** mean the archive will run at the exact time, but that the archive session will apply to the nearest backup that runs *after* this time.

7. Select the data source(s) to apply the archive to
8. Select the months you wish the archive to be applied to

9. Now select either
   - **Days of month**: This will allow you to set the dates of days in the month you wish the archive to be set, for example the 15th of the month and the last day of the month:



   - **Weekdays**: This will allow you to set the day of the week and which week of the month(s) selected in step #8 you wish the archive to be set, for example every Monday:



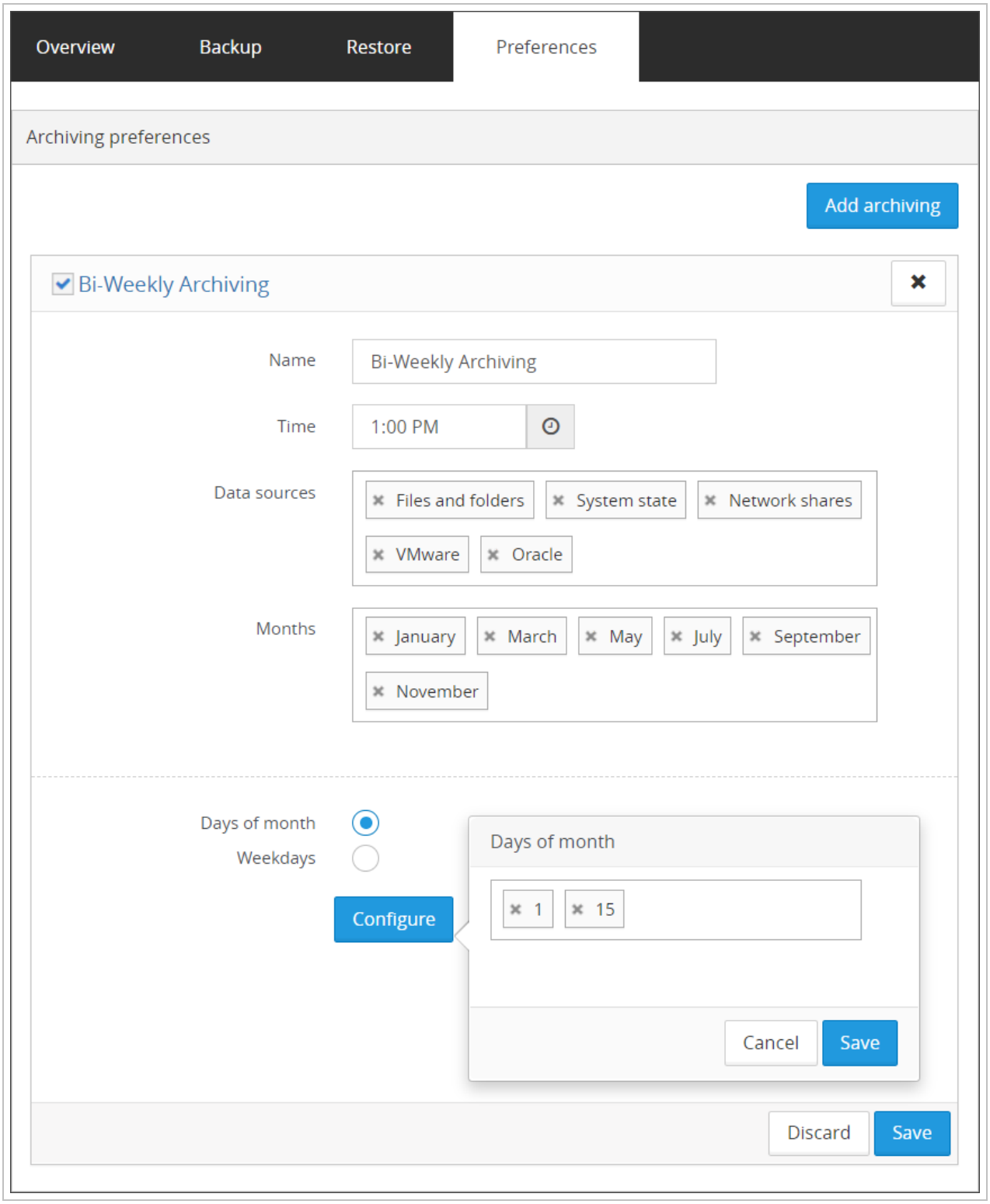
> If you want to run an archive more frequently than the **Weekdays** selection but you do not wish to use the **Days of month** selection (for example you wish it to be set for every Monday, Wednesday and Friday) you must create multiple archives and select each day per Archive.

Edit Archive tasks

You can easily change the task after it has been created.

1. Open the Backup Manager client for the device you wish to edit archiving on
2. Navigate to the **Preferences**tab
3. Go to **Archiving** on the left hand menu

4. Click the Archive task you wish to edit to expand the current settings



5. Make all changes you need

6. Click **Save**

Delete Archive tasks

When an archiving task is not needed anymore, you can delete it.

> This will not make any difference to the backup sessions that have been archived through this task.

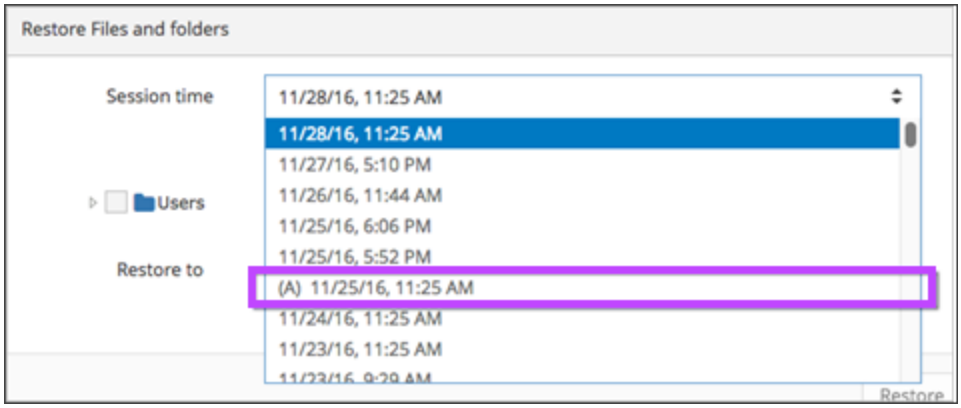
To delete an archive task:

1. Open the Backup Manager client for the device you wish to delete the archive task on
2. Navigate to the **Preferences**tab
3. Go to **Archiving** on the left hand menu
4. Click the Delete button to the right of the Archiving task

5. Confirm deletion by clicking **Yes** on the confirmation box

Recovering backup sessions from Archive

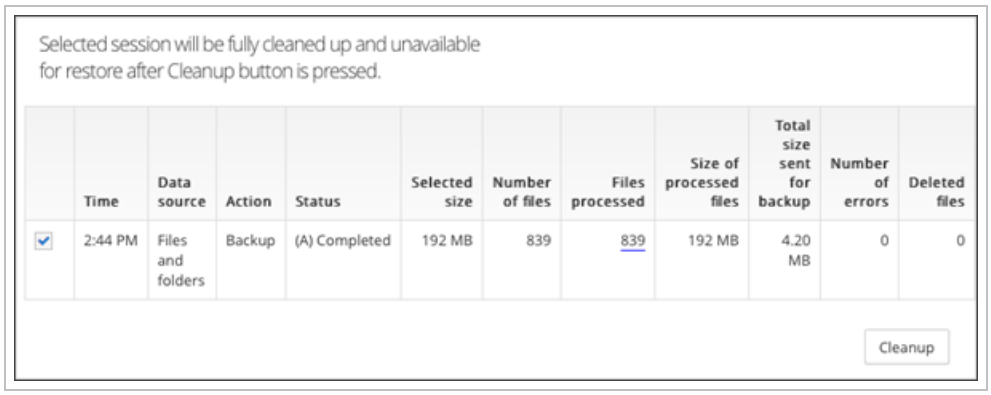
Data from archived sessions is recovered is the same way as from regular backup sessions. You will only notice that archived sessions have a special mark (A) in the **Session time** list which is intended to make it clear that the session is archived.



Clean up unneeded archiving sessions

If you no longer want to keep an archived session in the storage, you can clean it up. The (A) mark gets removed from the session. Then the session is cleared from the storage and is no longer available for recovery.

1. Go to **Preferences > Archiving**
2. Click **Cleanup** (You will see the list of all archived sessions that have passed their retention periods)
3. Select the sessions to clean up
4. Click the **Cleanup** button at the bottom
5. Confirm your intention to clean up the selected sessions



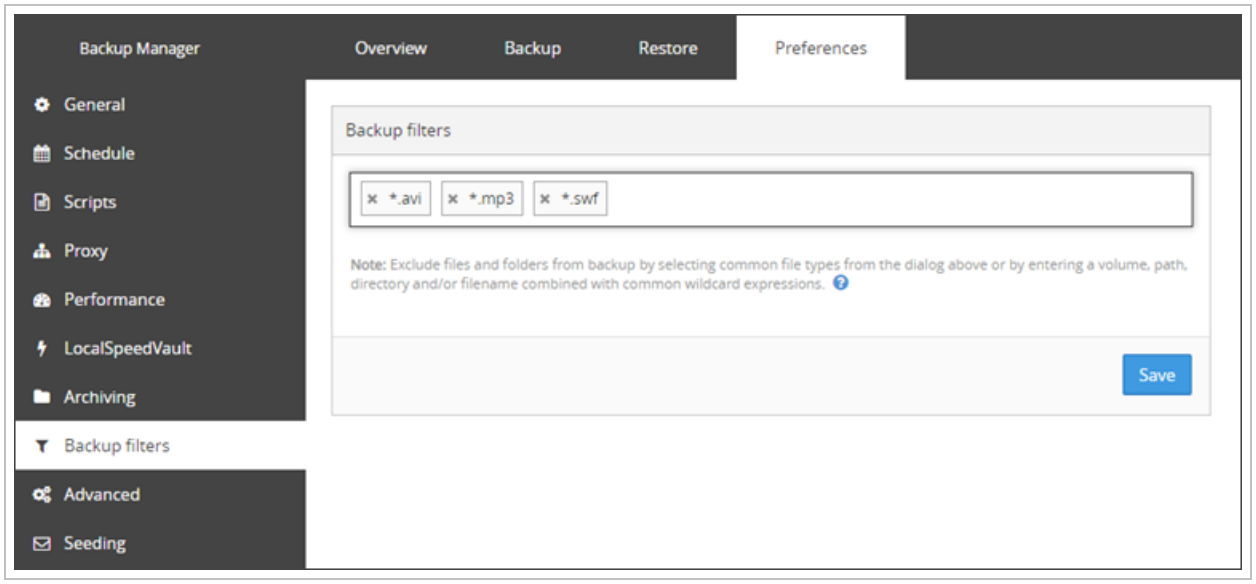
> The action **cannot be undone**. Once a session has been cleaned up, there is no way to get its contents back.

Save

You must make sure to save any changes you make before moving away from this page.

Backup Filters in Backup Manager

You can automatically exclude certain directories or types of files from backup. This is done using exclusion filters on the devices Backup Manager, by going to **Preferences > Backup filters**.



Predefined filters

Some files are automatically **excluded from backup** on Windows devices **only**, except when using certain security features of Products.

> These predefined filters only work on Windows devices by the use of a standard 'files not to backup' entry in the **Windows Registry**, meaning there is no alternative for Linux or macOS devices.

What files are automatically excluded from backup:

1. All files indicated in the registry subkey:

   ```
   HKEY_LOCAL_
   MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup
   ```

   Typical examples:

   - `\Pagefile.sys`
   - `\hiberfil.sys`
   - `%TEMP%\* /s`

2. All files from the Backup Manager installation folder

3. Temporary files of no importance:
   - ```
     C:\Users\<username>\AppData\Local\Microsoft\Windows\Explorer\IconCacheToDelete
     ```

     > There is such a file for every user account registered in the system
   - ```
     C:\Users\<username>\AppData\Local\Microsoft\Internet Explorer\DomainSuggestions
     ```

     > There is such a file for every user account registered in the system
   - ```
     C:\Windows\System32\config\systemprofile\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\64bit
     ```
   - Files from the **Print Spooler** folder
4. Files/folders matching the following masks:
   - `*\Local Settings\Temporary Internet Files\*`
   - `?:\RECYCLER`
   - `?:\System Volume Information`
   - `%systemdrive%\$WINDOWS.~??` (for example `C:\$WINDOWS.~BT` or `C:\$WINDOWS.~WS`
   - `%SYSTEM_ROOT%/Windows/*.config.cch`
   - `?:\swapfile.sys`
   - `?:\pagefile.sys`
   - `?:\hiberfil.sys`
   - `*\AppData\Local\Temp\*` (on Windows Vista and Windows 7)
   - `*\Local Settings\Temp\*` (on Windows XP)

File Type Examples

Filters based on file type are the same across all Operating Systems.

Here are some example filters you can add:

- **a*** - excludes all files starting with the letter "a"
- ***.mp3** - excludes all files with the .mp3 extension
- `C:\Data\*.*` - excludes all files in the `C:\Data\..` path and underlying folders
- `C:\Data\*.mp3` - excludes all files in the `C:\Data\..` path, with the .mp3 extension
- `C:\Data\*.m??` - excludes all files in the `C:\Data\..` path, with a three-character extension starting with .m and ending with any two other characters, such as .mob, .mp3, .mov or .mpg
     ```

> The filters are applied to **upcoming backup sessions**. Older backups stay as they are.

Suggested Additional Filters

We would strongly advise to add the following additional exclusions to your filters:

Windows temp locations

- `*\Microsoft\Windows Defender\Scans\mpcache*`
- `*\AppData\Local\Microsoft\Outlook\*.ost`

Chrome/Edge/Firefox browser cache and update files

- `*\Chrome\User Data\*\Cache\*`
- `*\Local\Microsoft\Edge\User Data\Default\Cache\*`
- `*\Local\Mozilla\Firefox\Profiles\*\cache\*`

N-central cache directories

- `*\PME\archives\*`
- `*\NablePatchCache\*`
- `*\SolarWinds.MSP.CacheService\cache\*`
- `*\N-able Technologies\UpdateServerCache\*`

AV Defender cache files

- `*\ThreatScanner\Antivirus*\Plugins\cache.*`

EDR/SentinelOne

- `*\ProgramData\Sentinel\data\*`

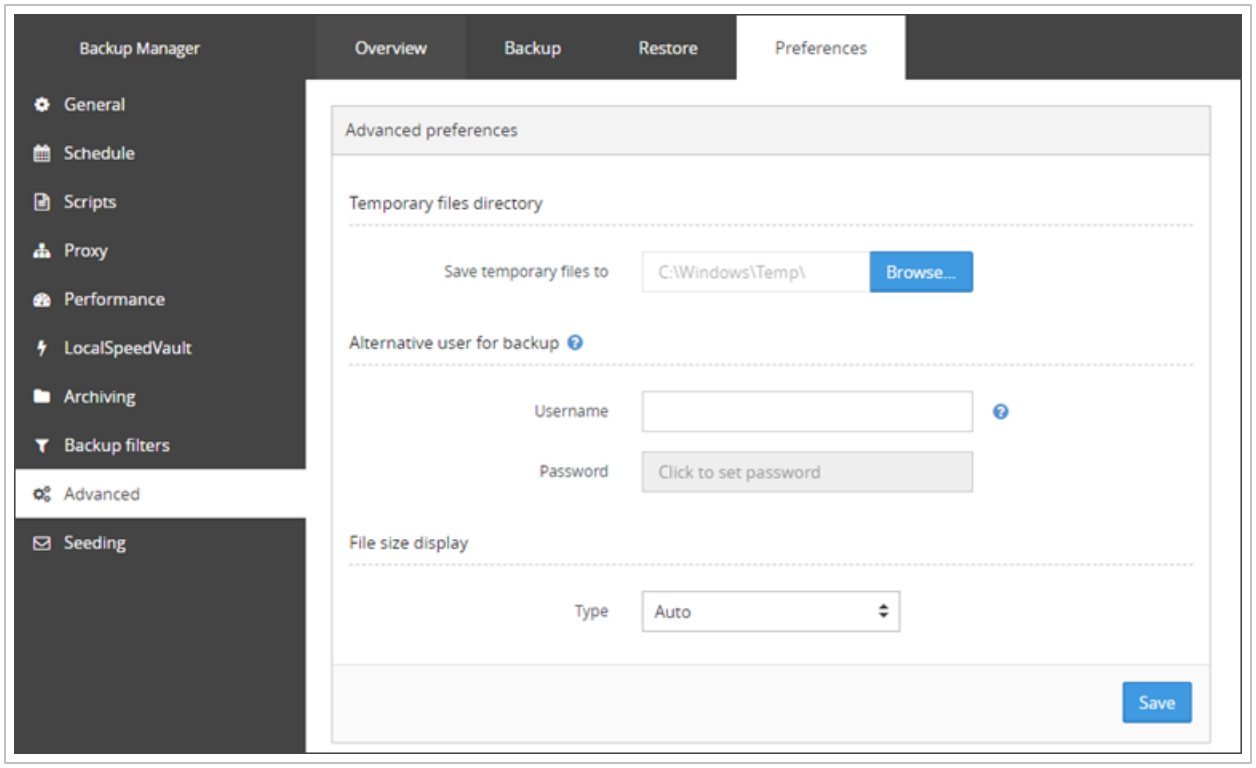
Save

You must make sure to save any changes you make before moving away from this page.

Advanced

In the Advanced tab of the Preferences section on Backup Manager, there is functionality to change the directory of temporary files, configure an alternative user for backup and the format in which the file size will be displayed.

> It is recommended to restart the Backup Service Controller after any changes are made in the Advanced tab so that the changes may take effect.



Temporary files Directory

Here is how to change the location of temporary files for Backup Manager.

1. Click **Preferences > Advanced**
2. Click **Browse** next to the 'Save temporary files to' text box
3. Navigate through the file tree to select the new location of the temporary files
4. Click **Save**

Alternative user for backup (only available for Windows devices)

This setting allows you to specify an alternative set of user account credentials which will be used to allow Backup Manager permission to backup any files or data sources which are restricted on the device.

1. Click **Preferences > Advanced**
2. Specify the credentials of the alternative account to be used

   > The username can be added as either domain\username or username

3. Click **Save**

File size display

1. Click **Preferences > Advanced**
2. Using the **Type** dropdown, select the format you would like to view the file size in

> The choices for type are **Auto**, **KB**, **MB** or **GB**

3. Click **Save**

Save

You must make sure to save any changes you make before moving away from this page.

Seed backup in Backup Manager

Backing up a large volume of new data can take time if a user's Internet connection is slow. For such cases Backup Manager users have the option to use our seeding function. It works both for initial and subsequent backups.

> Seed backup is a **self-service** operation. End users can perform it all by themselves without the involvement of their service provider.

Once the below requirements have been met, see the following instructions on using the Seed Backup feature:

- Step 1. Set seeding path
  - Step 1. Set seeding path
  - Step 2. Enable seeding
  - Step 3. Transfer seeding folder to storage

Terms

- **Seed backup**
  1. Any backup session performed while a device is in the **seeding mode**
  2. The process of uploading backup data to the cloud in bulk. Seed backups are performed to a **temporary storage medium** and then transferred to the cloud from a different machine with a high-speed Internet connection (see the scheme below). Also called *seeding*

- **Seeding path** - a path to a folder on a temporary storage medium (required by the Backup Manager). This is where a seeding folder is created
- **Seeding folder** - a directory that is created automatically for seed backup purposes. It contains backup files in a compressed and encrypted format, ready for cloud storage. The folder is titled using the name of the backup device it belongs to
- **Seeding mode** - the mode that starts as soon as seeding is enabled and ends when a user clicks **Complete seeding**. In the seeding mode, all backups are performed to the seeding folder (rather than directly to the cloud)
- **Post-seeding mode** - the mode that starts when a user clicks **Complete seeding** and ends shortly after seed data is uploaded to the cloud. While in the post-seeding mode, regular cloud backups are available but it is not possible to restore data that has been backed up since the seeding mode started

Options available in the seeding mode:

Option	What it does	Available	Location
Run seeding	Starts a seed backup session (can be used multiple times)	In the seeding mode	"Backup" tab
Disable seeding	Disables the seeding mode (subsequent backups will be performed to the cloud)	In the seeding mode **until the first backup** is performed	Notification ribbon (all tabs)
Complete seeding	Sets to Backup Manager to the post-seeding mode	In the seeding mode **after the first backup** is performed	Notification ribbon (all tabs)

Requirements

Source machine requirements

The source machine on which the seed folder is created can function on Windows, macOS or Linux (view list of supported versions).

This is the machine whose data needs to be backed up.

Temporary storage medium requirements

Seeding can be performed to any of the following storage media:

- A removable storage device (a USB drive or hard disk)
- A network share or network-attached storage device (NAS)

> The user being used for the backup on the device **must** have **both** read and write access to the Network Share. If not, the backup will fail with an **Access denied** error

The **removable storage device** must operate on a standard file system. A non-standard file system such as HFS can make seeding data unreadable (you will get a warning if this is the case). The following file systems are recommended for removable drives:

- **Windows** - exFAT, NTFS
- **macOS** - exFAT
- **Linux** - exFAT, NTFS

Host machine requirements

The host machine from which you transfer the seeding data to the cloud must run on **Windows**.

It is possible to upload multiple devices' seed backups at the same time if the host machine's disk and internet can handle the increased load.

Optional Preparatory setup

If you plan to use the LocalSpeedVault with the device, consider enabling the feature **prior to starting your initial seed**. This will help prevent data seeded to the cloud from later having to be downloaded and synchronized to the LocalSpeedVault.

> ✖ Care must be taken when transferring the seeding folder to the cloud (see step 3 of the instructions). Some users specify a path to the LocalSpeedVault directory instead, which results in errors.

If in doubt, you can differentiate the LocalSpeedVault from the seeding directory by its name. Both of them are titled using the device name, but the LocalSpeedVault directory also has an ID attached. To avoid confusion, configure unique paths such as these:

- `x:\localspeedvault\` and `y:\seed\` (local)
- `\\server\backup\speedvault` and `\\server\backup\seed\` (network)

Troubleshooting

If missing or corrupt data is identified on the seed drive, you may receive an error message offering you to invalidate the missing data. This is done by adding the `-invalidate-missing-data` parameter to the `seeds.upload` command.

```
C:\Users\Administrator\Downloads\mxb-st-windows-x64>ServerTool.exe seeds.upload -
path F:\Seed\sony-vaio-hdqtrs -threadscount 3 -invalidate-missing-data
```

> ! Missing data invalidation is a **destructive operation** and should only be done if you understand why the data is missing and the risks that can occur. Consulting technical support is recommended.

> i If a seed upload or download is interrupted and restarted, the seed will pick up where it left off after a scan is ran of the data.

Seed backup Instructions

Before following the seed backup instructions below, please ensure you understand and have checked the following:

- Terms
- Requirements
  - Source machine requirements
  - Temporary storage medium requirements
  - Host machine requirements
- Optional Preparatory setup

Step 1. Set seeding path

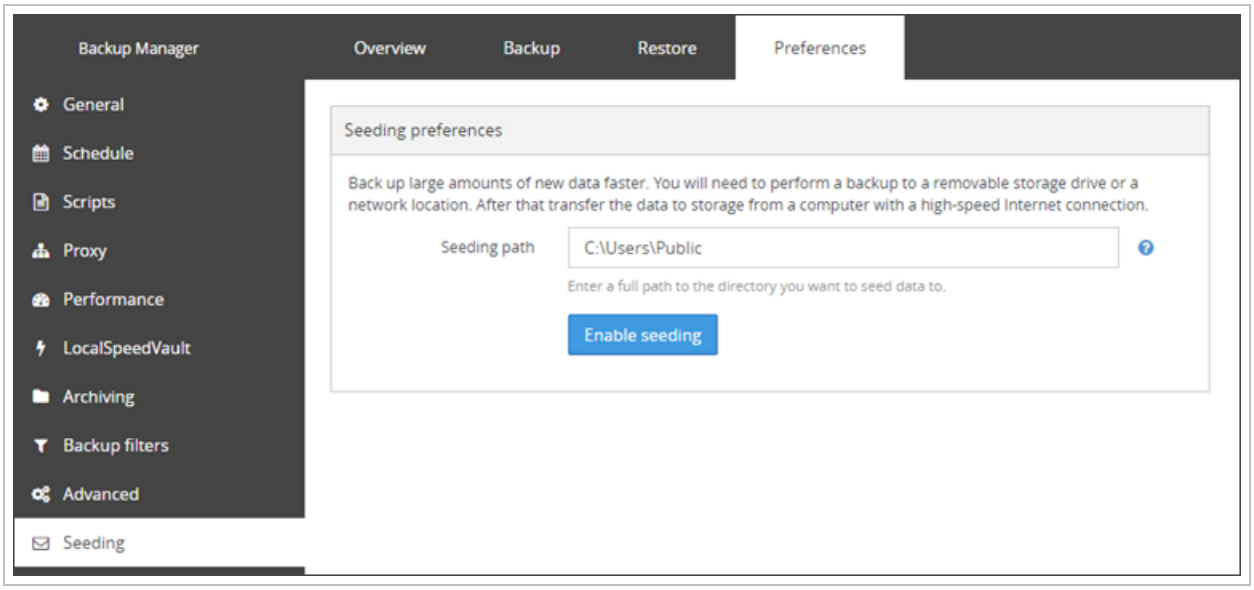
Connect a temporary storage medium to the computer that has data for backup. Then identify and **copy the full path** to the root of the storage medium or a directory on it. This will be used as the **seeding path** in the **Preferences > Seeding** section of Backup Manager.

How to copy the seeding path

- On **Windows**, copy the path from Windows Explorer. Examples: `F:\` or `F:\Seed`
- On **macOS**, use the Finder:
  1. Open the Finder (the removable drive will show under "Devices" in the Sidebar)
  2. Click the removable drive
  3. Right-click (or control-click) any directory on the removable drive. If no directories exist, you can create one first
  4. Choose **Get info** from the context menu
  5. Copy the path from the "Where" field. Example: `/Volumes/Seed`
- On **Linux**, follow instructions for your distribution

Step 2. Enable seeding

1. Launch the Backup Manager for the device
2. Click **Preferences > Seeding**
3. Paste the seeding path to the **Seeding path** field
4. Click **Enable seeding**

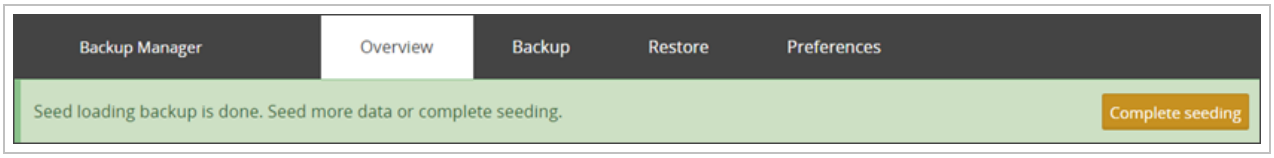


5. Open the **Backup** tab
6. Click **Run seeding**

> To monitor the status of the Seed backup, switch to the **Overview** tab and you will see the backup progress bar, which will detail the speed and size of the backup (among other things) as it does with any regular backup. Alternately, you can navigate using your file explorer to the seed location and monitor this for the seed data load, ensuring that this appears and has an appropriate modified date.

7. When the initial seeding session is completed, click **Run seeding** again to back up more data (if necessary). You can run a second backup, modify selections, or even add additional data sources

8. When all necessary data has been backed up, click **Complete seeding** on the notification ribbon



Once completed, you will find a new folder on the removable drive (located in the directory specified in **Preferences > Seeding**). This is the **seeding folder**. It has the same name as the backup device on which seeding has been done (for example "sony-vaio-hdqtrs").

> ✖ When seeding is enabled on the device, the Backup manager cancels any backup operations currently in-progress and prevents additional backup or restore jobs from running (including scheduled backups) until the device is switched to post-seeding mode.

Step 3. Transfer seeding folder to storage

Finally, transfer the offline files created by seeding to the cloud.

> ℹ A good thing is that while the data is on its way, the Backup Manager stays **functional**. You can continue backing up changed data to the cloud and to the LocalSpeedVault. Data recovery options while in the seeding and post-seeding modes are **temporarily limited** though.

1. Connect the removable drive to a **Windows computer** with a high-speed Internet connection
2. Download the **Server Tool** utility. You can get an installer from the Downloads module in the Management Console or from the Additional downloads page

   > ℹ The process name for the **Server Tool** utility is `servertool.exe`

3. Unpack the archive you have downloaded
4. Start Command Prompt from the Server Tool directory and run the following command:

   ```
   ServerTool.exe seeds.upload -path <path_to_seed_load_folder> -threadscount
   <number_of_threads>
   ```

   - `<path_to_seed_load_folder>` is the explorer path to the seed load folder
   - `<number_of_threads>` is the number of CPU threads used to process the seed. The higher the number, the more threads are used and so the faster the upload can complete

     > ℹ This variable is a number between 1 and 15, we recommend leaving this as the default of 3.

Here is an example:

```
C:\Users\Administrator\Downloads\mxb-st-windows-x64>ServerTool.exe seeds.upload -
path F:\Seed\sony-vaio-hdqtrs -threadscount 3
```

If the path to the folder contains **spaces**, double quotation marks are necessary (for example `"F:\Seed backup\sony-vaio-hdqtrs"`).

> The command window will show the percentage of the seed upload complete, so this can be monitored until completion.

After the upload completes and the data is processed on the server, the Backup Manager will exit the seeding mode. The data transferred to the cloud using the seed loading feature will soon become available for recovery.

Additional advanced options for Backup Manager

- Command-line interface for Backup Manager
- Virtual Drive: for quick access to backups
- Configuration File
  - Config.ini location
  - Required settings for Backup configuration file

Command-line interface for Backup Manager

It is possible to operate the Backup Manager through the command line interface. This is done with the help of the Client Tool (ClientTool.exe) - an executable file included into all Backup Manager installations.

Instructions

1. Start a terminal emulator as an Administrator, for example Command Prompt on Windows or Terminal on macOS
2. Change directory to the location containing the Client Tool executable
   - Windows:

     ```
     cd "C:\Program Files\Backup Manager"
     ```

   - GNU/Linux:

     ```
     cd /opt/backup-manager/bin
     ```

   - macOS:

     ```
     cd /Applications/Backup Manager.app/Contents/MacOS/ClientTool
     ```

3. Submit an appropriate command (the list of available commands is available below)
   - Windows example:

     ```
     ClientTool.exe "command"
     ```

   - GNU/Linux and macOS example:

     ```
     sudo ./ClientTool "command"
     ```

Commands by Category

See below a breakdown of each command, their purposes and examples of use for your quick reference:

> For any command that shows the output with the '*SELS*', '*SENTS*' and '*PROCS*' columns: these can be in Bytes, MB and GB depending on selection. If more than 1MB, the column will show an 'M' next to the figure, and if more than 1GB, the column will show a 'G' next to the figure.

Help

- `help` - returns the list of **available commands** with a brief description of the commands purpose

```
C:\Program Files\Backup Manager>clienttool.exe help
Client Tool, version 21.10.0.21280 (#13afc99a76-5305)
Copyright (c) (c) 2021 N-able Technologies Ltd.
All rights reserved.

Usage:
    clienttool.exe [global arguments] command [arguments] ...

    Multiple commands could be given at once.

    To get help on a command, run ``clienttool.exe help -command command.name''

Commands:
    bm-ui.open                        Open Backup Manager User Interface in a default browser
    control.application-status.get    Print current application status.
    control.archiving.add             Create new archiving rule.
    control.archiving.list            List existing archiving rules.
    control.archiving.modify          Modify existing archiving rule.
    control.archiving.remove          Remove existing archiving rule.
    control.backup.start              Start backup.
    control.dashboard.unsubscribe     Reset dashboard email.
    control.filter.list               List FileSystem datasource filters.
    control.filter.modify             Modify filters for FileSystem datasource.
    control.initialization-error.get  Gets application initialization error in json format
    control.mysqldb.add               Create new MySQL server entry.
    control.mysqldb.list              List existing MySQL server entries.
    control.mysqldb.modify            Modify existing MySQL server entry.
    control.mysqldb.remove            Remove existing MySQL server entry.
    control.networkshare.add          Create new network share entry.
    control.networkshare.list         List existing Network share entries.
    control.networkshare.modify       Modify existing Network share entry.
    control.networkshare.remove       Remove existing Network share entry.
    control.oracledb.add              Create new Oracle server entry.
    control.oracledb.list             List existing Oracle server entries.
    control.oracledb.modify           Modify existing Oracle server entry.
    control.oracledb.remove           Remove existing Oracle server entry.
    control.restore.start             Start restore.
    control.schedule.add              Create new schedule.
    control.schedule.list             List existing schedules.
    control.schedule.modify           Modify existing schedule.
    control.schedule.remove           Remove existing schedule.
    control.script.add                Create new script.
    control.script.list               List existing scripts.
    control.script.modify             Modify existing script.
    control.script.remove             Remove existing script.
    control.selection.clear           Clear backup selections.
    control.selection.list            List backup selections.
    control.selection.modify          Modify backup selections.
    control.session.abort             Abort backup or restore session.
    control.session.error.list        List session errors.
    control.session.list              List backup and restore sessions.
    control.session.node.export       Export session nodes to file.
    control.session.node.list         List session nodes.
    control.setting.list              List application settings.
    control.setting.modify            Modify application settings.
    control.status.get                Print current program status.
    fp                                Setup connection to functional process.
    help                              Print various help information.

Global arguments:
   -machine-readable
        Produce command output (if any) in machine-readable format.
   -non-interactive
        Do not ask questions (if any).
   -version
        Print program version and exit.
```

- `help -c "command"` - returns details for a **particular command** (sample output, required arguments and optional arguments)

```
C:\Program Files\Backup Manager>clienttool.exe help -command help
Client Tool, version 21.10.0.21280 (#13afc99a76-5305)
Copyright (c) (c) 2021 N-able Technologies Ltd.
All rights reserved.

Usage:
    clienttool.exe [global arguments] command [arguments] ...

    Multiple commands could be given at once.

Command:
    help
        Print various help information.

Optional command arguments:
   -arguments
        Print list of command arguments instead of description.
   -command <NAME>
        Specific command name to print help information about.

Global arguments:
   -machine-readable
        Produce command output (if any) in machine-readable format.
   -non-interactive
        Do not ask questions (if any).
   -version
        Print program version and exit.
```

Archiving

- `control.archiving.add` - Create new archiving rule. You can view existing archiving rules using the `control.archiving.list` command (which also prints ID for each rule)

Required:

Name

```
-name "string"
```

Name of the rule/entry, cannot be empty.

Optional:

Active

```
-active "bool"
```

Determines whether the rule is active. Possible values are **0** (not active) or **1** (active). If not specified, the default value is **1**.

Data Sources

```
-datasources "data source name"
```

The possible data sources are **Exchange**, **FileSystem**, **NetworkShares**, **Oracle**, **SystemState**, **VMware**, **VssHyperV**, **VssMsSql**, **VssSharePoint** or **All**. Default value is **All**.

Day of the Week

```
-day-of-week "name"
```

Day (or days) of the week when the rule us active. If you use this argument, `-weeks` should also be specified. Possible values are **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday** or **Sunday**.

Day of the Month

```
-days-of-month "day1,day2..."
```

Day (or range of days) when the rule is active, separated by comma. This argument is mutually exclusive with `-day-of-week` and `-weeks` arguments. Possible values are **numbers between 1 and 31**, ranges in the form **[N-M]** or **Last** (matching last day of month). Default value is **[1-31]**.

Example:

```
-days-of-month 2,[5-10],20,Last
```

Months

```
-months "Month1,Month2"
```

Month (or months) of the year when rule is active, separated by comma. Possible values are **Jan**, **Feb**, **Mar**, **Apr**, **May**, **Jun**, **Jul**, **Aug**, **Sep**, **Oct**, **Nov**, **Dec** and **All**. Default value is **All**.

Example:

```
Jan,Sep,Dec,May
```

Time

```
-time "time"
```

Time for rule activation. Must be in format **hh:mm**. Default value is **00:00**.

Weeks

```
-weeks "Week1, Week2"
```

Week (or weeks) when the rule is active, separated by comma. If you use this argument, `-day-of-week` should also be specified. Possible values are 1, 2, 3, 4, Last and All.

Example:

```
-weeks 1,2,Last
```

EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.archiving.add -name name-of-archive -datasource FileSystem -days-of-
month 1,15 -months All -time 13:07
```

OR

```
control.archiving.add -name name-of-archive -datasource FileSystem -day-of-
week Monday -months All -time 13:07 -weeks Last
```

```
control.archiving.add -name "name of archive" -active "1" -datasource
"FileSystem,SystemState" -day-of-week "Monday" -days-of-month"1,15" -months
"All" -time "13:07" -weeks "1,3"
```

- `control.archiving.list` - List existing archiving rules. Produces a table with columns in this order:
  1. `ID` -- Unique archiving rule identifier
  2. `ACTV` -- Is rule active or not
  3. `NAME` -- Archiving rule name
  4. `DSRC` -- Datasources to archive
  5. `TIME` -- Time archiving will fire at
  6. `MONTHS` -- Months archiving will fire in
  7. `MDAYS` -- Days of month archiving will fire on
  8. `WEEKS` -- Weeks archiving will fire on
  9. `WDAYS` -- Days of week archiving will fire on

  > Rule ID (first column) could further be used to modify or remove that specific rule.

Optional:

Delimiter

```
-delimiter "string"
```

This argument breaks the output up by the delimiter given and displays the output in table format. If no string is given to specify the delimiter, the default is the TAB character.

No Header

```
-no-header
```

This argument will print the table without the header column

EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.archiving.list -delimiter "-" -no-header
```

- `control.archiving.modify` - Modify existing archiving rule. Rule ID is used to locate the rule to be modified. All other arguments are optional and will not affect corresponding rule properties unless specified. You can view existing archiving rules using the `control.archiving.list` command (which also prints ID for each rule).

Required:

ID

```
-id "NUMBER"
```

ID of rule to be modified.

Optional:

Active

```
-active "bool"
```

Determines whether the rule is active. Possible values are **0** (not active) or **1** (active). If not specified, the default value is **1**.

Data Sources

```
-datasources "data source name"
```

The possible data sources are **Exchange**, **FileSystem**, **NetworkShares**, **Oracle**, **SystemState**, **VMware**, **VssHyperV**, **VssMsSql**, **VssSharePoint** or **All**. Default value is **All**.

Day of the Week

```
-day-of-week "name"
```

Day (or days) of the week when the rule us active. If you use this argument, `-weeks` should also be specified. Possible values are **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday** or **Sunday**.

Day of the Month

```
-days-of-month "day1,day2..."
```

Day (or range of days) when the rule is active, separated by comma. This argument is mutually exclusive with `-day-of-week` and `-weeks` arguments. Possible values are **numbers between 1 and 31**, ranges in the form **[N-M]** or **Last** (matching last day of month). Default value is **[1-31]**.

Example:

```
-days-of-month 2,[5-10],20,Last
```

Months

```
-months "Month1,Month2"
```

Month (or months) of the year when rule is active, separated by comma. Possible values are **Jan**, **Feb**, **Mar**, **Apr**, **May**, **Jun**, **Jul**, **Aug**, **Sep**, **Oct**, **Nov**, **Dec** and **All**. Default value is **All**.

Example:

```
Jan,Sep,Dec,May
```

Name

```
-name "string"
```

Name of the rule/entry, cannot be empty.

Time

```
-time "time"
```

Time for rule activation. Must be in format **hh:mm**. Default value is **00:00**.

Weeks

```
-weeks "Week1, Week2"
```

Week (or weeks) when the rule is active, separated by comma. If you use this argument, `-day-of-week` should also be specified. Possible values are 1, 2, 3, 4, Last and All.

Example:

```
-weeks 1,2,Last
```

EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.archiving.modify -id 2 -datasource FileSystem -days-of-month 2,16 -
months Jan,Mar,May,Jul,Sep,Nov -name name of file -time 17.30
```

OR

```
control.archiving.modify -id 2 -datasource FileSystem -day-of-week Tuesday -
months Jan,Mar,May,Jul,Sep,Nov -name name of file -time 17.30 -weeks Last
```

- `control.archiving.remove` - Remove existing archiving rule. Rule ID is used to locate the rule to be removed. You can view existing archiving rules using the `control.archiving.list` command (which also prints ID for each rule).

  Required:

  ID

  ```
  -id "NUMBER"
  ```

  ID of rule to be modified.
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.archiving.remove -id 3
  ```

MySQL

- `control.mysqldb.add` - Create new MySQL server entry. You can view existing entries using the `control.mysqldb.list` command.

  Required:

  ### Name

  ```
  -name "string"
  ```

  Name of the rule/entry, cannot be empty.

  ### Password

  ```
  -password "STRING"
  ```

  Password to use to connect.

  ### MySQL Server Port

  ```
  -server-port "NUMBER"
  ```

  MySQL server port.

  ### User

  ```
  -user "STRING"
  ```

  Username to use to connect.
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.mysqldb.add -name ServerEntry -server-port ServerPort# -user
  ServerUsername -password ServerPassword
  ```

- `control.mysqldb.list` - List existing MySQL server entries. Produces a table with columns in this order:
  1. `NAME` -- Unique entry name
  2. `USER` -- Login username
  3. `PASSWD` -- Login password
  4. `SRVPORT` -- MySQL server port

> Entry name (first column) could further be used to modify or remove that specific entry.

Optional:

Delimiter

```
-delimiter "string"
```

This argument breaks the output up by the delimiter given and displays the output in table format. If no string is given to specify the delimiter, the default is the TAB character.

No Header

```
-no-header
```

This argument will print the table without the header column
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.mysqldb.list -delimiter - -no-header
```

- `control.mysqldb.modify` - Modify existing MySQL server entry. Entry name is used to locate the entry to be modified. All other arguments are optional and will not affect corresponding entry properties unless specified. You can view existing entries using the `control.mysqldb.list` command.

Required:

Name

```
-name "string"
```

Name of the rule/entry, cannot be empty.

MySQL Server Port

```
-server-port "NUMBER"
```

MySQL server port.

Optional:

New Port

```
-new-port "NUMBER"
```

MySQL server port number.

Password

```
-password "STRING"
```

Password to use to connect.

User

```
-user "STRING"
```

Username to use to connect.
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.mysqldb.modify -name ServerEntry -server-port ServerPort# -new-port
NewPort# -user ServerUsername -password ServerPassword
```

- `control.mysqldb.remove` - Remove existing MySQL server entry. Server port is used to locate the entry to be removed. You can view existing entries using the `control.mysqldb.list` command.

  Required:

  MySQL Server Port

  ```
  -server-port "NUMBER"
  ```

  MySQL server port.
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.mysqldb.remove -serve-port ServePort#
  ```

Network Share

- `control.networkshare.add` - Create new network share entry. You can view existing entries using the `control.networkshare.list` command.

Required:

Domain

```
-domain "STRING"
```

Domain to use to connect to network share.

Path to Network Share

```
-path "STRING"
```

Path to network share, cannot be empty.

User

```
-user "STRING"
```

Username to use to connect.

Optional:

Password

```
-password "STRING"
```

Password to use to connect.
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.networkshare.add -domain domainName -path ../network/share/path -user
NetworkShareUsername -password NetworkSharePassword
```

- `control.networkshare.list` - List existing Network share entries. Produces a table with columns in this order:

  1. `PATH` -- Unique path to network share
  2. `DOMAIN` -- Login domain
  3. `USER` -- Login username
  4. `PASSWD` -- Login password

  > Entry name (first column) could further be used to modify or remove that specific entry.

  ## Optional:

  ### Delimiter

  ```
  -delimiter "string"
  ```

  This argument breaks the output up by the delimiter given and displays the output in table format. If no string is given to specify the delimiter, the default is the TAB character.

  ### No Header

  ```
  -no-header
  ```

  This argument will print the table without the header column
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.networkshare.list -delimiter - -no-header
  ```

- `control.networkshare.modify` - Modify existing Network share entry. Entry path is used to locate the entry to be modified. All other arguments are optional and will not affect corresponding entry properties unless specified. You can view existing entries using the `control.networkshare.list` command.

Required:

Path to Network Share

```
-path "STRING"
```

Path to network share, cannot be empty.

Optional:

Domain

```
-domain "STRING"
```

Domain to use to connect to network share.

New Path

```
-new-path "STRING"
```

New path to network share, non-empty.

Password

```
-password "STRING"
```

Password to use to connect.

User

```
-user "STRING"
```

Username to use to connect.
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.networkshare.modify -path ../network/share/path -domain domainName -
new-path ../new/network/share/path -user NetworkShareUsername -password
NetworkSharePassword
```

- `control.networkshare.remove` - Remove existing Network share entry. Path is used to locate the entry to be removed. You can view existing entries using the `control.networkshare.list` command.

  Required:

  Path to Network Share

  ```
  -path "STRING"
  ```

  Path to network share, cannot be empty.
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.networkshare.remove -path ../network/share/path
  ```

Oracle

- `control.oracledb.add` - Create new Oracle server entry. You can view existing entries using the `control.oracledb.list` command.

  Required:

  ### Local Backup Directory

  ```
  -local-backup-dir "DIR"
  ```

  Path to temporary directory to use during backup.

  ### Name

  ```
  -name "string"
  ```

  Name of the rule/entry, cannot be empty.

  ### Password

  ```
  -password "STRING"
  ```

  Password to use to connect.

  ### User

  ```
  -user "STRING"
  ```

  Username to use to connect.
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.oracledb.add -local-backup-dir ../directory/to/use -name
  OracleRuleName -user username -password password
  ```

- `control.oracledb.list` - List existing Oracle server entries. Produces a table with columns in this order:
  1. `NAME` -- Unique entry name
  2. `USER` -- Login username
  3. `PASSWD` -- Login password
  4. `LOCDIR` -- Path to local backup directory

  > Entry name (first column) can further be used to modify or remove that specific entry.

  ## Optional:

  ### Delimiter

  ```
  -delimiter "string"
  ```

  This argument breaks the output up by the delimiter given and displays the output in table format. If no string is given to specify the delimiter, the default is the TAB character.

  ### No Header

  ```
  -no-header
  ```

  This argument will print the table without the header column
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.oracledb.list -delimiter - -no-header
  ```

- `control.oracledb.modify` - Modify existing Oracle server entry. Entry name is used to locate the entry to be modified. All other arguments are optional and will not affect corresponding entry properties unless specified. You could view existing entries using the `control.oracledb.list` command.

Required:

Name

```
-name "string"
```

Name of the rule/entry, cannot be empty.

Rename

```
-rename "string"
```

Name of the rule/entry, cannot be empty.

Optional:

Local Backup Directory

```
-local-backup-dir "DIR"
```

Path to temporary directory to use during backup.

Password

```
-password "STRING"
```

Password to use to connect.

User

```
-user "STRING"
```

Username to use to connect.
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.oracledb.modify -name OracleRuleName -rename newOracleRuleName -
local-backup-dir ../directory/to/use -user username -password password
```

- `control.oracledb.remove` - Remove existing Oracle server entry. Entry name is used to locate the entry to be removed. You could view existing entries using the `control.oracledb.list` command.

  Required:

  Name

  ```
  -name "string"
  ```

  Name of the rule/entry, cannot be empty.

  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.oracledb.remove -name OracleRuleName
  ```

Schedule

- `control.schedule.add` - Create new schedule. You can view existing schedules using the `control.schedule.list` command.

Required:

Name

```
-name "string"
```

Name of the rule/entry, cannot be empty.

Optional:

Active

```
-active "bool"
```

Determines whether the rule is active. Possible values are **0** (not active) or **1** (active). If not specified, the default value is **1**.

Data Sources

```
-datasources "data source name"
```

The possible data sources are **Exchange**, **FileSystem**, **NetworkShares**, **Oracle**, **SystemState**, **VMware**, **VssHyperV**, **VssMsSql**, **VssSharePoint** or **All**. Default value is **All**.

Days

```
-days "day1,day2"
```

Day (or days) of the week when the rule us active. If you use this argument, `-weeks` should also be specified. Possible values are **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, **Sunday** or **All**. Default is **All**.

Post-Backup Script

```
-post-backup-action "NUMBER"
```

ID of post-backup script. All available scripts can be viewed with the `control.script.list` command.

Pre-Backup Script

```
-pre-backup-action "NUMBER"
```

ID of pre-backup script. All available scripts can be viewed with the `control.script.list` command.

Time

```
-time "time"
```

Time for rule activation. Must be in format **hh:mm**. Default value is **00:00**.
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.schedule.add -name NameOfSchedule -datasources Exchange,SystemState -
days All -post-backup-action Script #1 -pre-backup-action Script #2 -time
18:00
```

- `control.schedule.list` - List existing schedules. Produces a table with columns in this order:
  1. `ID` -- Unique schedule identifier
  2. `ACTV` -- Is schedule active or not
  3. `NAME` -- Schedule name
  4. `TIME` -- Time backup will fire at
  5. `DAYS` -- Days backup will fire on
  6. `DSRC` -- Datasources to backup
  7. `PRESID` -- Pre-backup script ID
  8. `POSTSID` -- Post-backup script ID

> Schedule ID (first column) could further be used to modify or remove that specific schedule.

Optional:

Delimiter

```
-delimiter "string"
```

This argument breaks the output up by the delimiter given and displays the output in table format. If no string is given to specify the delimiter, the default is the TAB character.

No Header

```
-no-header
```

This argument will print the table without the header column
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.schedule.list -delimiter - -no-header
```

- `control.schedule.modify` - Modify existing schedule. Schedule ID is used to locate the schedule to be modified. All other arguments are optional and will not affect corresponding schedule properties unless specified. You can view existing schedules using the `control.schedule.list` command (which also prints ID for each schedule).

Required:

ID

```
-id "NUMBER"
```

ID of rule to be modified.

Optional:

Active

```
-active "bool"
```

Determines whether the rule is active. Possible values are **0** (not active) or **1** (active). If not specified, the default value is **1**.

Data Sources

```
-datasources "data source name"
```

The possible data sources are **Exchange**, **FileSystem**, **NetworkShares**, **Oracle**, **SystemState**, **VMware**, **VssHyperV**, **VssMsSql**, **VssSharePoint** or **All**. Default value is **All**.

Days

```
-days "day1,day2"
```

Day (or days) of the week when the rule us active. If you use this argument, `-weeks` should also be specified. Possible values are **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, **Sunday** or **All**. Default is **All**.

Name

```
-name "string"
```

Name of the rule/entry, cannot be empty.

Post-Backup Script

```
-post-backup-action "NUMBER"
```

ID of post-backup script. All available scripts can be viewed with the `control.script.list` command.

Pre-Backup Script

```
-pre-backup-action "NUMBER"
```

ID of pre-backup script. All available scripts can be viewed with the `control.script.list` command.

Time

```
-time "time"
```

Time for rule activation. Must be in format **hh:mm**. Default value is **00:00**.
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.schedule.modify -id 1 -datasource FileSystem -days
Tuesday,Wednesday,Thursday -name name of rule -post-backup-action Script #1 -
pre-backup-action Script #2 -time 17.30
```

- `control.schedule.remove` - Remove existing schedule. Schedule ID is used to locate the schedule to be removed. You can view existing schedules using the `control.schedule.list` command (which also prints ID for each schedule).

Required:

ID

```
-id "NUMBER"
```

ID of rule to be modified.
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.schedule.remove -id 1
```

Script

- `control.script.add` - Create new script. Scripts can be used in combination with schedules as pre- and post-backup actions. To do this, add new (or find existing) script and provide its ID to `control.schedule.add` or `control.schedule.modify` command. You can view existing scripts using `control.script.list` command (which also prints ID for each script).

Required:

Content File path

```
-content-file "PATH"
```

Path to file with non-empty script body.

Name

```
-name "string"
```

Name of the rule/entry, cannot be empty.

Password

```
-password "STRING"
```

Password to use to connect.

User

```
-user "STRING"
```

Username to use to connect.

Optional:

Fail Session on Error

```
-fail-session-on-error "BOOL"
```

Whether backup session should fail on script error, when used as pre-backup action. Possible values are **0** (do not fail) or **1** (fail). Default value is **0**.

Timeout

```
-timeout "NUMBER"
```

Execution timeout, in seconds. Default value is **0** (no timeout).

EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.script.add -content-file ../path/to/script/file -name NameOf Rule -
user username -password password -fail-session-on-error 0 -timeout 240
```

- `control.script.list` - List existing scripts. Produces a table with columns in this order:
  1. `ID` -- Unique script identifier
  2. `NAME` -- Script name
  3. `USER` -- User to run script as
  4. `PASWD` -- User password
  5. `TOUT` -- Execution timeout
  6. `FAIL` -- Fail backup on error

> Script ID (first column) could further be used to modify or remove that specific script.

Optional:

Delimiter

```
-delimiter "string"
```

This argument breaks the output up by the delimiter given and displays the output in table format. If no string is given to specify the delimiter, the default is the TAB character.

No Header

```
-no-header
```

This argument will print the table without the header column
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.script.list -delimiter - -no-header
```

- `control.script.modify` - Modify existing script. Script ID is used to locate the script to be modified. All other arguments are optional and will not affect corresponding script properties unless specified. You can view existing scripts using `control.script.list` command (which also prints ID for each script).

Required:

ID

```
-id "NUMBER"
```

ID of rule to be modified.

Password

```
-password "STRING"
```

Password to use to connect.

User

```
-user "STRING"
```

Username to use to connect.

Optional:

Content File path

```
-content-file "PATH"
```

Path to file with non-empty script body.

Fail Session on Error

```
-fail-session-on-error "BOOL"
```

Whether backup session should fail on script error, when used as pre-backup action. Possible values are **0** (do not fail) or **1** (fail). Default value is **0**.

Name

```
-name "string"
```

Name of the rule/entry, cannot be empty.

Timeout

```
-timeout "NUMBER"
```

Execution timeout, in seconds. Default value is **0** (no timeout).
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.script.modify -id 1 -user username -password password -content-file
../path/to/script/file -fail-session-on-error 0 -name NameOfRule -timeout 240
```

- `control.script.remove` - Remove existing script. Script ID is used to locate the script to be removed. You could view existing scripts using `control.script.list` command (which also prints ID for each script).

Required:

ID

```
-id "NUMBER"
```

ID of rule to be modified.
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.script.remove -id 2
```

Selection

You can specify what you want to back up through the Client Tool. These are the same settings that you can find on the Preferences tab in the Backup Manager.

- `control.selection.clear` - This function deselects the current backup selection for the data sources given but does not affect any data previously backed up. Currently selected files data on disk not affected in any way. If no datasource is specified, selections for all datasources are cleared.

> If left blank, all data source selection will be cleared.

Optional:

Data Sources

```
-datasources "data source name"
```

The possible data sources are **Exchange**, **FileSystem**, **NetworkShares**, **Oracle**, **SystemState**, **VMware**, **VssHyperV**, **VssMsSql**, **VssSharePoint** or **All**. Default value is **All**.
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.selection.clear -datasource FileSystem
```

- `control.selection.list` - List backup selections. List backup selections. Produces a table with columns in this order:
  1. `DSRC` -- Datasource
  2. `TYPE` -- Type (inclusive, exclusive)
  3. `PRIO` -- Priority
  4. `PATH` -- Selected path

  ## Optional:

  ### Data Sources

  ```
  -datasources "data source name"
  ```

  The possible data sources are **Exchange**, **FileSystem**, **NetworkShares**, **Oracle**, **SystemState**, **VMware**, **VssHyperV**, **VssMsSql**, **VssSharePoint** or **All**. Default value is **All**.

  ### Delimiter

  ```
  -delimiter "string"
  ```

  This argument breaks the output up by the delimiter given and displays the output in table format. If no string is given to specify the delimiter, the default is the TAB character.

  ### No Header

  ```
  -no-header
  ```

  This argument will print the table without the header column
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.selection.list -datasource FileSystem -delimiter - -no-header
  ```

- `control.selection.modify` - Modify backup selections.

  Inclusive selections point to files (folders, databases etc.) to be backed up. Exclusive selections denote files (folders, databases etc.) which should not be.

  Paths to be excluded can only be subpaths of those to be included. So if you need to backup a folder, but not a file within it, the former would be an inclusive selection while the latter - an exclusive one.

  ### Required:

  #### Data Sources

  ```
  -datasources "data source name"
  ```

  The possible data sources are **Exchange**, **FileSystem**, **NetworkShares**, **Oracle**, **SystemState**, **VMware**, **VssHyperV**, **VssMsSql**, **VssSharePoint** or **All**. Default value is **All**.

  ### Optional:

  #### Exclude

  ```
  -exclude "PATH"
  ```

  Path to file/folder to deselect. Can be used multiple times to deselect different items.

  #### Include

  ```
  -include "PATH"
  ```

  Path to file/folder to select. Can be used multiple times to select different items.

  #### Priority

  ```
  -priority "NAME"
  ```

  Backup priority assigned to selection, valid for inclusive paths only. Possible values are Low, Normal or High. Default value is Normal.
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.selection.modify -datasource FileSystem -exclude "../path/to/exclude"
  -include "../path/to/include" -include "System State" -priority High
  ```

Session

- `control.session.abort` - Abort backup or restore session. There is no way to abort a specific session, so all currently active sessions will be aborted.
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.session.abort
  ```

- `control.session.error.list` - List session errors. Displays session errors for specific datasource. Produces a table with TAB-separated (by default) columns in this order:
  1. `DATETIME` -- Error time
  2. `PATH` -- Node path
  3. `CONTENT` -- Error description

Required:

Data Sources

```
-datasources "data source name"
```

The possible data sources are **Exchange**, **FileSystem**, **NetworkShares**, **Oracle**, **SystemState**, **VMware**, **VssHyperV**, **VssMsSql**, **VssSharePoint** or **All**. Default value is **All**.

Optional:

Delimiter

```
-delimiter "string"
```

This argument breaks the output up by the delimiter given and displays the output in table format. If no string is given to specify the delimiter, the default is the TAB character.

No Header

```
-no-header
```

This argument will print the table without the header column

Limit

```
-limit "number"
```

The output will only show this number of errors. The default is **100**.

Date & Time

```
-time "datetime"
```

This should be the start time of the backup session whose errors you wish to view. The value must be provided in the format **yyyy-mm-dd hh:mm:ss**.
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.session.error.list -datasource FileSystem -delimiter - -limit 50 -no-
header -time 2020-05-14 13:52:07
```

- `control.session.list` - List backup and restore sessions. Displays sessions for specific datasource or (if none specified) for all datasources. Produces a table with TAB-separated (by default) columns in this order:
  1. `DSRC --` Datasource name
  2. `TYPE --` Session type
  3. `STATE --` Status
  4. `FLAGS --` Session flags (see below)
  5. `START --` Start time
  6. `END --` End time
  7. `SELS --` Selected size
  8. `SELC --` Selected files count
  9. `PROCS --` Processed size
  10. `PROCC --` Processed files count
  11. `SENTS --` Sent size
  12. `ERRC --` Errors count
  13. `REMC --` Removed files count

> Session start time (fifth column) could further be used to restore files and folders from that specific session.

Optional:

Data Sources

```
-datasources "data source name"
```

The possible data sources are **Exchange**, **FileSystem**, **NetworkShares**, **Oracle**, **SystemState**, **VMware**, **VssHyperV**, **VssMsSql**, **VssSharePoint** or **All**. Default value is **All**.

Delimiter

```
-delimiter "string"
```

This argument breaks the output up by the delimiter given and displays the output in table format. If no string is given to specify the delimiter, the default is the TAB character.

No Header

```
-no-header
```

This argument will print the table without the header column
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.session.list -datasource FileSystem -delimiter - -no-header
```

- `control.session.node.export` - Export session nodes to file.

Required:

Domain

```
-domain "STRING"
```

Domain to use to connect to network share.

Optional:

Format

```
-format "NAME"
```

Output format. Possible values are **xml** or **csv**.

Output Field

```
-output-file "PATH"
```

Write output to specified file. Default is to use standard output stream, which could also be specified explicitly with "-" value.

Date & Time

```
-time "datetime"
```

This should be the start time of the backup session whose errors you wish to view. The value must be provided in the format **yyyy-mm-dd hh:mm:ss**.
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.session.node.export -datasource FileSystem -format csv -outout-file
../path/to/output-file -time 2021-10-20 02:10:44
```

- `control.session.node.list` - List session nodes. Displays changed or removed session nodes for specific datasource. Produces a table with TAB-separated (by default) columns in this order:
  1. `START --` Backup start time
  2. `END --` Backup end time
  3. `SIZE --` Node size
  4. `SENTS --` Sent size
  5. `PATH --` Node path

  > For removed nodes, only the last (PATH) column is displayed since others are not applicable.

  ### Required:

  #### Domain

  ```
  -domain "STRING"
  ```

  Domain to use to connect to network share.

  ### Optional:

  #### Delimiter

  ```
  -delimiter "string"
  ```

  This argument breaks the output up by the delimiter given and displays the output in table format. If no string is given to specify the delimiter, the default is the TAB character.

  #### No Header

  ```
  -no-header
  ```

  This argument will print the table without the header column

  #### Limit

  ```
  -limit "number"
  ```

  The output will only show this number of errors. The default is **100**.

  #### Offset

  ```
  -offset "number"
  ```

  Offset the number to start showing. The default is 0, so will show list from the beginning.

Removed Nodes

```
-removed
```

Displays removed nodes. The default is to show changed nodes

Date & Time

```
-time "datetime"
```

This should be the start time of the backup session whose errors you wish to view. The value must be provided in the format **yyyy-mm-dd hh:mm:ss**.
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.session.node.list -datasource FileSystem -delimiter - -no-header -
offset 0 -removed -time 12.30
```

Settings

- `control.setting.list` - List application settings. Produces a table with columns in this order:
  1. `NAME --` Setting name
  2. `VALUE --` Setting value

> Setting name (first column) could further be used to modify this specific setting value.

Optional:

Delimiter

```
-delimiter "string"
```

This argument breaks the output up by the delimiter given and displays the output in table format. If no string is given to specify the delimiter, the default is the TAB character.

No Header

```
-no-header
```

This argument will print the table without the header column

Plugin

```
-plugin "string"
```

Supported plugins for Settings: sims

Setting Name

```
-setting.name "string"
```

Supported setting names: **sims.server**, **sims.database**, **sims.db.attach.path**, **sims.path.to.shared**, **sims.path.to.dms**, **sims.backup.master**, **discover.database**, **discover.db.attach.path**, **fms.server**, **fms.database**, **fms.db.attach.path**
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.setting.list -delimiter - -no-header -plugin sims -setting.name
sims.server
```

- `control.setting.modify` - Modify application settings. Provided values are coupled with settings in same order. All available settings can be listed with `control.setting.list' command.

  Required:

  Name

  ```
  -name "string"
  ```

  Name of the rule/entry, cannot be empty.

  Value

  ```
  -value "string"
  ```

  Setting value. One value for each setting should be provided.
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.setting.modify -name sims.server -value setting.value
  ```

  LocalSpeedVault examples:

  The control.setting.modify command can be used to configure LocalSpeedVault use:

  - Disable LSV:

    ```
    control.setting.modify -name LocalSpeedVaultEnabled -value 0
    ```

  - Enable LSV:

    ```
    control.setting.modify -name LocalSpeedVaultEnabled -value 1
    ```

  - Enable LSV to local volume:

    ```
    control.setting.modify -name LocalSpeedVaultEnabled -value 1 -name
    LocalSpeedVaultLocation -value "F:\LocalSpeedVault" new
    ```

  - Enable LSV to network share:

    ```
    control.setting.modify -name LocalSpeedVaultEnabled -value 1 -name
    LocalSpeedVaultLocation -value \\server\localspeedvaultshare -name
    LocalSpeedVaultUser -value "Server\Administrator" -name
    LocalSpeedVaultPassword -value "password"
    ```

Status

- `control.status.get` - Print current program status.
  Optional:

  Path to Configuration File

  ```
  -path "DIR"
  ```

  Full path to config.ini file.
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.status.get -path ../path/to/config.ini
  ```

- `control.application-status.get` - Print current application status.
  Optional:

  Path to Configuration File

  ```
  -path "DIR"
  ```

  Full path to config.ini file.
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.application-status.get -path ../path/to/config.ini
  ```

Other Commands

- `control.backup.start` - Start backup. If no datasource is specified, the backup will start for all datasources. Backup would only be started if datasource in question has selections (and thus needs to be backed up).
  Optional:

  Data Sources

  ```
  -datasources "data source name"
  ```

  The possible data sources are **Exchange**, **FileSystem**, **NetworkShares**, **Oracle**, **SystemState**, **VMware**, **VssHyperV**, **VssMsSql**, **VssSharePoint** or **All**. Default value is **All**.
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.backup.start -datasource FileSystem
  ```

- `control.dashboard.unsubscribe` - Reset dashboard email. Disables dashboard generation after device uninstall.
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.dashboard.unsubscribe
  ```

- `control.filter.list` - Lists FileSystem data source filters one filter mask per line. Produces a list with one filter mask per line.
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.filter.list
  ```

- `control.filter.modify` - Modify filters for FileSystem datasource. Already existing filters will not be added, already missing filters will not be removed. If same filter mask is specified with both `-add` and `-remove` arguments, it will be added to the list (or remain if it was already there). All available filters can be listed with `control.filter.list` command.

  ## Optional:

  ### Add

  ```
  -add "MASK"
  ```

  Filter mask to add.

  Example:

  ```
  -add "*.txt" -add "*.docx" -add "*.doc".
  ```

  ### Remove

  ```
  -remove "MASK"
  ```

  Filter mask to remove. Example:

  ```
  -remove "*.mp3" -remove "*.avi".
  ```

  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.filter.modify -add *.txt -remove *.mp3
  ```

- `control.initialization-error.get` - Gets application initialization error in json format.

  ## Optional:

  ### Path to Configuration File

  ```
  -path "DIR"
  ```

  Full path to config.ini file.
  EXAMPLE COMMAND USING ALL ARGUMENTS:

  ```
  control.initialization-error.get -path ../path/to/config.ini
  ```

- `control.restore.start` - Start restore. Restores specific or all nodes of specific datasource which were backed up at specific time. Restore destination path can also be specified (but is optional).

  > You can view existing sessions to determine which one to restore using `control.session.list` command (which also prints start time for each session).

  ### Required:

  Data Sources

  ```
  -datasources "data source name"
  ```

  The possible data sources are **Exchange**, **FileSystem**, **NetworkShares**, **Oracle**, **SystemState**, **VMware**, **VssHyperV**, **VssMsSql**, **VssSharePoint** or **All**. Default value is **All**.

- **Optional:**

Add Suffix

```
-add-suffix
```

Add suffix to restored files

Existing Files Restore Policy

```
-existing-files-restore-policy "POLICY"
```

Existing files restore policy. Possible values are **Overwrite** or **Skip**. Default value is **Overwrite**.

Outdated Files Restore Policy

```
-outdated-files-restore-policy "POLICY"
```

Outdated files restore policy. Possible values are **CheckContentOfAllFiles** or **CheckContentOfOutdatedFilesOnly**. Default value is **CheckContentOfAllFiles**.

Restore To

```
-restore-to "DIR"
```

Path to start restore of selected sessions to. Default value is empty (in-place restore).

Selection

```
-selection "PATH"
```

Path to node (file, folder, etc.) to include in restore session. Can be used multiple times to select different nodes. If not specified, all session nodes are restored.

Session Search Policy

```
-session-search-policy "POLICY"
```

Backup session search policy. Possible values are **ClosestToRequested** or **OldestIfRequestedNotFound**. Default value is **ClosestToRequested**

Date & Time

```
-time "datetime"
```

This should be the start time of the backup session whose errors you wish to view. The value must be provided in the format **yyyy-mm-dd hh:mm:ss**.

EXAMPLE COMMAND USING ALL ARGUMENTS:

```
control.restore.start -datasource FileSystem -add-suffix -existing-files-
restore-policy Overwrite -outdated-files-restore-policy
CheckContentOfAllFiles -restore-to ../path/to/restore/to/ -selection
../path/of/file/to/restore -session-search-policy ClosestToRequested -time
2019-02-15 12:30:00
```

- `fp` - Setup connection to functional process. Using this command alone doesn't make sense, it should always precede other commands in the same command line invocation (including `help` command, if needed). It allows you to modify default values used to connect to functional process.

Optional:

Host

```
-host "STRING"
```

Host address of running functional process. Default is "**127.0.0.1**".

Password

```
-password "STRING"
```

Password to use to connect.

Port

```
-port "NUMBER"
```

Port number of running functional process. Default is taken from config.ini, or is an empty string otherwise.

Timeout

```
-timeout "NUMBER"
```

Number of seconds to wait for functional process response. Default is **120**.

Username

```
-username "STRING"
```

Username to use to connect to functional process. Default is taken from config.ini, or is an empty string otherwise.
EXAMPLE COMMAND USING ALL ARGUMENTS:

```
fp -host 127.0.0.1 -username username -password password -port Port# -timeout
240
```

Global Arguments

These are arguments that may be used in conjunction with all commands in Client Tool:

- `-machine-readable`

  Produce command output (if any) in machine-readable format.
- `-non-interactive`

  Do not ask questions (if any).
- `-version`

  Print program version and exit.

Miscellaneous

- `vss.check`

  Runs a generic vss check on the backup device, detailing the status of the service. If any issues, the appropriate vss error code will be displayed. e.g.

```
C:\Program Files\Backup Manager>clienttool.exe vss.check
Check operation system version:  Ok
Check NTFS partitions: Ok
Shadow copies could be made on the following drives: C:\  C:\ProgramData\Microsoft\Windows\Containers\BaseImages\7daf52fb-356b-4bd0-8409-1265e889cc76\BaseLayer\
Check VSS service: Ok
Check MS Software Shadow Copy Provider service: Ok
Attempt to create test snapshot for available drives...
Test snapshot was not created. Reason: VSS error 0x8004230c: Shadow copying the specified volume is not supported.
```

Virtual Drive: for quick access to backups

> The Virtual Drive is a **Windows utility** only.

The Virtual Drive **must be installed alongside the Backup Manager**. It will create **a drive letter on the Windows Explorer** where you can browse through your backup sessions locally. Files can be dragged and dropped out of the Virtual Drive to **restore backup data to the local filesystem**.

> If you backed up a Virtual Machine with a dynamic disk (also known as **thin provisioning**), you will **not** be able to expand this via the Virtual Drive feature.

Requirements

The Virtual Drive utility relies on the **Backup Manager installation**.

- Windows login credentials of a user in the **Administrators'** group, or a member of the automatically created **N-able Backup Users** group

  > Due to a File Explorer limitation, to open Virtual Drive via the Windows File Explorer, the user must be a member of the **N-able Backup Users** group. See Users and Groups Permissions

- The Backup Manager must be installed on the machine prior to the Virtual Drive installation
- The version of the Virtual Drive must be same as the Backup Manager

  > You will see a warning message in case of version incompatibility

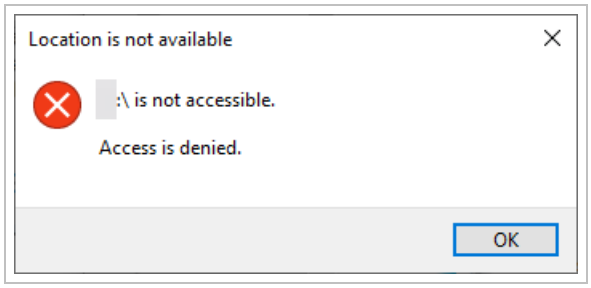
- Download the Virtual Drive installation file prior to beginning

  > This can be found from the Downloads page in Management Console, or from the Backup Downloads page on our website.

Users and Groups Permissions

Virtual Drive can **only** be opened on the device by an **Administrators'** group user or a member of the automatically created **N-able Backup Users** group.

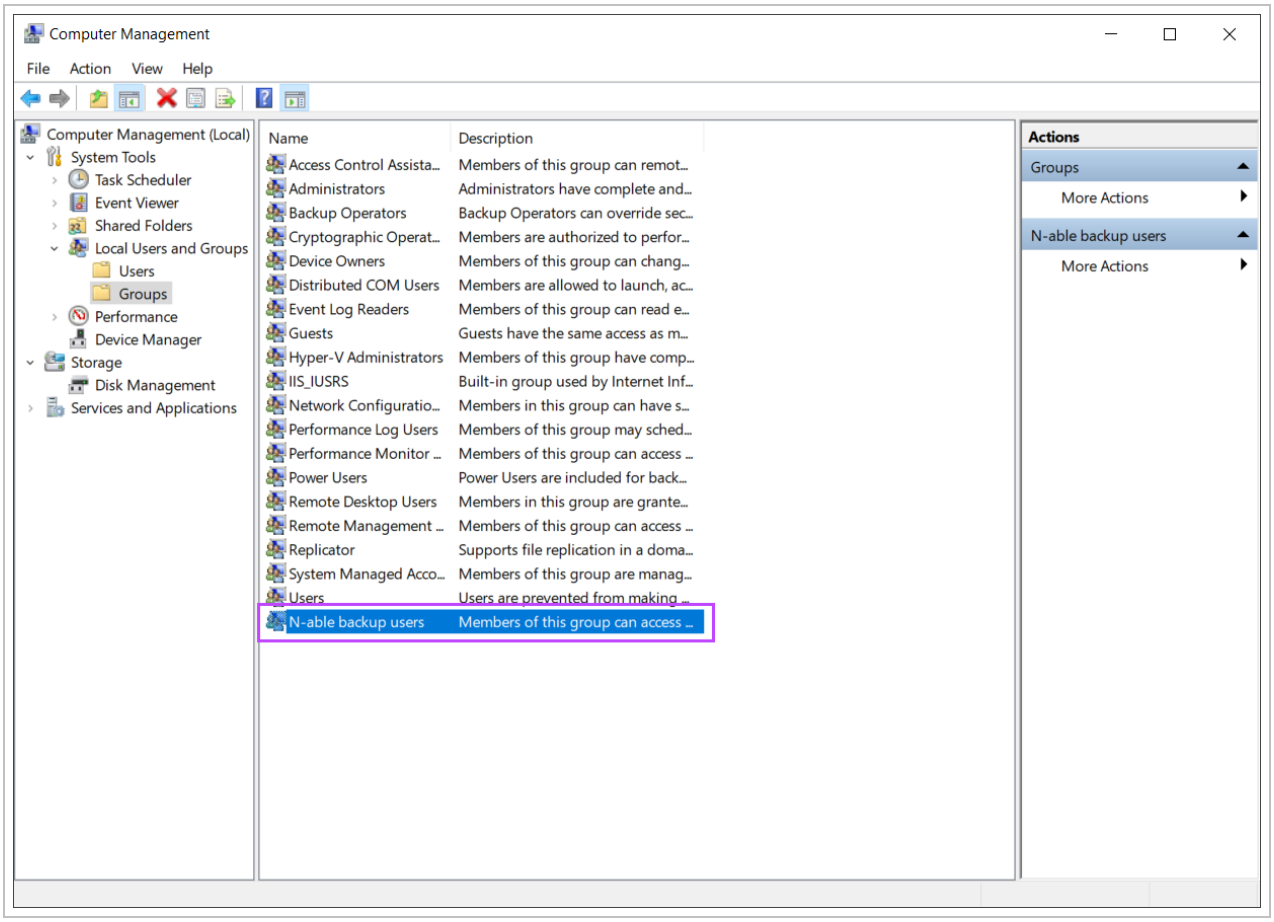
If the user is not a member of either of the above groups, you will see the following error when trying to open the drive letter:



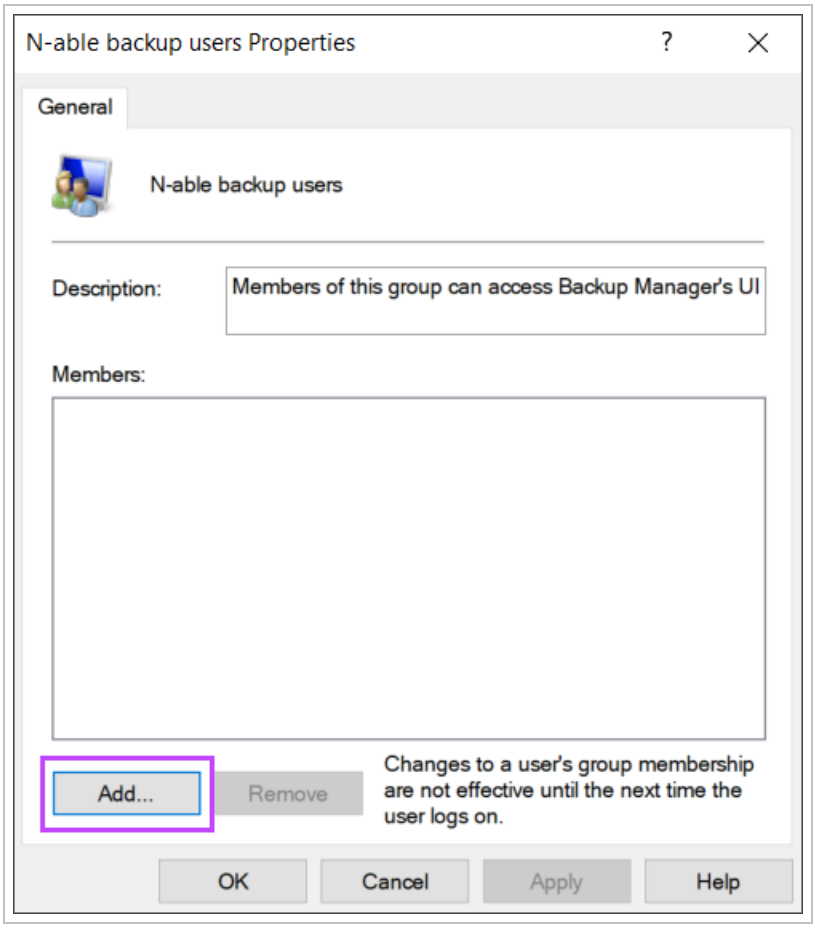
To allow the user the appropriate permissions:

1. Open the **Start** menu and open **Computer Management**
2. Navigate to **System Tools** > **Local Users and Groups**
3. Open **Groups**

4. Open the **N-able Backup Users** group

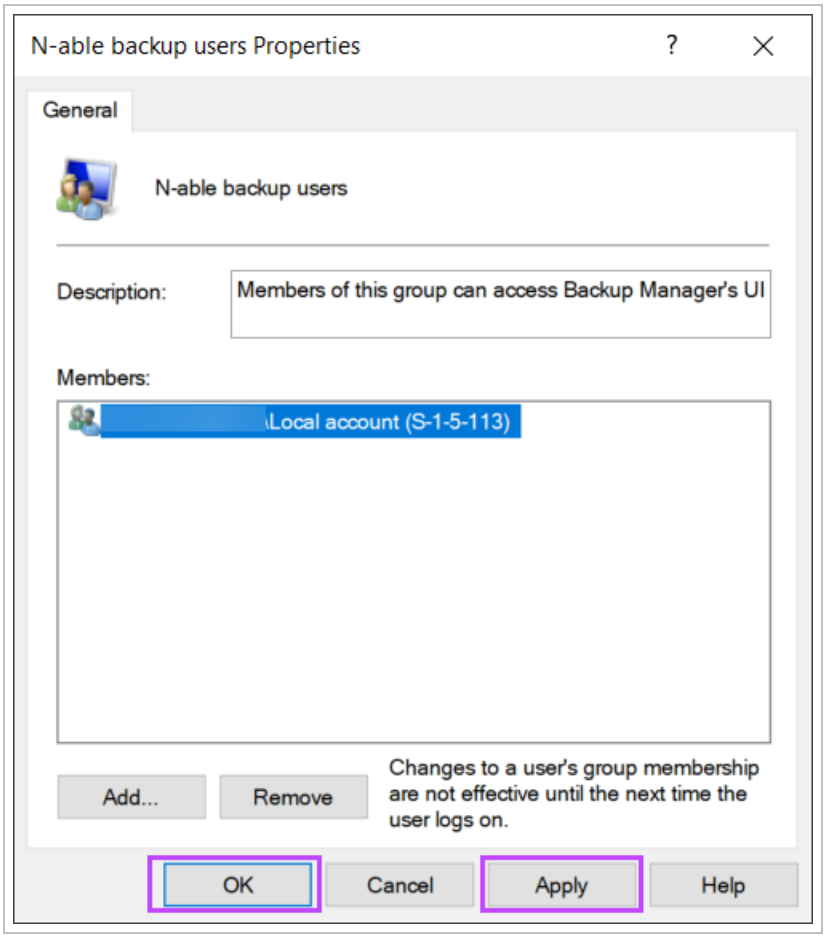


5. Click **Add**



6. Add the user or local account as a member of the group
7. **Apply** the changes

8. Click **OK** to close out of the properties window

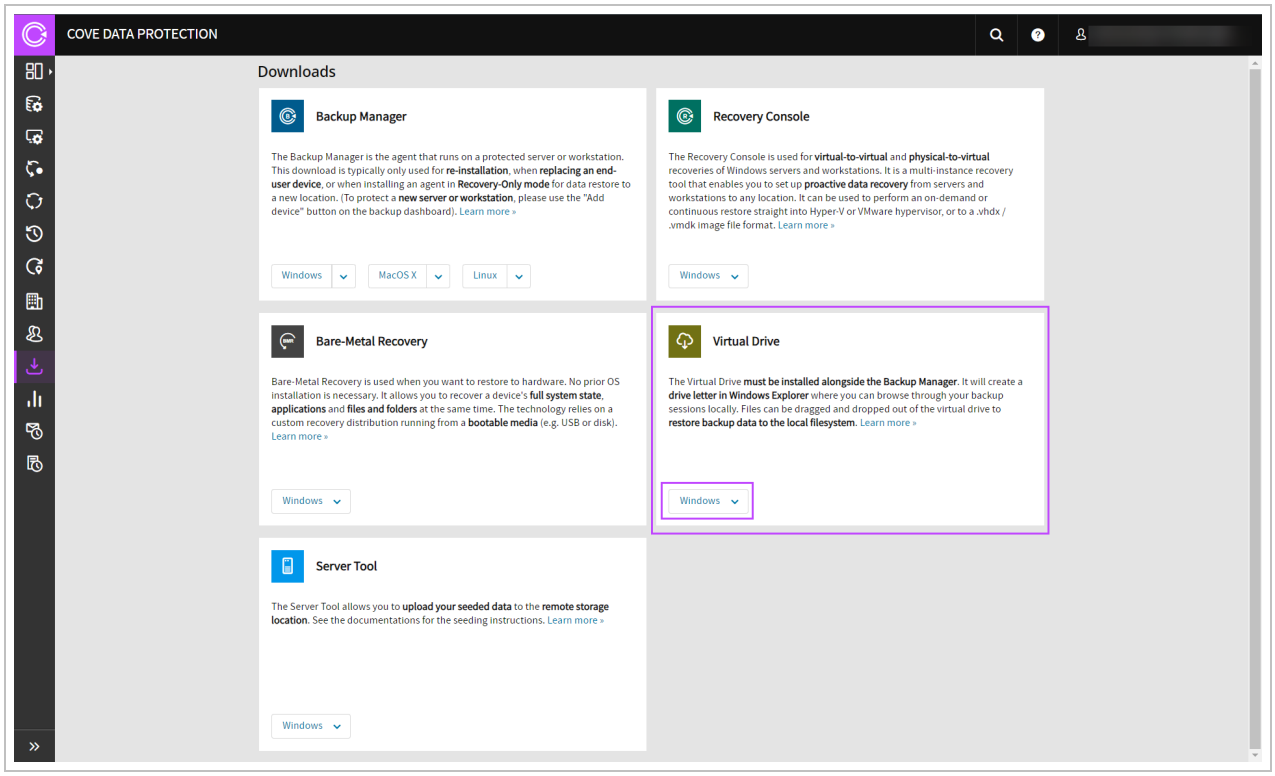


9. Reboot the device

Virtual Drive Installation

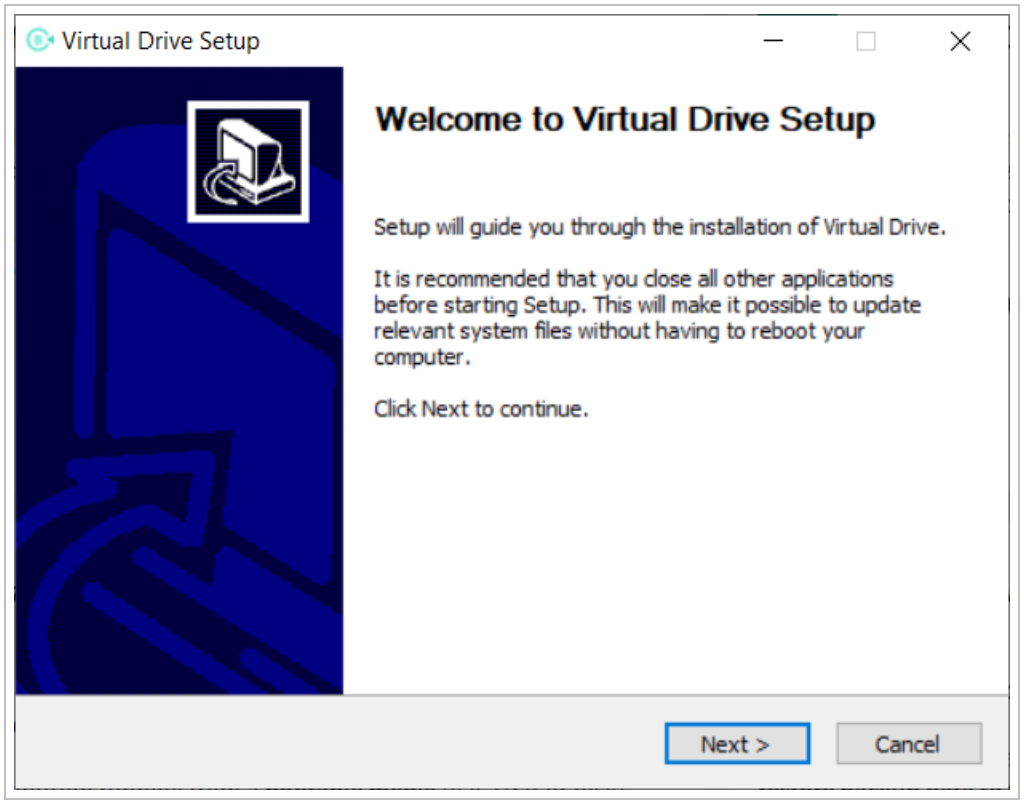
Virtual Drive can be installed through either an install **Wizard** or via **command-line installation**.

Before beginning, ensure you have downloaded the appropriate version of the Virtual Drive for your machine. This can be found from the Downloads page in Management Console, or from the Backup Downloads page on our website.

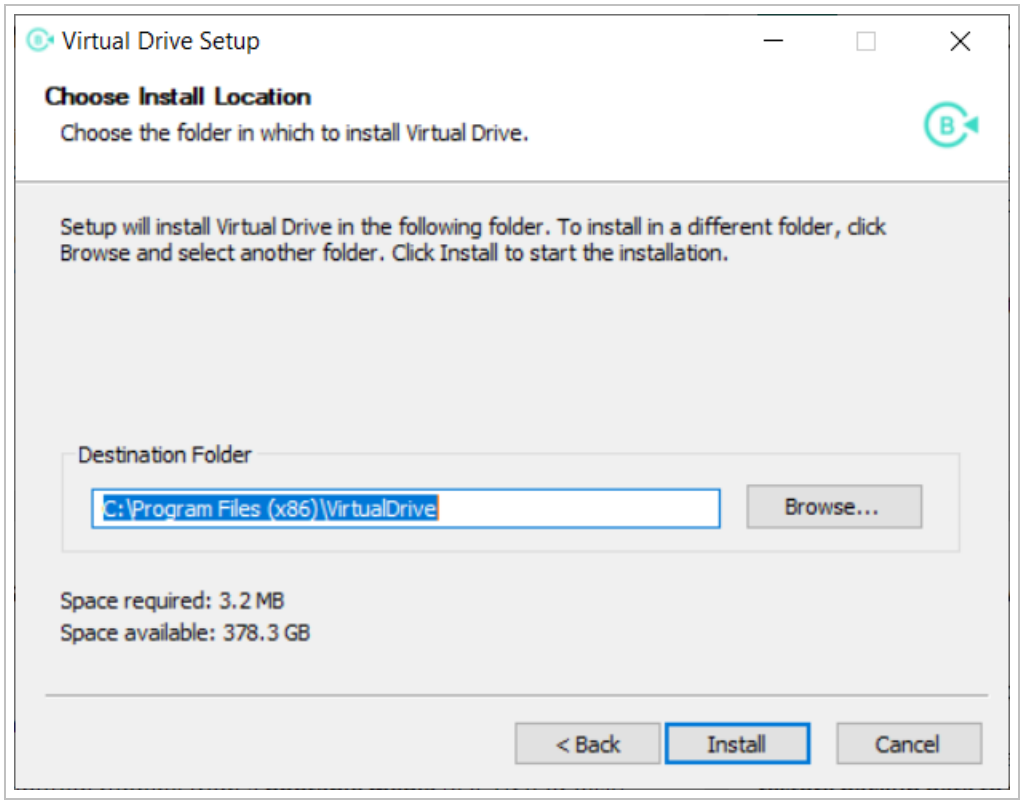

COVE DATA PROTECTION
Downloads
Backup Manager
The Backup Manager is the agent that runs on a protected server or workstation. This download is typically only used for re-installation, when replacing an end-user device, or when installing an agent in Recovery-Only mode for data restore to a new location. (To protect a new server or workstation, please use the "Add device" button on the backup dashboard). Learn more »
Windows
MacOS X
Linux
Recovery Console
The Recovery Console is used for virtual-to-virtual and physical-to-virtual recoveries of Windows servers and workstations. It is a multi-instance recovery tool that enables you to set up proactive data recovery from servers and workstations to any location. It can be used to perform an on-demand or continuous restore straight into Hyper-V or VMware hypervisor, or to a .vhdx / .vmdk image file format. Learn more »
Windows
Bare-Metal Recovery
Bare-Metal Recovery is used when you want to restore to hardware. No prior OS installation is necessary. It allows you to recover a device's full system state, applications and files and folders at the same time. The technology relies on a custom recovery distribution running from a bootable media (e.g. USB or disk). Learn more »
Windows
Virtual Drive
The Virtual Drive must be installed alongside the Backup Manager. It will create a drive letter in Windows Explorer where you can browse through your backup sessions locally. Files can be dragged and dropped out of the virtual drive to restore backup data to the local filesystem. Learn more »
Windows
Server Tool
The Server Tool allows you to upload your seeded data to the remote storage location. See the documentations for the seeding instructions. Learn more »
Windows

Installation Wizard

1. Double click the downloaded file to run the install wizard
2. Click Next to begin setup

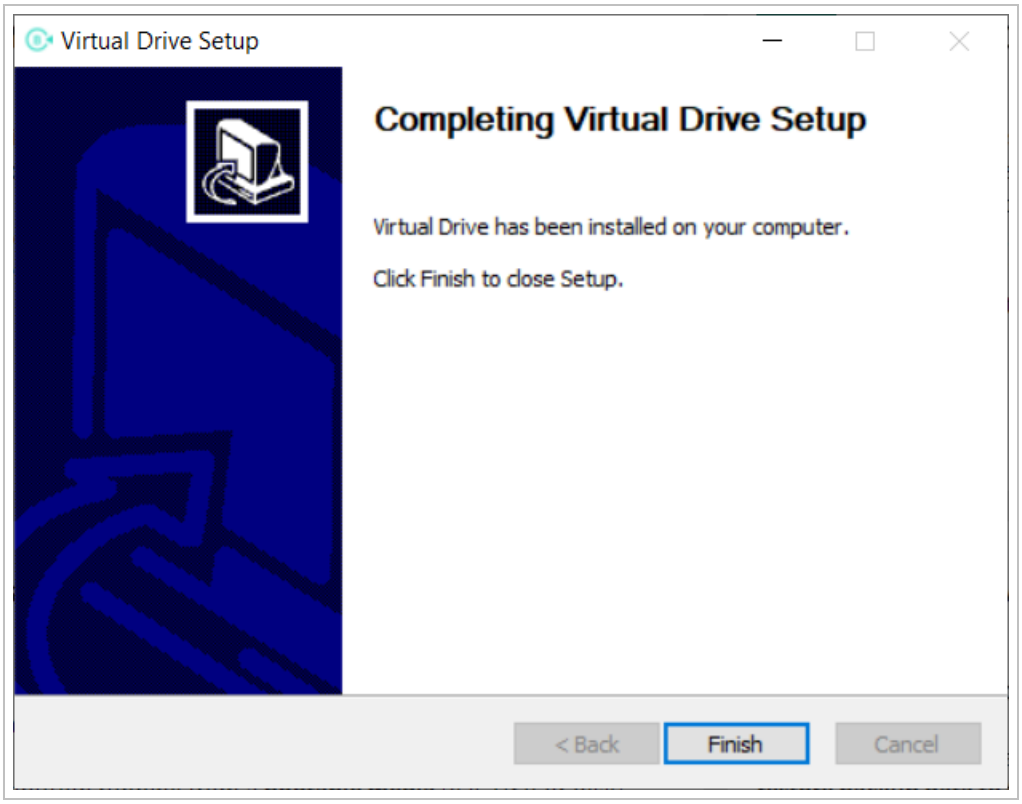


3. Use the **Browse** function to allocate an appropriate destination folder for the installation



4. Allow the installation to run

5. Click **Finish** to complete the installation and close the wizard



Command-Line Installation

To use the silent installation mode:

1. Start *cmd.exe* as an Administrator on the device
2. Run the following command:

```
mxb-vd-windows-x64.exe /S /D=C:\Program Files\VD
```

Parameters

The command is broken down into the following parameters:

- `mxb-vd-windows-x64.exe`/`mxb-vd-windows-x86.exe` - This is the name of the installation file downloaded prior, ensure you are using the correct filename
- `/S` - This stands for the silent installation mode
- `/D` - This is the indicator to a directory

> This must be immediately followed by the directory path where you want to install the Virtual Drive

> This parameter must be the **last** parameter on the command line and *must not* contain quotes, even if the path contains spaces.

- `-InitialVirtualDriveLetter` (optional) -This (if used) must be placed **before** the directory parameter and lets you **customize the letter** the Virtual Drive is mounted to during installation, for example:

```
-InitialVirtualDriveLetter Q
```

> ✗ If this parameter is used **after** the path, installation will **not** be completed.

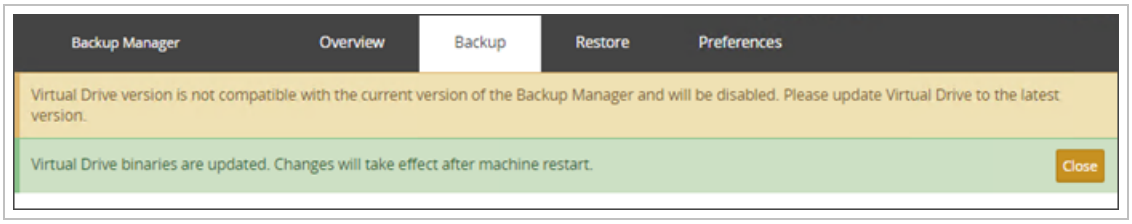
Post Installation

When the installation is completed, a new **local** drive appears in the system, along with the regular "C:", "D:", and "E:" (DVD) drives.

> The drive letter usually used by Virtual Drive is "`B:`" unless this letter is already taken.

You can specify any other letter using the `InitialVirtualDriveLetter` parameter in the configuration file as detailed in Example.

After the Virtual Drive has been installed, it will be **automatically updated** with each Backup Manager update.

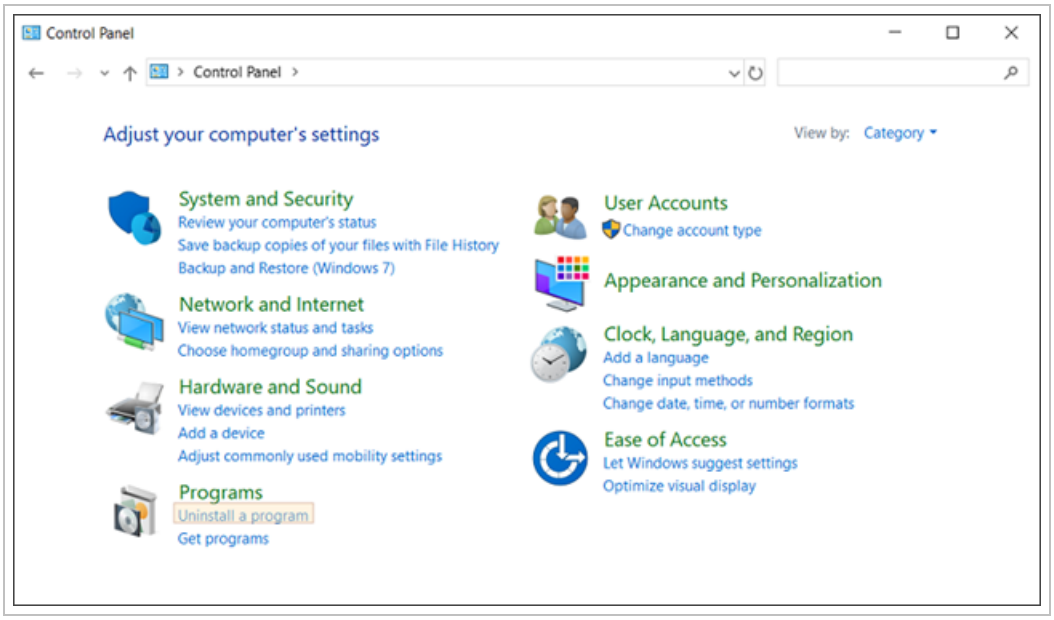


> If you make changes within the data on the Virtual Drive, these changes will not be reflected in the data kept on the cloud.

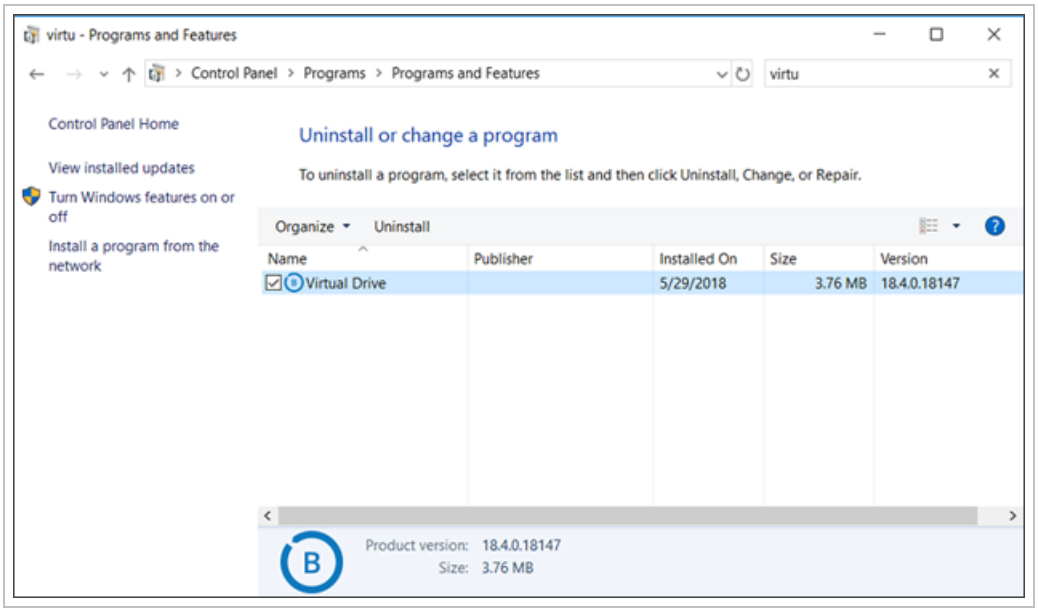
Uninstalling Virtual Drive

Use the Control Panel to uninstall the Virtual Drive.

1. Go to **Programs > Uninstall a program**



2. Select **Virtual Drive** and click **Uninstall**

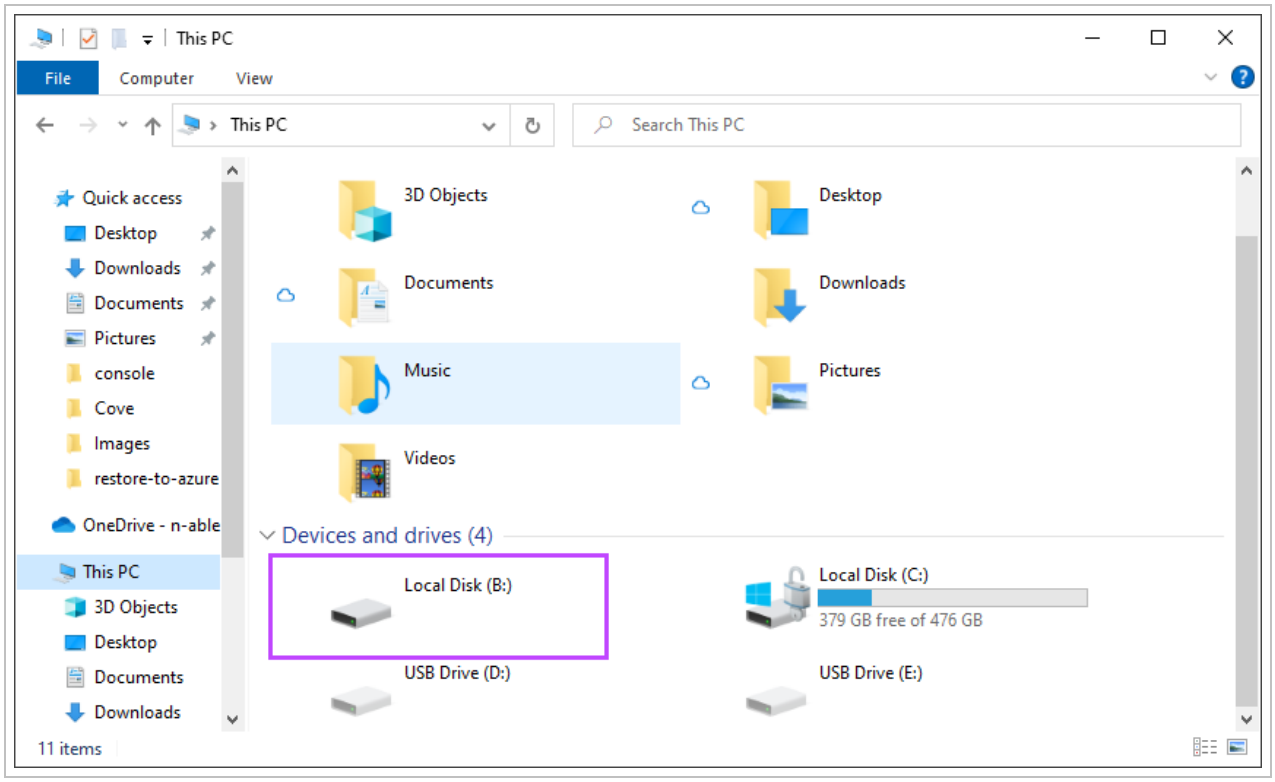


Virtual Drive Recovery

The N-able Virtual Drive tool creates a drive letter on the devices Windows Explorer, where you can browse through your previous backup sessions locally.

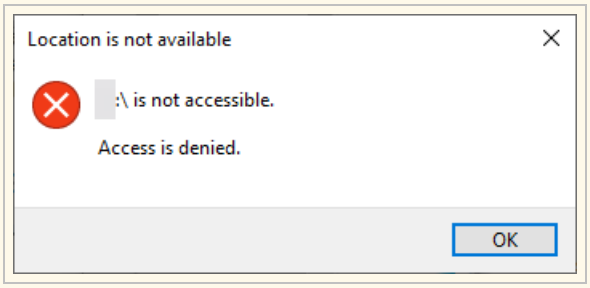
Files and Folders can be dragged and dropped out of Virtual Drive to restore backup data to the local filesystem on a file-by-file bases.

1. Open your Windows Explorer
2. Navigate to **This PC** > **Devices and Drives**



3. Open the Virtual Drive letter

> The drive letter usually used by Virtual Drive is `B:` unless this letter was already taken, or you have specified a different letter during installation, or by changing the settings in the config.ini file

> If you see the following error, ensure the user is a part of the appropriate permissions group by following the Users and Groups Permissions:
>
> 
>

4. Browse through the backed up data sources then through the backup session date and time to find the files or folders you wish to restore
5. Copy the required data and paste into a different location outside of the Virtual Drive, for example into a **Recovered Data** folder stored on the machine's desktop, or as a copy to it's original location

Virtual Drive Settings

The Virtual Drive is usually used with predefined settings. If needed, advanced users can change them through the configuration file *(config.ini).*

1. Open the *config.ini* file, which can be found at:

   ```
   C:/Program Files/Backup Manager/config.ini
   ```

2. Add the `[VirtualDrive]` section (if it is not there yet)
3. Populate the section with the parameters you want to configure as shown in the example below
4. Restart the internal backup process to apply the new settings (view instructions)

Example

```
[VirtualDrive]
ShowAllSessions=1
VirtualDriveRestoreCacheType=memory
```

Settings that can be turned on and off

The settings listed below are disabled by default (set to `=0`). To enable any of them, change `0` to `1`.

- `ShowLatestAvailableFiles` - gives you access to files that were removed or excluded from the backup selection
- `ShowAllSessions` - gives you access to failed backup sessions (on condition that some valid data got successfully backed up)
- `ExtendedVirtualDriveLogging` - starts extended logging. The logs are written down to the application log. Keep in mind that the logs can take up a considerable amount of disk space

The following setting is enabled by default (set to `=1`):

- `VirtualDriveRestoreCacheEnabled` - starts Virtual Drive caching to speed up viewing and copying large data sets

Settings that can be adjusted

- `VirtualDriveRestoreCacheType` - defines a storage type for Virtual Drive cache. Supported values: `memory` (default) and `FS`. When `VirtualDriveRestoreCacheType` is set to `memory`, the cache files are kept in the **operation memory** (it helps improve performance). When `VirtualDriveRestoreCacheType` is set to `FS`, the cache is saved to the **file system** (your hard disk). This can lower overall performance but lets you allocate more space for the cache
- `VirtualDriveRestoreCacheLocation` - defines a directory that the cache is written to (if `VirtualDriveRestoreCacheType` is set to `FS`). By default, the value is set to your temporary folder. You can change it to another location, for example: `C:\virtual-drive\vd-restore-cache`

  > Network Shares cannot be used for the cache location, only local paths can be used.

> If the cache folder becomes too large, you can clear the contents without issue.

- `VirtualDriveRestoreCacheSizeLimitInMb` - defines the maximum memory or disk size (set to `256` MB by default)
- `InitialVirtualDriveLetter` - the drive letter the Virtual Drive must use (instead of the default "B:" drive). In case the specified letter is taken, the Virtual Drive will search for the next available letter in the alphabet. For example, if `InitialVirtualDriveLetter=M`, the Virtual Drive is mounted to the "M:" drive. If this is not possible, it will try "N" and so on

Configuration File

When you install the Backup Manager, a special **configuration file** is created in its installation folder *(config.ini)*. Advanced users can find it convenient to change some basic settings through this file and also to access advanced settings.

- Config.ini location
- Required settings for Backup configuration file

Updating configuration file

You can update the Backup Manager configuration file in the following way:

1. Stop the internal backup processes and service on the machine
2. Open a text editor on the device as an Administrator
3. Open the *config.ini* file found in the Backup Manager installation folder (see the table below for the exact file path on each operating system)
4. Edit the settings as needed
5. Save the changes
6. Close the file
7. Start the internal backup processes and service on the machine. This is necessary to apply the new settings

Config.ini location

The location of the *config.ini* file depends on your operating system:

Operating system	File path
Windows	`C:/Program Files/Backup Manager/config.ini`
macOS	`/Library/Application Support/MXB/Backup Manager/config.ini`
GNU/Linux	`/opt/MXB/etc/config.ini`

Required settings for Backup configuration file

By default, the Backup Manager configuration file *(config.ini)* contains 3 **sections**. Each of the sections has a set of **parameters** required by the Backup Manager.

If you remove any of these parameters, they will be automatically reset to the default values when the internal processes associated with the Backup Manager are restarted. If some critical installation details happen to be missing, you will be offered to repeat the installation when attempting to start Backup Manager.

```
[General]
InstallationId=372da5d2fa048be724831
User=5D609D865BEDD460D8C0F9606AD691
Password=1F8E90E89BC4745FB836A5B1FC184
ManagementBasedConfiguration=1
EncryptionKey=459D688G3JK6B0DX891PA4

[HttpServer]
HttpServerPort=5000

[Versioning]
AccountHomeFolderVersion=1
BackupAcceleratorVersion=1
LocalSpeedVaultVersion=1
LocalSpeedVaultVersionValidityMarkerVersion=1
TableFieldRangeCheckerVersion=1
PostAllClientSettingsToServiceVersion=1
```

When this file is edited, it is important the parameters stay in their original sections.

The table below lists frequently used optional parameters:

Section	Parameter	Definition	Supported values
`[General]`	`InstallationId`	A unique identifier automatically assigned to the current Backup Manager installation.	Text
`[General]`	`User`	The **device name** that was used during the installation (issued through the Console).	Text
`[General]`	`Password`	The **password** that was used during the installation (issued through the Console).	Text
`[General]`	`EncryptionKey`	The **security code/encryption key** set during the Backup Manager installation. It is not possible to re-install the and recover data without this key.	Text[1] Supported length - from 6 to 50 symbols.

[1]For security purposes, the displayed values are encrypted. If you enter another value, it will also be encrypted after the Backup FP is restarted.

Section	Parameter	Definition	Supported values
`[HttpServer]`	`HttpServerPort`	The number of the port through which the Backup Manager connects to the network.	Number - usually 5000. If port 5000 is unavailable, the Backup Manager tries 5001, 5002 and up.

Logging

Backup Manager automatically details its operations to a logging file, called an **application log** or **Backup FP** log. This file contains non-personal data that lets system administrators and support engineers make sure all backup and recovery processes are set up correctly and are running smoothly. If something goes wrong, the log files are a valuable asset for troubleshooting.

Versions of the application log

There are two versions of the application log: a local version and a server version. The local version is available on the hard drive of the device where the Backup Manager is installed. The server version is stored in the Cloud and can be accessed from the Backup Manager by appending the URL.

How to view the application log (local and server versions)

The local version is able to display more data while the server version displays the **latest records** only.

For detail, see the **Application log settings** section below.

Application log structure

Each log record is structured in the following way:

```
[timestamp] [type] [thread_id] [module]: message
```

> The `[module]` component is optional and may not always be shown

An example log entry may look as follows:

```
[2015-01-14 10:30:22.083339] [D] [07200] [Periodic Task Thread]: "Profiler
controller" is being executed...
```

Where:

- `[2015-01-14 10:30:22.083339]` is the [timestamp]
- `[D]` is the [type]
- `[07200]` is the [thread_id]
- `[Periodic Task Thread]` is the [module]
- `"Profiler controller" is being executed...` is the message

Application log settings

As the size of each log file on the hard drive reaches 5 MB, the Backup Manager stops adding new entries to it and **creates a new file** instead. The files are saved to the same folder. If debug logging is on, the size limit is extended to 50 MB.

Generally, after the total size of **all application log files** on the user's computer reaches 50 MB (or 500 MB in case of debug logging), the oldest of them are cleared to free space for new files. These settings have proven to be comfortable for most users. However, sometimes (for example, when a tricky case is investigated), it may be necessary to customize the predefined size limits. This is done by adding parameters to the `[Logging]` section of the configuration file.

For information on different log types see:

- View application log
- Enable debug logs
- Enable protocol logs

> For additional Logging parameters, see the Additional Logging parameters section of the Enable debug logs page.

View application log

There are two versions of the application log: a local version and a server version. The local version is available on the hard drive of the device where the Backup Manager is installed. The server version is stored in the Cloud and can be accessed from the Backup Manager by appending the URL.

View the logs on the hard drive

The log file is saved as a local version on the hard drive where Backup Manager is installed.

The location depends on the operating system:

- **Windows**: `C:\ProgramData\MXB\Backup Manager\logs\BackupFP`
- **macOS**: `/Library/Logs/MXB/Backup Manager/BackupFP`
- **GNU/Linux**: `/opt/MXB/var/log/BackupFP`

View the server version in Backup Manager

1. Launch the Backup Manager for the device
2. Once the Backup Manager is open in a browser, add `/logs/app` to the URL and browse there
3. The **application logs**(also referred to as "BackupFP logs") or **debug logs** (if debug logging is enabled) will open in the window

> You can find the records you need by scrolling or using page search `(Ctrl+F)`.

Filter application logs

Backup Manager application log entries can be **filtered** by appending parameters to the URL. Most of the parameters coincide with the log components. The `[timestamp]` component can be filtered using several parameters.

See View application log for ways to view the application logs.

Supported parameters

Parameter	Definition	Type	Corresponding component in log structure
`time.year`	The year when the record was created	Numeric	`[timestamp]`
`time.month`	The month when the record was created	Numeric	
`time.day`	The date when the record was created	Numeric	
`time.hour`	The hour at which the record was created	Numeric	
`time.minute`	The minute at which the record was created	Numeric	
`time.second`	The second at which the record was created	Numeric	
`type`	The type of log: ▪ `E` - error ▪ `W` - warning ▪ `L` - informational logging ▪ `D` - debug	String	`[type]`
`thread_id`	The thread ID of a record	String	`[thread_id]`
`module`	The name of the module the log record is related to	String	`[module]`
`message`	An explanatory message	String	`[message]`

Supported filters

Filters for string parameters:

- `eq` - "equals"
- `ne` - "does not equal"
- `cn` or no parameter - "contains" (default)
- `nc` - "does not contain"
- `sw` - "starts with"
- `ew` - "ends with"

Filters for numeric parameters:

- `eq` or no parameter - "equals" (default)
- `ne` - "does not equal"

- `gr` - "greater than"
- `le` - "less than"

Syntax to use

A filter is formatted in the following way:

```
parameter=[condition]value
```

`[condition]` can be omitted. In this case a default value will be used: `cn` for string parameters or `eq` for numeric ones.

You can create several filters for the **same parameter**. For example:

`127.0.0.1:4001/logs/app?time.hour=gr16&time.hour=le18` (show records created between 16 o'clock and 18 o'clock)

Here are some examples.

URL string	What it means
`127.0.0.1:4001/logs/app?time.year=2015`	Show log records created in 2015
`127.0.0.1:4001/logs/app?time.day=16&time.hour=gr13&time.hour=le16&module=BackupShell&message=ncTag`	Show log records matching the following conditions: ▪ created on the 16th between 13 and 16 o'clock ▪ belong to the module which name contains "BackupShell" ▪ have a message that does not contain the "Tag" substring

Enable debug logs

Debug logs are logs with an extended logging level. They can be helpful to support engineers when the application logs are insufficient to investigate an issue. Debug logs can be enabled for both Backup Manager and Recovery Console. For steps on enabling debug logs for Recovery Console, see the Advanced settings in Recovery Console page.

Here is how to enable debug logs:

1. Stop the Backup Service Controller. See Restarting the internal backup processes and service for details
2. Open the Backup Manager **configuration file** (where to find configuration file)
3. Add a new section with the following content to the configuration file:

   ```
   [Logging]
   LoggingLevel=Debug
   ```

4. Start the backup process
5. Try to reproduce the issue
6. Compress the "logs" folder and send it to the support team

The location of the "logs" folder depends on your operating system, you can find the logs for Backup Manager here:

- Windows: `C:\ProgramData\MXB\Backup Manager\logs`
- GNU/Linux: `/opt/MXB/var/log`
- macOS: `/Library/Logs/MXB/Backup Manager/logs`

Please do not forget to disable debug logging when the issue is resolved. It will save your disk space.

1. Open the configuration file and delete `LoggingLevel=Debug` section from it
2. Restart the backup process

Additional Logging parameters

Section	Parameter	Definition	Supported values
`[Logging]`	`LoggingLevel`	The level of logging information you require the device to take	▪ `0` - debug ▪ `1` - warning ▪ `2` - error ▪ `3` - log (This is the default)
`[Logging]`	`[LogsLocation]`	This parameter allows you to change the location of the log files. Debug logs are normally stored in the following locations: ▪ Windows: `C:\ProgramData\MXB\Backup Manager\logs` ▪ GNU/Linux: `/opt/MXB/var/log` ▪ macOS: `/Library/Logs/MXB/Backup Manager/logs`	`desired file path`
`[Logging]`	`SingleLogMaxSizeInMb`	The maximum size of a single application log file on a user's hard drive (in MB)	Any whole number. Default values: ▪ `5` (when debug logging is disabled) ▪ `50` (when debug logging is enabled)

Section	Parameter	Definition	Supported values
`[Logging]`	`TotalLogsMaxSizeInMb`	The maximum size of all application log files on a user's hard drive (in MB)	Any whole number. Default values: ▪ `50` (when debug logging is disabled) ▪ `500` (when debug logging is enabled)

Enable protocol logs

Protocol logs help support engineers and system administrators investigate miscellaneous network issues.

Protocol logs must be enabled at least **15 minutes** before they are sent for investigation to the support department.

To enable protocol logging, stop Backup Manager functional process and create the **BackupFP.Protocol** folder in the Backup Manager **logs** folder.

- Windows: `C:\ProgramData\MXB\Backup Manager\logs`
- macOS: `/Library/Logs/MXB/Backup Manager/`
- GNU/Linux: `/opt/MXB/var/log`

When done, start the Backup Manager functional process (this is necessary to apply the new settings).

When you get all necessary details, you can disable protocol logging:

1. Stop the Backup Service Controller. See Restarting the internal backup processes and service for details
2. Remove the **BackupFP.Protocol** folder
3. Start the Backup Service Controller again

Restarting the internal backup processes and service

To apply advanced settings, you often need to restart the Backup FP (the internal process associated with Backup Manager).

The service will not restart itself if stopped, so will need to be manually restarted. However, it will start up as normal after a device reboot as long as it has not been disabled.

Windows instructions

Here is how to restart the Backup FP on Windows:

1. Open the Start menu
2. Start the Services Console by typing `Services` into the search menu, or `services.msc` in the **Run** program

3. Scroll until you find the **Backup Service Controller** service
4. Right-click and choose **Restart**

> You may also stop and start the service as needed by following the above instructions, but selecting **Stop** or **Start** in step 4

Linux instructions

On Linux, start a terminal emulator and run the following command:

```
/etc/init.d/ProcessController restart
```

> You may also stop and start the service as needed by using the `stop` and `start` commands individually

macOS instructions

On macOS, start the Terminal and run the following commands:

```
sudo launchctl unload -w /Library/LaunchDaemons/com.cloudbackup.BackupFP.plist
sudo launchctl load -w /Library/LaunchDaemons/com.cloudbackup.BackupFP.plist
```

> You may stop and start the service as needed by using the `unload` and `load` commands individually

FAQs

Under each subcategory, you will see some of the most commonly asked questions about each.

- General
- Installation & Setup
- Backup
- Restore

General

How much do services cost and how do I contact my sales representative?

We do not detail any costs within the documentation, please visit the Contact Us page for detailed contact information.

How do I submit a feature request?

You can submit feature requests and vote for them on the N-able Ideas page.

How do I cancel my account?

Please contact your sales representative.

Who do I speak to about paying a past due invoice?

For a single current invoice, contact the sales (they can take payments over the phone). For multiple or past due invoices, call the finance department (919 957 5099, option 3 for accounts).

How do I inherit another Partners backup clients?

This must be handled by our sales team as they will need to get permission from both Partners and the reseller before making any changes. Sales can be contacted at:

- 1-919-957-5099 (US/CAN)
- +44 (0) 1382 309040 (EMEA)
- +61 (0) 8 7123 4060 (APAC)

How to I set up automatic payment of bills?

Auto-pay details are now managed in the Community Resource Center profile. Please access your profile at https://community.n-able.com.

Please send any questions you might have to sw-msp-cloudbilling@n-able.com.

Where can I find update and release notes?

All update and release notes are available at https://status.n-able.com/cove/ where you can sign up to receive email notifications when anything is posted.

How do I move from a Trial account to Production in Management Console?

1. Log in to the Trial account as a SuperUser
2. Accept the End User License Agreement (EULA) if you have not done so already
3. At the top of your screen, select **Request Upgrade**

A member of our Sales team will then move your account from Trial to Production.

If a device is deleted, can it be put back onto the Management Console?

No.

Devices are removed together with **all data** that has been backed up for them. There is no way to restore a device or its data after the device has been deleted from the system.

Installation & Setup

How do I update the Backup Manager to the latest version?

Instructions on updating the Backup Manager to the latest version, with details per data source can be found here: Update Backup Manager

> All devices using Backup Manager version 16.11 and higher will automatically update when newer versions are released.

What are the best practices for the Backup Manager setup?

We do not have any best practices, as your usage of the product is all based on you and your customers' needs. If we recommend a specific setup as a best practice for one customer, it may not fit the needs of another. However, if you would like some assistance to resolve any issues or queries, contact our support team.

How many times can I try to guess my security code/encryption key?

There is no limit on the number of times you can guess this. If you cannot remember it and the device is still accessible, you can Convert devices to passphrase-based encryption.

Can I install the Backup Manager on multiple machines using the same device credentials?

Yes, you can. There can be **one Quick Installation** and any number of additional installations in the restore-only mode.

Can I rename a device or change the password/installation keyfor a device?

No. Unfortunately, device names and passwords/installation keys cannot be changed.

Can I merge data from several backup devices?

Unfortunately, there is no such feature.

How can I test my encryption key?

You can test this by downloading and installing the Recovery Console and adding the device to this. Adding successfully means the devices encryption key is valid.

Is there a minimum recommended upload speed for Backup?

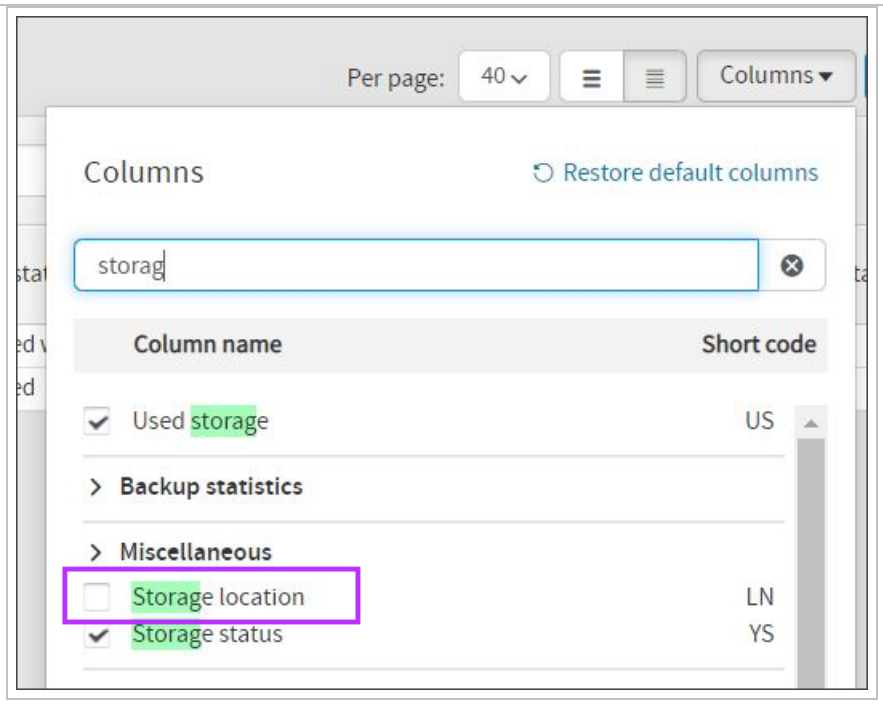
We do not have a minimum recommended upload speed but it must be more than capable of pushing the average amount of data changed daily.

We would suggest that you determine the average daily changes and then check the bandwidth is appropriate.

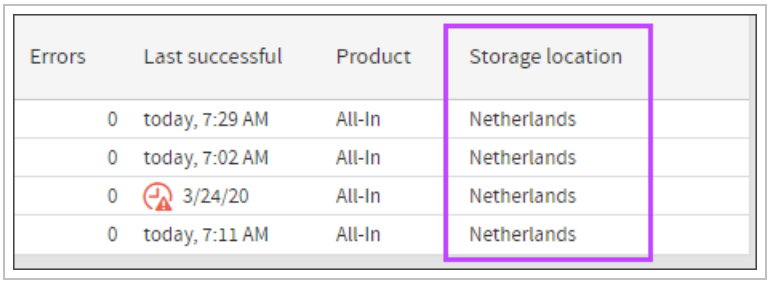
How do I find out the storage location of my backups?

The storage location can be found by adding the **Storage Location** column on the Management Console's devices page:

1. Log in to Backup Manager
2. Expand the **Columns** dropdown to the right of the page
3. Search for '**Storage Location**' and ensure this is ticked



4. Close this and check the location on your list of devices



Can I change the email address that sends the email notifications and automated reports?

Yes, this can be changed in the **Customize branding** section of the Customer Management edit customer dialog box.

Can I move a device to a different customer?

Yes, but any assigned products and profiles will have to exist at a parent level so that they will still be available at the destination customer.

If the products or profiles exist at the end-customer level, they must be removed from the device first, then recreated at the new customer level and assigned to the device once it has been moved.

Backup

Are files checked for viruses before or during backup?

No, they are not.

Cove Data Protection is not an Antivirus software and has no capability to scan files during backups or restores.

If I erase a bunch of files today, when will the size of used storage decrease?

The storage size will not decrease until the files are outside of your retention.

If you use the default retention of 28 days, then the file size will decrease on the 29th day. The retention period can be set by creating a custom Product, by configuring the **Retention per data source** fields in product settings.

Why is "Selected size" on a device larger than "Used storage"?

The **Selected Size** is the combined total of all data being backed up **before** it has been encrypted and compressed.

The **Used Storage** is the backup size **after** the data has been encrypted and compressed.

Can I seed multiple devices to the same drive?

Yes. One drive can be used for multiple devices at the same time. It will auto-generate a directory for each device's seed data.

Can I transfer backup data from another product?

No. You will need to restore the data from the other backup product and back up that location.

Can I back up files with "temp" in the name?

Yes, you can. Some predefined filters apply though.

Can I schedule multiple backups per day?

Yes, you can. See Enabling backups in Backup Manager for instructions.

Does the Backup Manager make use of VSS?

Yes. The Backup Manager uses VSS Writers supplied by the operating system, as well as Volume Shadow Copy to create a virtual copy of your files before a backup begins. Volume Shadow Copy allows for backing up files that are open or not in use. Files can be backed up in a consistent state, even if they are open. After the backup has completed, the virtual copy is removed and the original file stays intact.

During the backup, where are the snapshots held until the backup is complete?

They are held in your temp directory: `C:\Windows\Temp`.

How can I see the retention for my devices?

The retention period is handled by the product applied to the device. Please check the product applied by going to Product management in Management Console. If no product is applied, the default retention is 28 days and 3 file versions.

Will the backup run if there is no access to the node or internet but the device does have a LocalSpeedVault configured?

The backup will begin for the first scheduled backup but will get stuck in 'Uploading Backup Register' and will fail. Subsequent backups will not start.

Can I create a local only backup?

We do not offer a local only backup option. A LocalSpeedVault is available to work in conjunction with cloud storage but not as a replacement for it.

What are the service names for Backup Manager?

- **Windows**: Backup Service Controller
- **Linux**: Process Controller
- **Mac**: BackupFP

How can I see the status of the LocalSpeedVault on the Management Console?

You can add the 'LSV Status' column on dashboard by selecting it from the *Columns* dropdown > *Miscellaneous*.

How long will a backup or restore take?

Backup and Recovery time will depend on local environmental factors and the devices ability to upload, download and process data (list is not exhaustive):

- Processor Speed
- Available RAM
- Local bandwidth
- Disk write speed

Upload and download speed can be estimated using online calculators.
Factor in additional time for decryption and decompression of data.

What are the backup statuses and what do they mean?

Whenever a backup session is attempted either by a schedule or by starting manually, the Management Console and Backup Manager GUI will provide a status to advise.

Status	Meaning
Failed	The session has failed due to some errors encountered during backup.
Aborted	The session was manually canceled.
Interrupted	The session was interrupted while it was processing. This could be because the backup service was stopped or another program has caused a conflict.

Status	Meaning
Not Started	The session was not started. Could be due to the device having a bandwidth limitation interval, but a backup is scheduled to begin within this time-frame.
Blocked	The session was blocked from running for some reason.
Over Quota	The device has gone over the allocated storage space, check the product applied to the device.
Completed With Errors	The session has completed but has encountered some problems during backup. The backup may be incomplete.
Restarted	The session has been restarted because the backup service has been restarted or the device might have been rebooted during the backup process.
Completed	The session has completed with no errors.
In Process	The session is not yet finished running.
In Process with Faults	The session is not yet finished running, but has encountered some problems during backup. The backup may be incomplete.
No backups	There is no backup history for the device i.e. it is a new device.
No Selection	There are no data sources configured for the device.

How often does the Management Console update device information?

The Management Console will update:

- After a restart of the Backup Service Controller service
- Every 15 minutes if an active backup is taking place
- Every 8 hours if no active backup is taking place

Can backups be infected if a device has a virus?

The files will be backed up as they are on the device.

Any files backed up *before* the device is infected will be fine, but all files backed up *after* it was infected will be affected.

Are Sage databases supported for backup?

Backup Manager does not support Sage Database backups. To backup these databases you will need to create a dump of the databases and backup this dump via the **Files and Folders** data source.

Is it possible to backup NSS volumes containing metadata?

Backup Manager cannot see NSS filesystem volumes.

What are differencing disks and why are they created during Hyper-V backups?

Differencing disks or AVHD(x) files are files containing the changes in data between the current backed up data set and the new one.

These files are created when you make a snapshot of a running machine. When the device is powered down, the AVHD(x) and VHD(x) files will merge.

What encryption methods are supported by Cove Data Protection (Cove) Backups?

Cove supports AES-256 for encrypting the user data during a backup.

AES-256 is a more secure but slower version of the AES-128 method which is not supported. Encryption is done at the client side (Workstation/Server) and all pieces of data are sent and stored fully encrypted.

What are the Event ID's and their meanings that the Backup Manager writes to the application Event Logs on Windows?

Event ID's are listed below in the following format 'ID - Description':

- 10 - BackupFP started
- 51 - Backup Started
- 52 - Restore Started
- 101 - In Progress
- 102 - Failed
- 103 - Aborted
- 105 - Completed
- 106 - Interrupted
- 107 - Not Started
- 108 - Completed With Errors
- 109 - In Progress With Faults
- 110 - Over Quota
- 111 - NoSelection
- 112 - Restarted

Can you stop the cleaning process?

There is no way to avoid the cleaning process. Once the process has started, it cannot be stopped.

Do consistency checks run automatically or will I have to do this manually?

Consistency checking is automatically done on the back-end periodically.
It is only recommended to run consistency checks manually if remote or local storage is not synchronizing and the restore sessions show (L) [local only].

If data is not changed but moved to a new location on the same device, will this be backed up again?

Data is not sent again, as deduplication is done on the client side (workstation/server), and so will not reflect in the transferred size or in the used storage.

We simply detect that the file has changed and write those changes in the backup registry.

Can I change the location of the temporary files directory for Backup Manager?

The location of the Temporary Files Directory can be changed on the Preference Tab of the Backup Manager:

1. Launch the Backup Manager
2. Select **Preference** tab
3. Select **Advanced**
4. In the field that displays **Save temporary files to**: type desired directory path

Can I backup an external USB drive or stick with Cove?

Drives that are marked as removable media by the operating system will not be detected for backup. The software will only detect USB drives that are mounted as fixed drives.

What does the blue arrow mean in Files and Folders data selection?

The blue arrow indicates that the directory is not local on the device.

Can you filter for all files created or modified on a certain day?

The Backup Manager cannot filter any backup sessions based on a files modified time.

How can I prevent the device from backing up?

1. Remove the schedule from the accounts Preferences tab on the Backup Manager GUI
2. Modify the expiration date box on the Management Console
    a. Click on the device in the Management Console to open the Device Properties window
    b. Select the **Settings** tab
    c. Un-check the **No Expiration** box in the expiration date section and change the date as needed
    d. Save the changes before closing the properties window

Will Backups continue if a physical server is virtualized?

Yes, backups can continue after a physical device has been virtualized.

Why can't I see TimeMachine's backup data in Backup Manager?

Backup Manager will not see TimeMachine files as this is displayed as removable media which cannot be backed up at this time.

Why can I see several devices when clicking on Launch Backup Client?

Additional devices show under the option to **Launch Backup Client** when the account is added to a restore only platform. These devices will remain in the list until they do not check in for 7 days.

Can I speed my backup up?

You can increase the number of simultaneous connections made during a backup by allowing more of your computers resources to be used for the backup. This can be done by implementing the `BackupThreadsCount` parameter within the config.ini file. By default, this is set to 4, but can be changed to any whole number between 1 and 10. Find more information on Config.ini location here.

Can I change the location of my local Storage folder?

You may change the storage location of the local Backup Register[1] by adding the `PathToLocalStorage` parameter to the config.ini file and directing this to the new location.

The default locations are:

- Windows: `C:\ProgramData\MXB\Backup Manager\storage\`
- Linux: `/opt/MXB/var/storage/`
- macOS: `/Library/Application Support/MXB/Backup Manager/storage/`

Find more information on Config.ini location here.

Can I put a backup device into restore-only mode?

Yes. This can be done by using the `ReadOnlyMode` parameter in the config.ini file and setting the value to `=1`. Restore-only mode is useful if you wish to temporarily disable backups on a machine but not uninstall the Backup Manager completely. Changing this back to `=0` will turn the device back to full mode. Find more information on Config.ini location here.

Restore

What is my security code/encryption key?

We do not store the security codes/encryption keys for regular backup devices. If you cannot remember it and the device is still accessible, you can Convert devices to passphrase-based encryption instead.

How do I restore data from a device that is powered off and inaccessible?

Install the device on another computer in the restore-only mode and recover the data from there.

Where is data downloaded from during recovery?

Data is downloaded from the cloud or from the LocalSpeedVault (if it is available and synchronized).

Can I choose where data is restored from (the cloud or LocalSpeedVault)?

During a restore data is automatically downloaded from the LocalSpeedVault to the local device (if the LocalSpeedVault is available and synchronized). This takes place automatically and cannot be reconfigured.

---

[1] A database of backup meta data that is formed and stored on a backup device and regularly uploaded to the cloud.

Can I restore only a specific file extension?

Yes. Specific file extensions can be restored from manual selection.

Will permissions carry over when a file is restored?

Files will retain their original permissions when restored to the original location.

Is it possible to restore to XenServer?

It is not possible to restore directly to XenServer but doing a virtual disaster recovery to VMWare VMDK will provide you with the appropriate files which can then be imported to XenServer.

Please see their documentation here: https://support.citrix.com/article/CTX140423 .

Can you backup and restore to Amazon AWS using Cove?

- You can backup a system on AWS by installing Backup Manager directly on the Virtual Machine.
- To restore the system, you will need to:
  - Spin up a new instance in AWS with the same operating system version, service pack and updates as the original device
  - Download the Backup Manager onto the device and install it in Restore-Only mode using the same device name, installation key, and encryption key as the original device
  - Restore data from the restore tab of Backup Manager

How can I speed up a restore?

The restore can be sped up by increasing the threads count for the Recovery Console:

1. Quit the Recovery Console
2. Terminate the BackupFP.exe and RecoveryConsole.exe processes from task manager
3. Navigate to **C:\Program Files\RecoveryConsole\config.ini**
4. In the [General] section, add the following:

   ```
   RestoreDownloadThreadsCount=#
   ```

   Where # can be a whole number value fro 1-50, the default is 10.

How can I clear the log entries shown in the Recovery Console?

To clear the log entries, you will need to remove the device then re-add it to the Recovery Console:

1. Remove or rename the device folder in **C:\Program Files\MXB or Managed Online Backup\Backup Manager\Storage\<device name>**
2. Remove the device from the Recovery Console
   a. Select the device in the Recovery Console
   b. Click **Remove**

3. End all Recovery Console processes within Task Manager
    a. Right-click on the task bar and select Task Manager
    b. Right-click on any task labeled 'Recovery Console' and select end-task
4. Re-add the device to the Recovery Console
    a. Click the **Add** button on Recovery Console
    b. Enter the devices credentials

Can I move my Recovery Console to a different device?

It is possible to install Recovery Console on numerous devices at once, so when moving it from one machine to another, you will follow the regular install process on the new device then uninstall from the old device. As such, you will need to add all the devices to the Recovery Console again on the new machine.

Is it possible to restore data if the initial backup has not completed?

It is not possible to restore data if the initial backup has not completed. The device will show no restore sessions in the Backup Manager GUI.

Can I put a backup device into restore-only mode?

Yes. This can be done by using the `ReadOnlyMode` parameter in the config.ini file and setting the value to `=1`. Restore-only mode is useful if you wish to temporarily disable backups on a machine but not uninstall the Backup Manager completely. Changing this back to `=0` will turn the device back to full mode.

Find more information on Config.ini location here.

Glossary of Cove Data Protection (Cove) terms

Recovery

There are several methods of recovering data from your Backup devices: using the Backup Manager Client; from the Management Console using Recovery Testing, One-Time Restore to Hyper-V or Azure, or Standby Image to Hyper-V or Azure; via the Recovery Console to process specific data recovery; using Virtual Disaster Recovery or continuous restore; using our independent Bare Metal Recovery; or Virtual Disaster Recovery tools.

Your decisions when deploying Cove Data Protection (Cove) should be guided by your recovery requirements. And Cove offers multiple different ways to perform recoveries. The best practices guide is intended to help you choose among the options at both deployment and recovery time.

What's inside:

Continuity In Management Console

Management Console contains different continuity services that can be used for disaster recovery:

- One-Time Restores - Cove has two separate methods of recovering data on an on-demand basis:
  - To Hyper-V - This service runs to restore data to a Hyper-V or Local VHDX as configured in Add Recovery Locations
  - To Azure - This service runs to restore data to an Azure Virtual Machine as configured in Azure Recovery Locations
- Standby Image - Cove has three separate methods of running a continuous restore of your data:
  - Standby Image to Hyper-V - This service runs a continuous restore of a device to a Hyper-V or Local VHDX as configured in Add Recovery Locations
  - Standby Image to ESXi - This service runs a continuous restore of your data to ESXi
  - Standby Image to Azure - This service runs a continuous restore of your data to Microsoft Azure and boots based on the frequency set during configuration of the plan
- Recovery Testing - This service runs and provides a screenshot as proof that the device is recoverable

Benefit

With these tools, we provide proof of recoverability and the ability to failover in case of a disaster.

Requirements

The following requirements must be met:

- The following **must** be backed up:
  1. The full System State of the device
  2. The whole system disk – `C:\` or another disk that has your operating system and that the OS boots from (the **Files and Folders** data source)
- For setup, you must be logged into the Backup console as a **SuperUser** or **Manager**

  > To manage devices and recovery locations, any other user role will suffice.

- You are required to enter the devices encryption key/security code, however, in cases where the device has been installed using Quick Installation of the Backup Manager you will be required to provide the passphrase instead

Operating System

Recovery Testing and Standby Images are available on **Windows** operating systems only (servers and workstations):

- Windows 8 / 8.1
- Windows 10
- Windows 11
- Windows Server 2012 / 2012 R2 (limited[1])
- Windows Server 2016 (limited[2])
- Windows Server 2019 (limited[3])
- Windows Server 2022 (limited[4])

> Recovery Testing and Standby Image only support **64-bit** architecture.

One-Time Restores

Cove has two separate methods of recovering data on an on-demand basis:

- To Hyper-V - This service runs to restore data to a Hyper-V or Local VHDX as configured in Add Recovery Locations
- To Azure - This service runs to restore data to an Azure Virtual Machine as configured in Azure Recovery Locations

What's inside:

One-Time Restore to Hyper-V

Cove Data Protection (Cove)'s **One-Time Restore** feature allows you to restore data to Hyper-V or Local VHDX as configured in Add Recovery Locations on an on-demand basis.

> It **is** possible to run one-time restores on devices assigned to either the Recovery Testing or Standby Image plans.

Requirements:

- Backup Manager version 17.4 and newer
- Devices and Recovery Locations must belong to the same Customer
- A Cove Data Protection (Cove) SuperUser or Manager account

---

[1]New features such as Docker-based containers, Storage Spaces Direct and Shielded VMs are not.
[2]Only the features compatible with Windows Server 2012 R2 are supported.
[3]Only the features compatible with Windows Server 2012 R2 are supported.
[4]Only the features compatible with Windows Server 2012 R2 are supported.

- Recovery Locations must be added to the Management Console and the Recovery service must be installed on the recovery location **before** one-time restore can occur

> - Recovery Location is an environment where restores will be performed
> - Recovery service is a service which perform restores on that Recovery location

Limitations

- One-Time Restores cannot be used on the RMM integrated version of Backup (Managed Online Backup) or on the N-central integrated version of Backup (Backup and Recovery)
- One-Time Restores are **not** available for devices with disabled 'Virtual disaster recovery' feature in an assigned Product
- 32-bit architecture is not supported
- Due to a Microsoft limitation, Hyper-V **does not** support FAT/FAT32/ExFAT formatted drives. For this reason, please use NTFS formatted drives for Standby Image. More information can be found in the Microsoft Documentation for Hyper-V
- Maximum supported capacity for virtual hard disks is **64 TB** per disk
- Devices can only be assigned to **one** Recovery Location

What is restored?

The following data sources are supported and restored to the Hyper-V recovery location given that they are selected for backup in the Product, or data source selection:

- System State
- Files and Folders
- Exchange
- SharePoint
- MS SQL

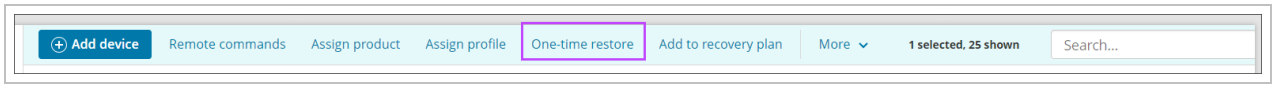
What's inside:

Configure One-Time Restore to Hyper-V

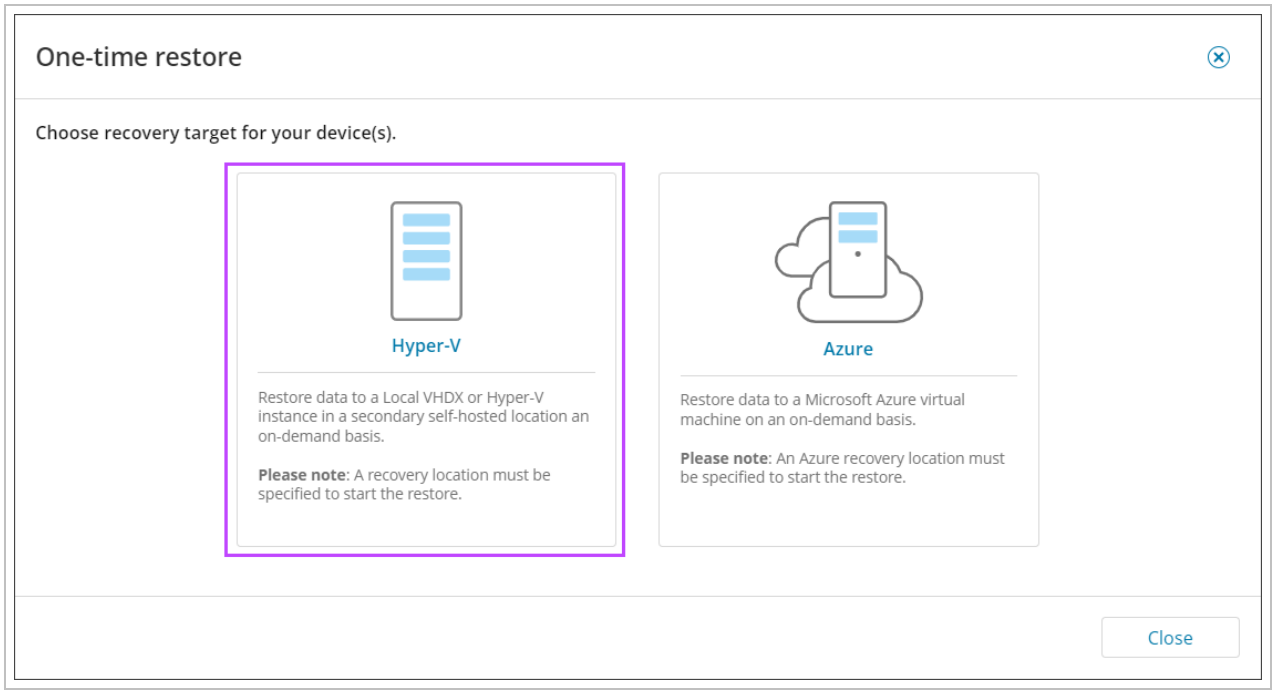
Before starting a One-Time Restore to Hyper-V, ensure you have checked all requirements and limitations, including setting up a Recovery Location.

From Backup Dashboard

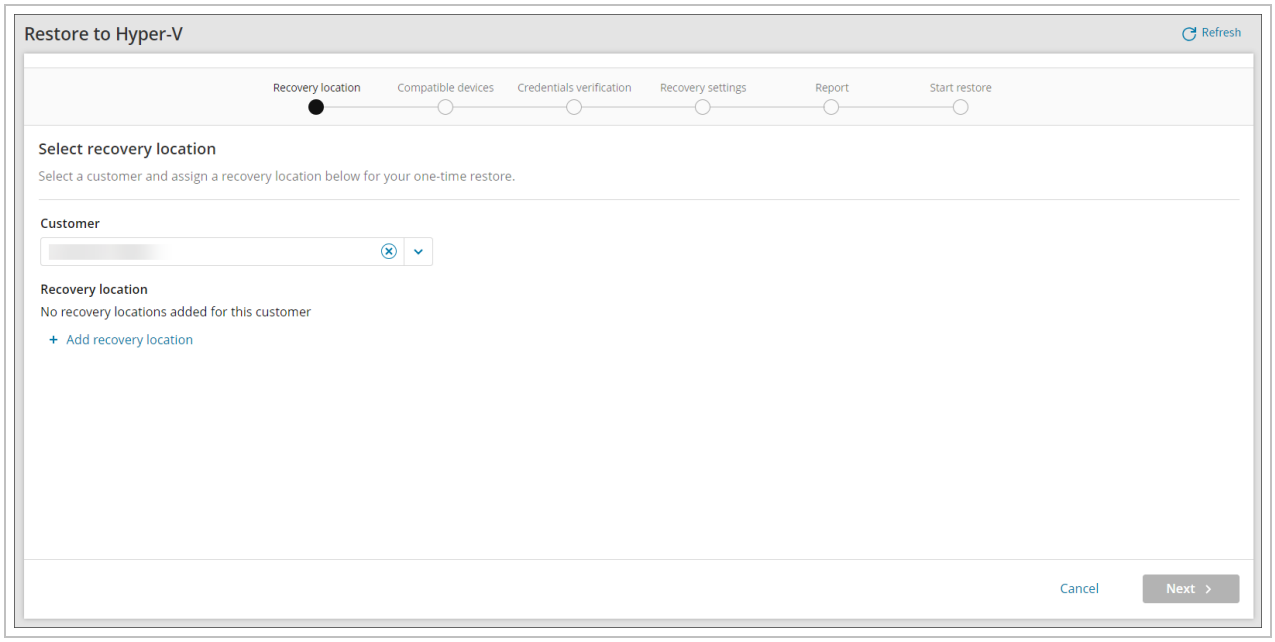
1. Log in to the Management Console under a **SuperUser** account
2. In the Backup Dashboard, tick the checkbox to the left of the device(s) to restore
3. Click **One-Time Restore**



4. Select the **Hyper-V** target

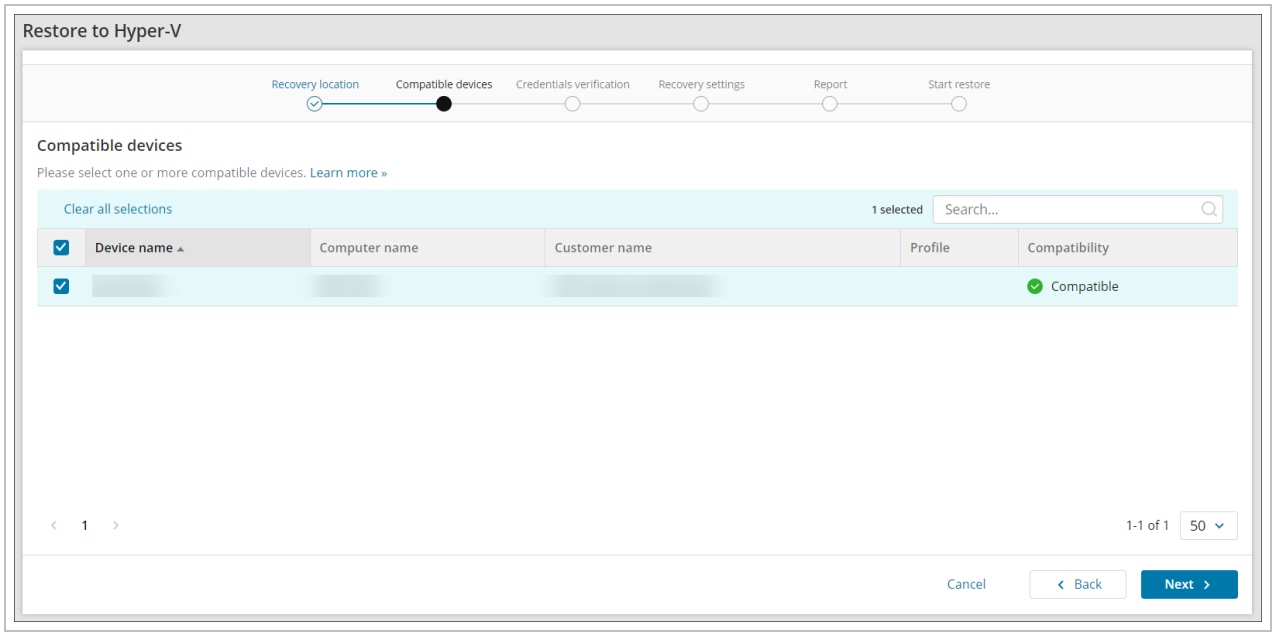


5. Select the Customer
6. Select the Recovery Location for the restore or click **+ Add recovery Location** to follow the steps to create a new Recovery Location



7. Click **Next**

8. Confirm compatibility of device(s) and click **Next**

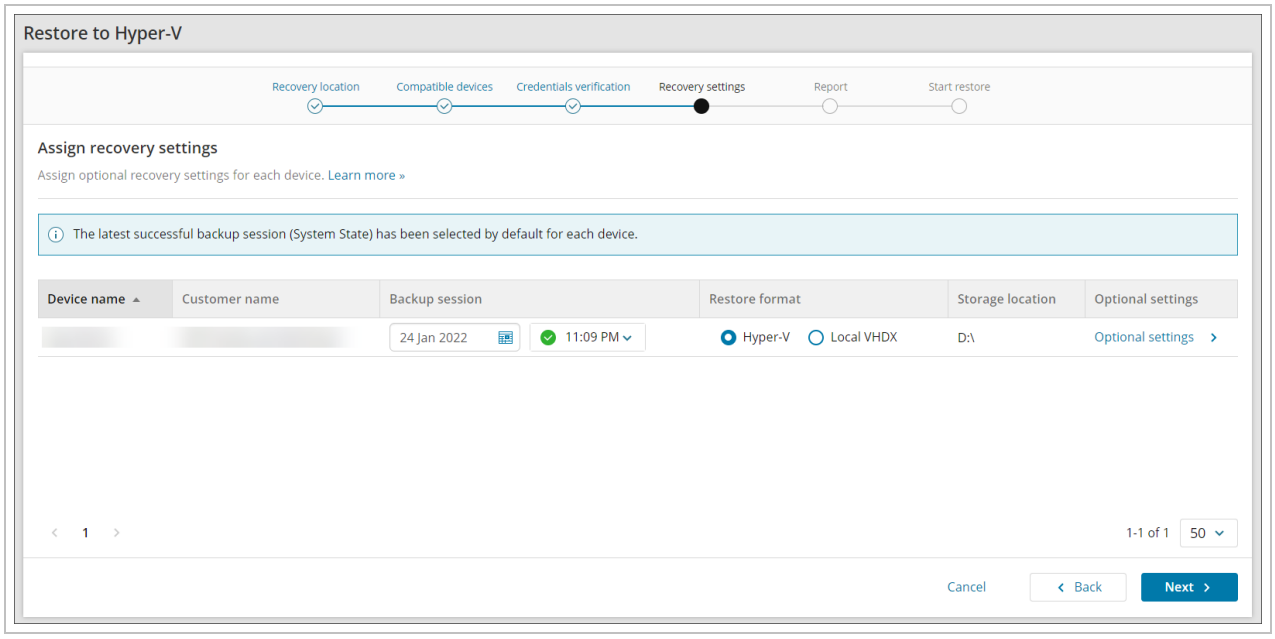


9. Enter the security code/encryption key or passphrase for the device(s). This can be either:
   - **Private encryption key** - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryption
   - **Passphrase encryption** - These are generated on demand for automatically installed devices. You can find information on this here

> If you are logged in as a security officer, this will be detected automatically.

10. Click **Next**

11. Select the date and time of the backup session to restore

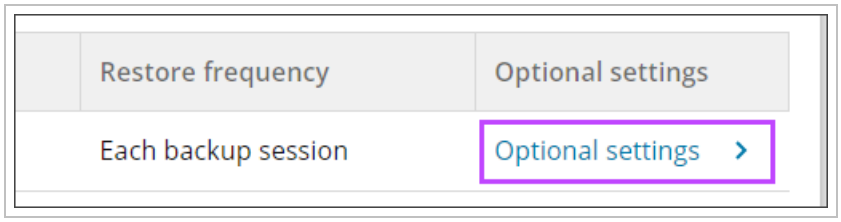


> During this step, **all** available sessions for **all devices** listed will be loaded in the backup session column. **Please allow time for these to load**, if the load of sessions fails, a message stating so will be displayed with a refresh button to try again.

> If the **Backup Target VM** option is enabled for one or more devices, be aware that if the backup agent is still running in backup mode on the source VM, this will lead to corrupted backup data for both the source and target VMs.

12. Choose the restore format:
    - Hyper-V
    - Local VHDX

13. Configure the **Optional Recovery Settings** for the restore format selected by clicking **Optional Settings** to the right of the storage location:



- Hyper-V optional settings:

OPTIONAL RECOVERY SETTINGS

Restore OS disk only

Backup target VM

FRS and DFSR services

Local Speed Vault

CPU cores

4

RAM (GB)

4

Virtual switch

default switch

Enter a virtual switch to enable network settings

VM Subnet mask

255.255.255.0

VM gateway

10.16.10.1

VM DNS server

10.16.10.5.8.8.8.8

Separate multiple DNS servers with a comma or semicolon

VM IP address

10.16.10.24

IP addresses will increment by 1, if applied to all devices

- **Restore OS disk only** - Restoring the OS disk only will speed up restores
- **Backup target VM** - Continuing to backup your target VM will protect the device according to its existing backup schedule
- **FRS and DFRS services** - If you are restoring Active Directory with multiple domain controllers, you should change the FRS and DFSR services to authoritative in the domain controller that will be started in the first place. Avoid marking several FRS/DFSR services as authoritative in the production environment as it can result in data loss. When the feature is on, the FRS and DFSR services are started on the target VM in the authoritative mode. The NETLOGON and SYSVOL shares become available, so the Active Directory and DNS services become functional again

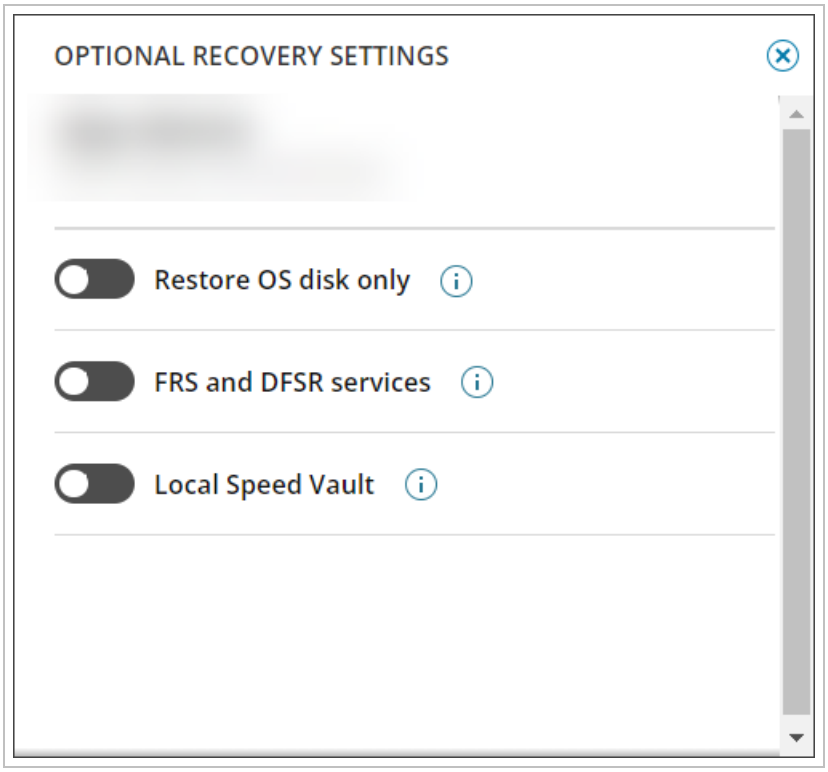
  > More information about FRS/DFSR is available in the Microsoft Knowledge Base. Article IDs: KB2218556 and KB290762

- **LocalSpeedVault** - If a LocalSpeedVault (LSV) is enabled on a backup device, the data is sent to both the LSV and the cloud or private storage location. During a restore, data is automatically downloaded from the LSV first to the local device which makes restore faster. If the LSV is not available or not synchronized, the restore data will be pulled from the cloud or private storage location. This takes place automatically and cannot be reconfigured
- **CPU Cores** - Select the number of CPU Cores to be allocated to the new virtual machine
- **RAM (GB)** - Select the amount of RAM in Gigabites to be allocated to the new virtual machine
- **Virtual switch** – Enter the Hyper-V network adapter that will be used by your new virtual machine
- **VM subnet mask** – Assign a custom subnet mask to the virtual machine
- **VM gateway** – Assign a custom gateway to the virtual machine
- **VM DNS servers** – Assign the list of custom DNS servers (separated by comma), Example:

  ```
  8.8.8.8 or 8.8.8.8,7.7.7.7
  ```

- **VM IP address** – Assign a custom IP address to the virtual machine

- Local VHDX optional settings:



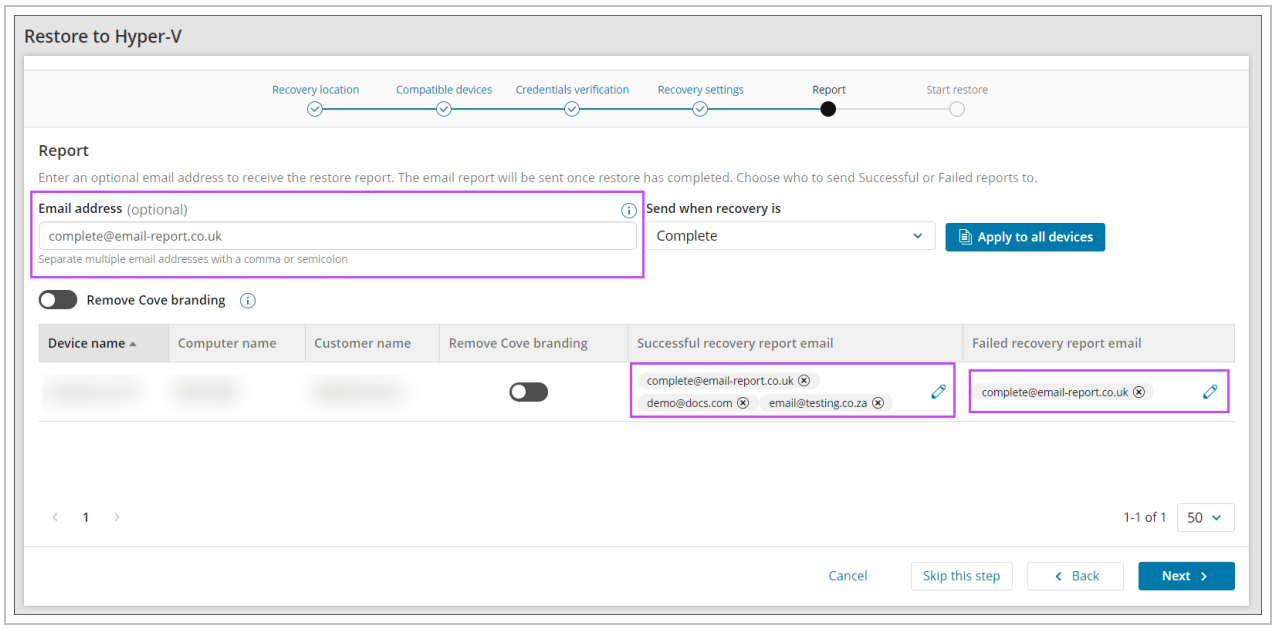
  - **Restore OS disk only** - Restoring the OS disk only will speed up restores
  - **FRS and DFRS services** - If you are restoring Active Directory with multiple domain controllers, you should change the FRS and DFSR services to authoritative in the domain controller that will be started in the first place. Avoid marking several FRS/DFSR services as authoritative in the production environment as it can result in data loss. When the feature is on, the FRS and DFSR services are started on the target VM in the authoritative mode. The NETLOGON and SYSVOL shares become available, so the Active Directory and DNS services become functional again

    > More information about FRS/DFSR is available in the Microsoft Knowledge Base. Article IDs: KB2218556 and KB290762

  - **LocalSpeedVault** - If a LocalSpeedVault (LSV) is enabled on a backup device, the data is sent to both the LSV and the cloud or private storage location. During a restore, data is automatically downloaded from the LSV first to the local device which makes restore faster. If the LSV is not available or not synchronized, the restore data will be pulled from the cloud or private storage location. This takes place automatically and cannot be reconfigured

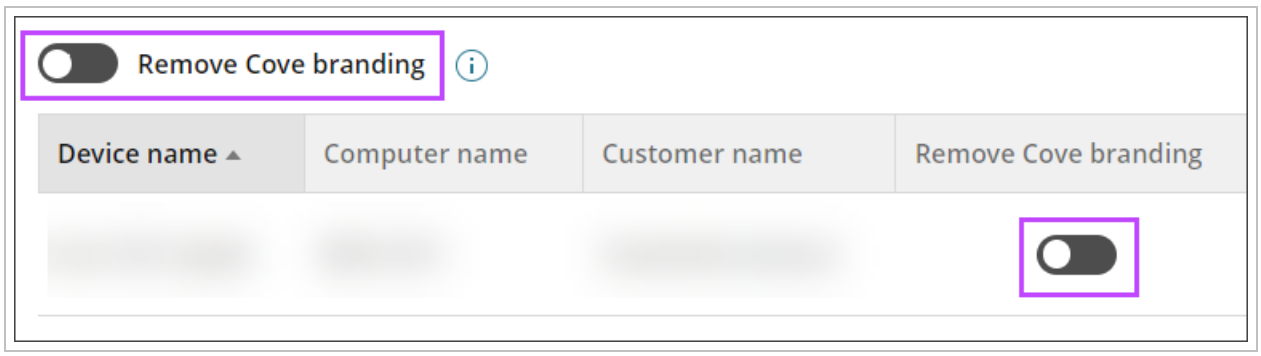
14. Click **Next** to progress to the **Report** window to enter one or more email addresses to receive a report when:
    a. The recovery is complete (Successful or Failed)
    b. The recovery was successful
    c. The recovery failed

> Multiple addresses should be separated using a comma or semi-colon



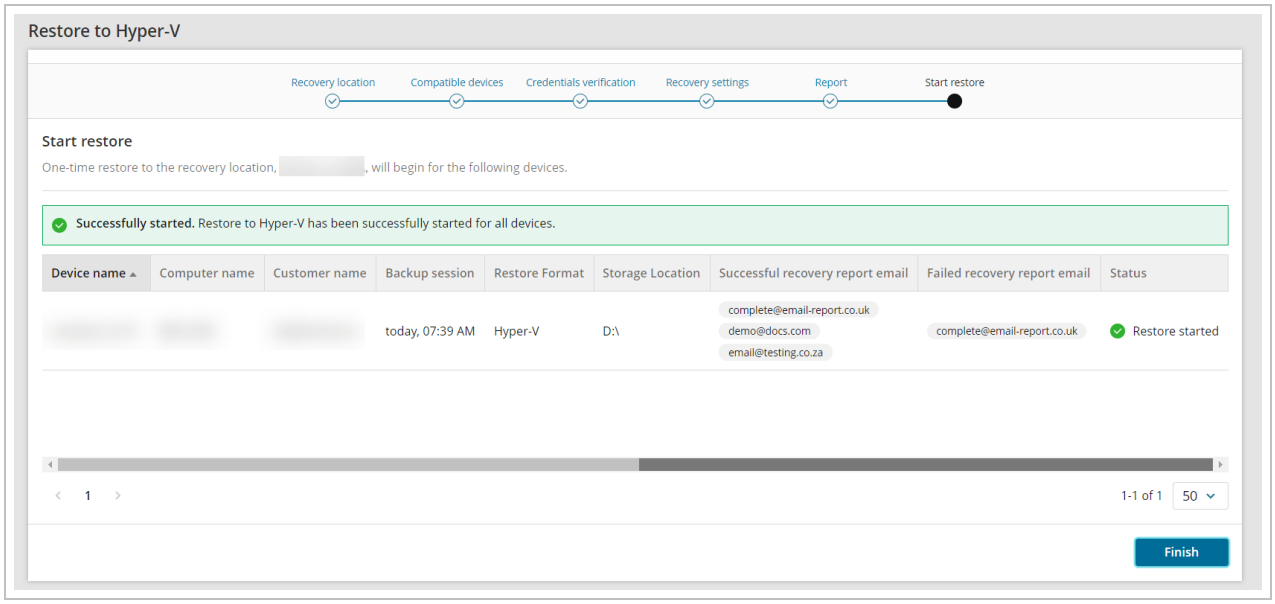
> If you do not want to add an email address to receive reports, click **Skip this step**

15. To remove all branding from the reports, use the **Remove Cove branding** toggle per device, or above the device list to apply the changes to all devices in this window



16. Confirm assigning the plan to the device(s)

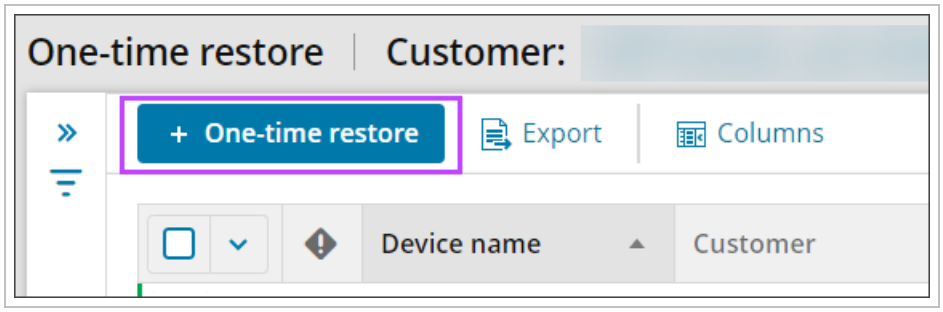
17. Wait for the plan to be assigned until you see a confirmation banner on the page



18. Click **Finish**

From One-Time Restore Overview

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to the **One-Time Restore** overview by selecting **Continuity** > **One-time Restore** from the vertical menu on the left hand side
3. Click **One-time restore** from the top bar



4. The wizard will open to target selection window, follow the above steps from Step #4 onwards

Recovery Reports

When the device(s) assigned to the plan have **Successful recovery report email** or **Failed recovery report email** recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox.

Here is an example report **with** Cove branding:

Cove Data Protection

Recovery completed

On demand restore to Hyper-V

Last recovery session completed successfully: April 05 2023 7:12:10 PM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Restore to Hyper-V dashboard.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Server
Operating system	Windows Server 2019 Standard Server (17763), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 05 2023 7:12:10 PM
Recovery status	Completed
Recovery duration	40 minutes and 58 seconds
Recovery location	

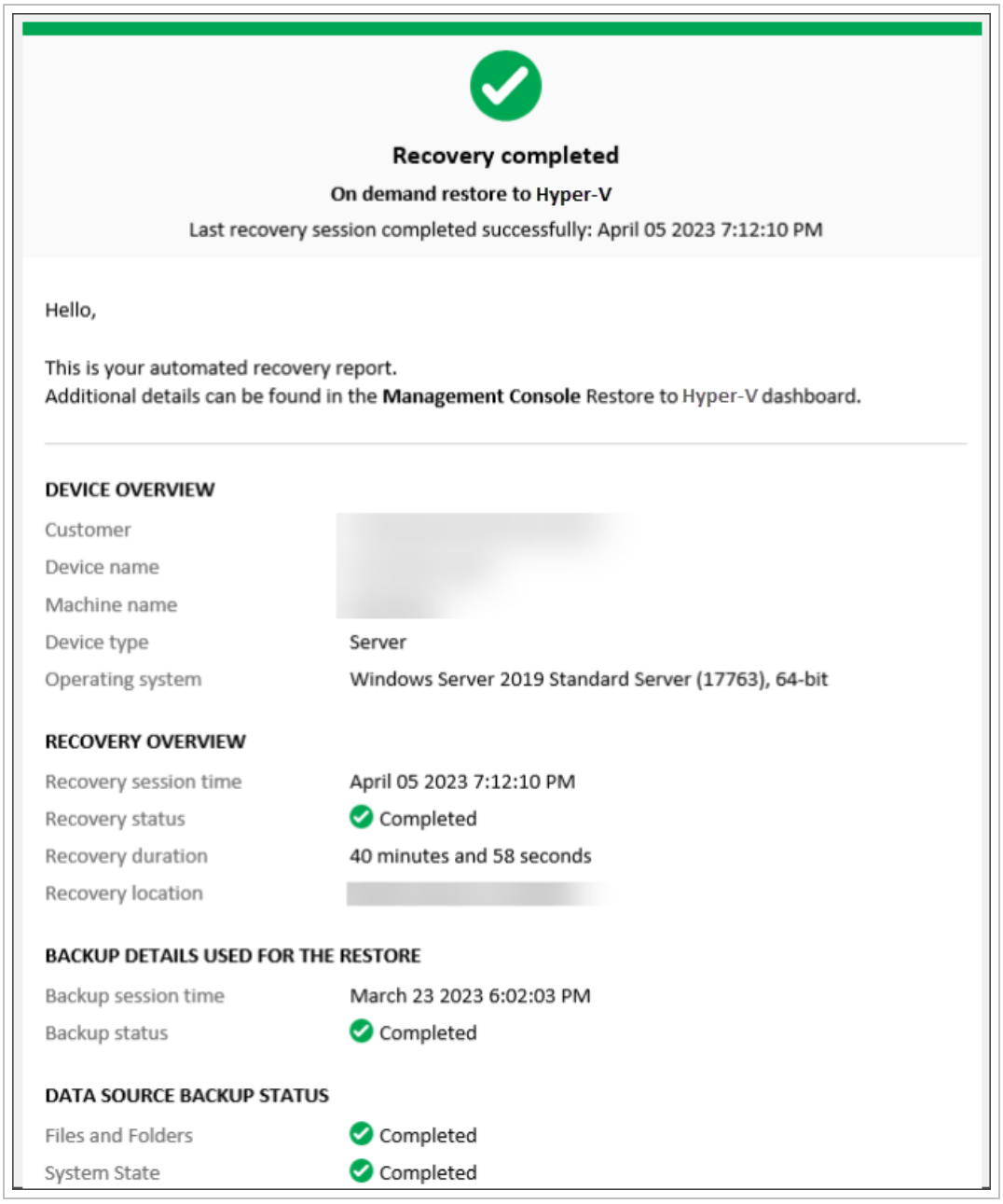
BACKUP DETAILS USED FOR THE RESTORE

Backup session time	March 23 2023 6:02:03 PM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

Here is an example **without** Cove branding:



Recovery completed

On demand restore to Hyper-V

Last recovery session completed successfully: April 05 2023 7:12:10 PM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Restore to Hyper-V dashboard.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Server
Operating system	Windows Server 2019 Standard Server (17763), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 05 2023 7:12:10 PM
Recovery status	Completed
Recovery duration	40 minutes and 58 seconds
Recovery location	

BACKUP DETAILS USED FOR THE RESTORE

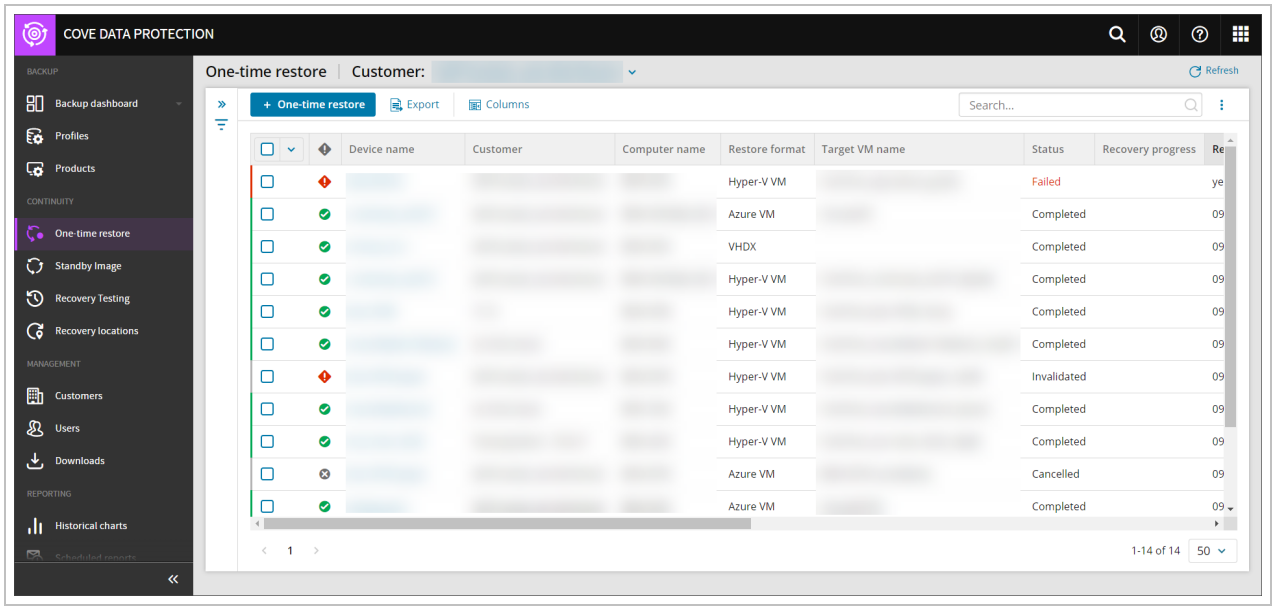
Backup session time	March 23 2023 6:02:03 PM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

Monitor Hyper-V Restore Progress

From the Management Console, you can view the dedicated One-Time Restore overview by selecting **Continuity** > **One-time Restore** from the vertical menu on the left hand side.



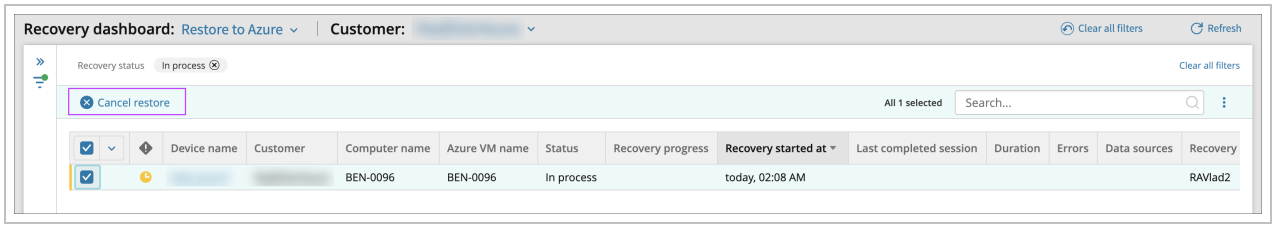
From this dashboard, you will see a specified set of columns detailing information relevant to devices using **One-time Restore**, including the status, restore format and data sources, along with other information relating to Azure and Hyper-V.

If no devices are active, the dashboard will display a message to advise.

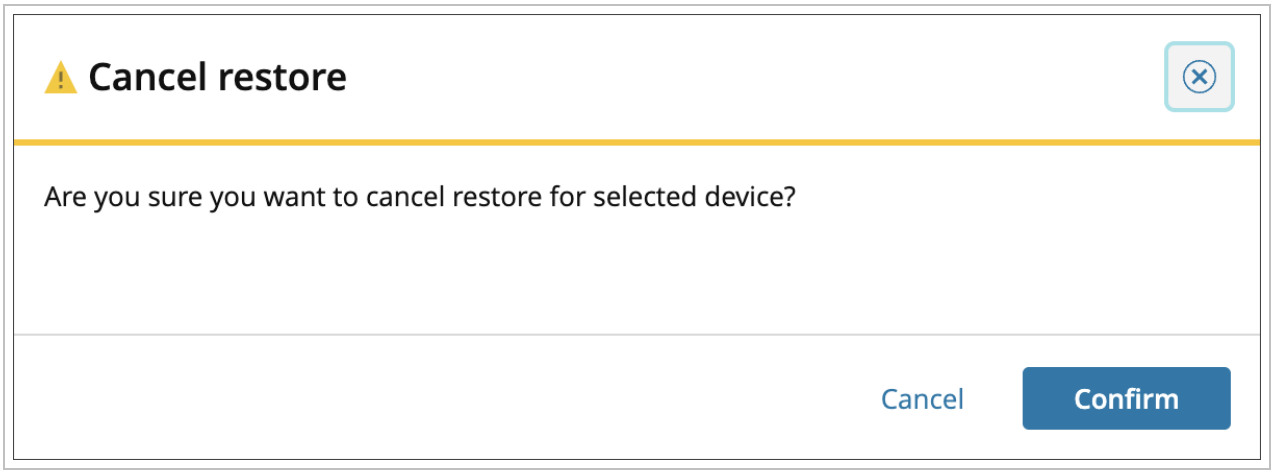
Cancel Restore

From the One-Time Restore overview, it is possible to cancel any recovery currently in progress:

1. Search for or use the filters to find the device in question where the recovery is currently running
2. Select the device
3. Click **Cancel restore** from the top bar



4. Confirm cancellation



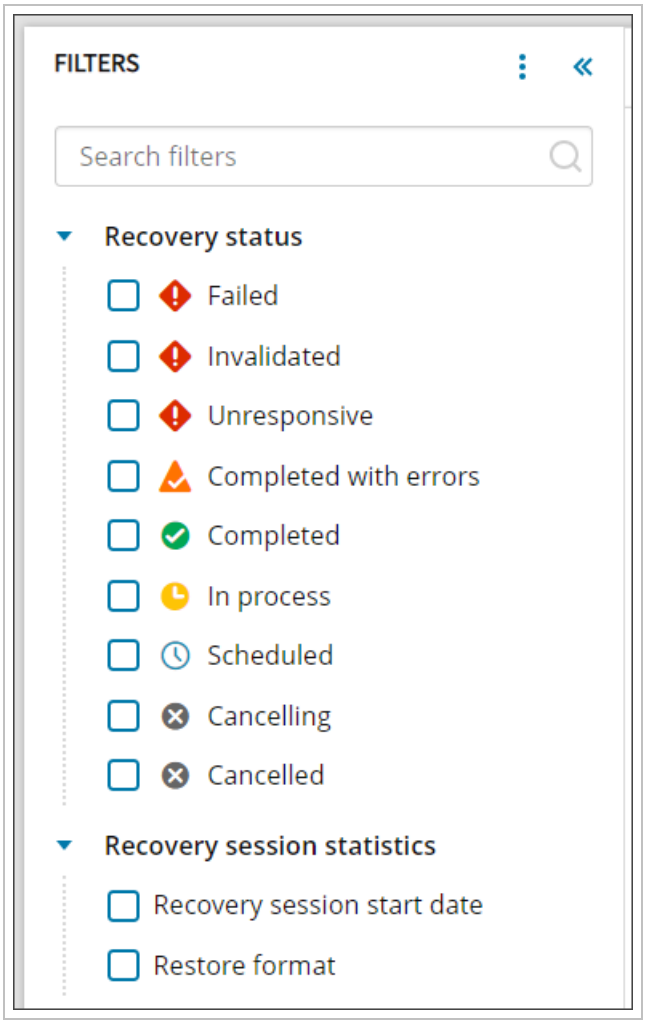
The device will now show in the list with a status of **Cancelled**

Searching

Searching within the One-Time Restore overview can be done by using the search box over to the right hand side of the page, just above the devices list. The search can be performed against any text field.

Filtering

The Standby Image overview also includes functionality to filter devices using the filter menu to the left of the device list and can be displayed or hidden by clicking the double arrows.



From this menu, you can filter by:

Recovery status

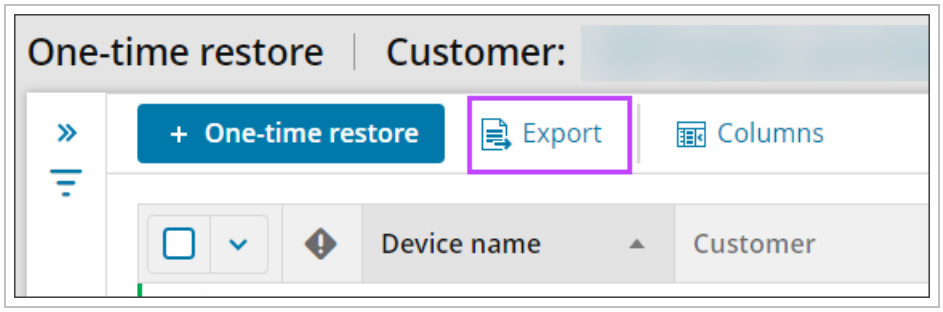
- **Failed** - The recovery session has failed
- **Invalidated** - Device was moved to an inappropriate partner and so the session has failed
- **Unresponsive** - The recovery session was initiated but did not receive updates for at least 30 minutes because the recovery location restarted or was offline.
- **Completed with errors** - The recovery session completed, but encountered errors
- **Completed** - The recovery session completed with no errors
- **In process** - The recovery is currently in progress
- **Scheduled** - Devices just added to a recovery plan and are waiting for their first recovery session or devices where restores were paused and have since been resumed will display as scheduled
- **Cancelling** - The recovery is in process of aborting
- **Cancelled** - The recovery has been cancelled

Recovery Session Statistics

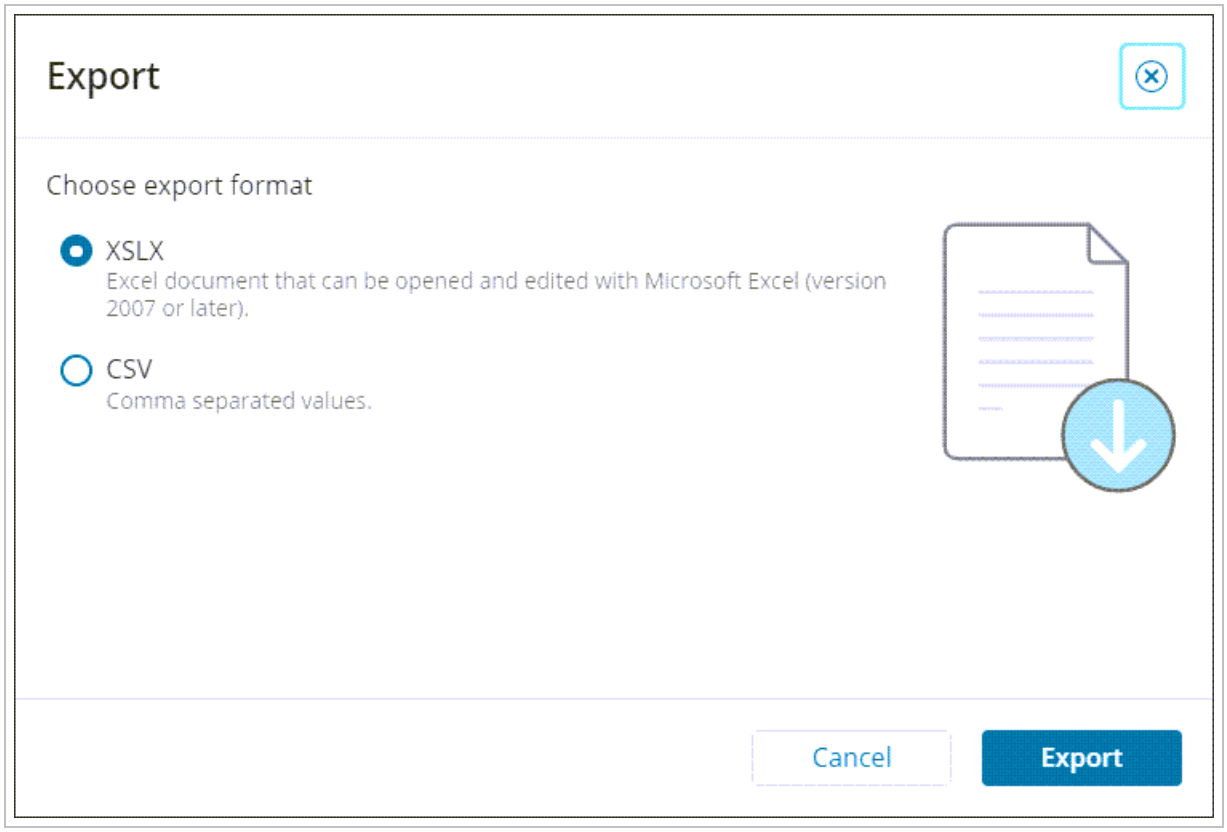
- Recovery session start date
- Restore format
  - Hyper-V VM
  - VHDX
  - Azure VM

Exporting

You may export a list of devices currently assigned a plan by clicking **Export**

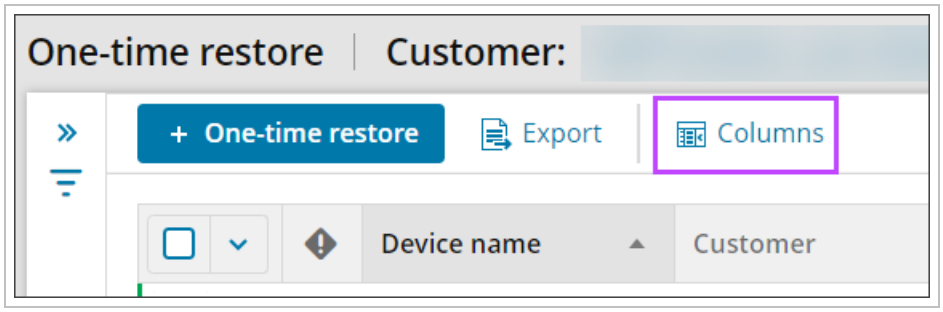


This will then provide a separate dialog where you can choose to export in either XSLX or CSV.

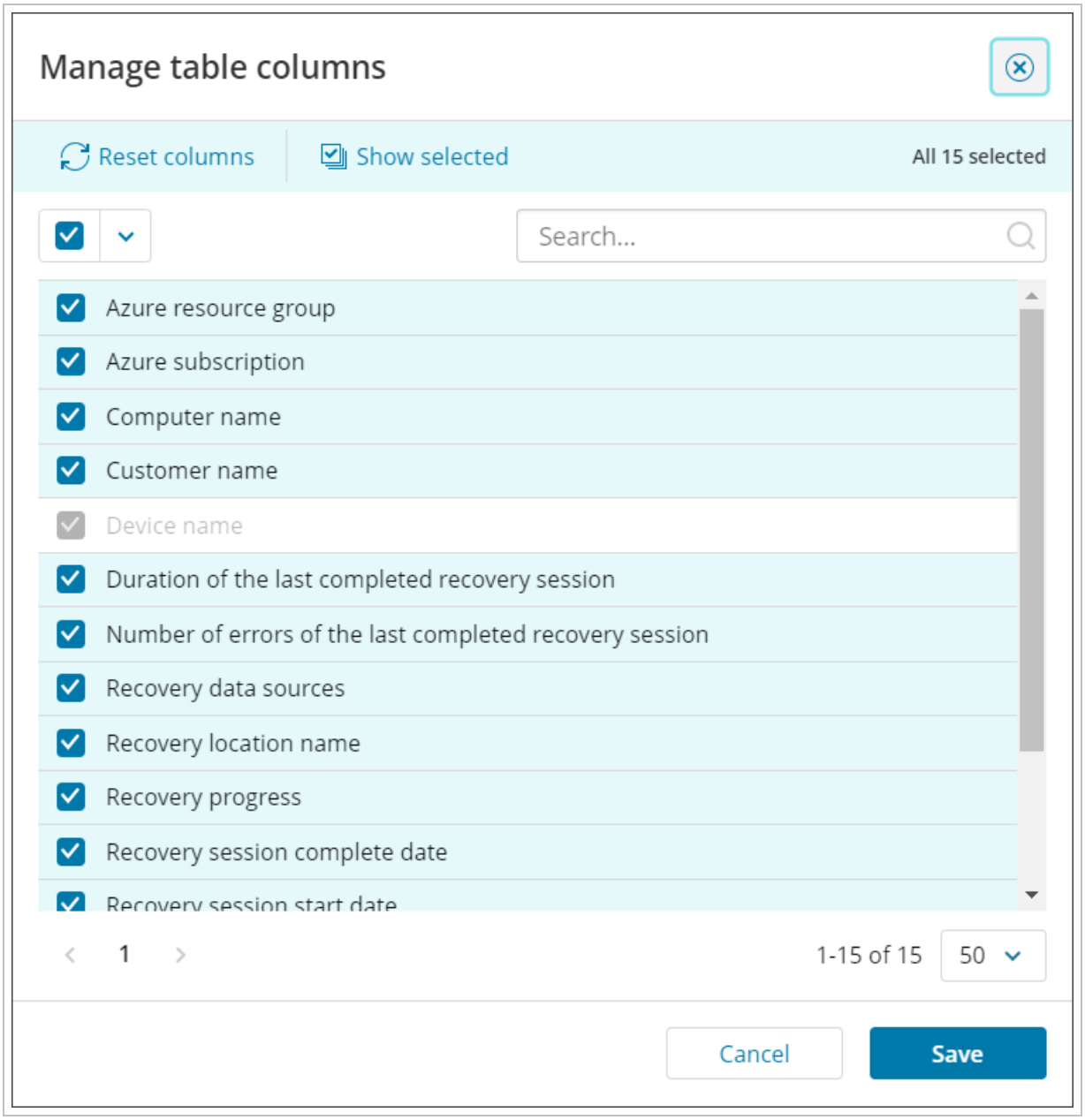


Manage Table Columns

Management Console allows you to manage the tables columns that can be seen within the One-Time Restore overview.



In the Manage table columns dialog, you can select and deselect columns based on the information you wish to view from the overview.



Accessing device properties

The Device Properties window displays several tabs detailing information on the Backup device. Full details of the contents of each tab can be found on the Device management in Management Console page.

This window can be accessed by clicking the **Device Name** from the One-Time Restore overview.

The two that are the most commonly used with One-Time Restore are the **Overview** tab and the **Settings** tab.

Remove Restore Record from Dashboard

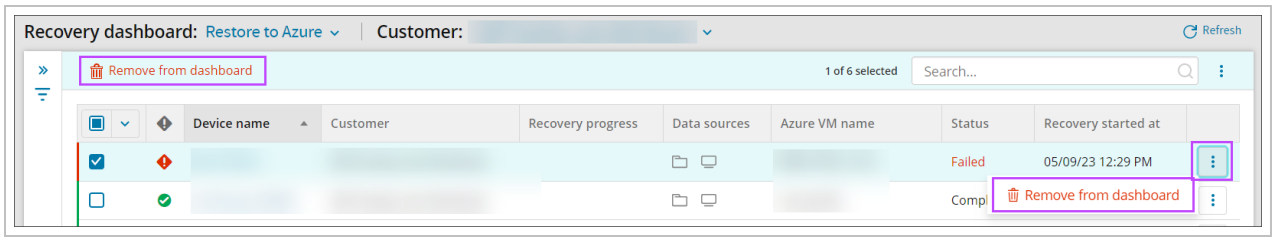
From the **One-Time Restore** overview, you may remove the record of a device's restore history.

This option is available for any restore status.

> This does **not** remove the device from any Standby Image plans or delete the device in Cove.

To remove a device's restore record:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity > One-Time Restore**
3. Using the search or filtering options, find the device(s) for which you need to delete the recovery record
4. Either:

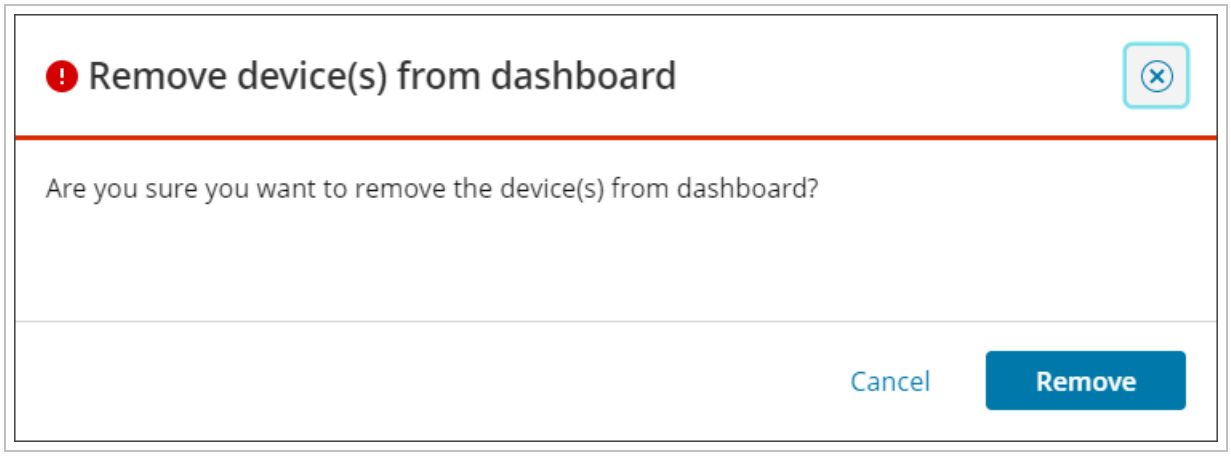


   a. Select the device(s) using the checkbox to the left of the Device Name and click **Remove from Dashboard** from the top bar

   or

   b. Using the action menu (three vertical dots) at the far right of the Device, select **Remove from Dashboard**

5. Confirm removal of the device's history



One-Time Restore to Azure

Cove Data Protection (Cove)'s **One-Time Restore** feature allows you to restore data to Microsoft Azure Virtual Machine as configured in Azure Recovery Locations on an on-demand basis.

Requirements

- An Azure Recovery Location
- Devices must be using Backup Manager version 17.4 or newer
- At minimum, you must have **Reader** role access to the subscription containing the Recovery Location VM
- An Application Administrator account for MS Azure or an account which has been granted permission to consent for apps
- A Cove Data Protection (Cove) SuperUser or Manager account
- The device to be restored must have `.NET Framework 4.0`

Limitations

- Available for Windows devices **only**
- **Files and Folders** and **System State** data sources must be included in the backup
- One-time restore is not available for devices where the 'Virtual disaster recovery' feature is disabled in an assigned Product
- 32-bit architecture is not supported
- Device should be In Agent Partner Tree
- Software-only devices are not supported
- Devices with operating system disks larger than **4TB** in size cannot be restored

What is restored?

The following data sources are supported and restored to the Azure recovery location given that they are selected for backup in the Product, or data source selection:

- Files and Folders
- System State
- MS SQL
- Exchange
- SharePoint

What's inside:

Configure One-Time Restore to Azure

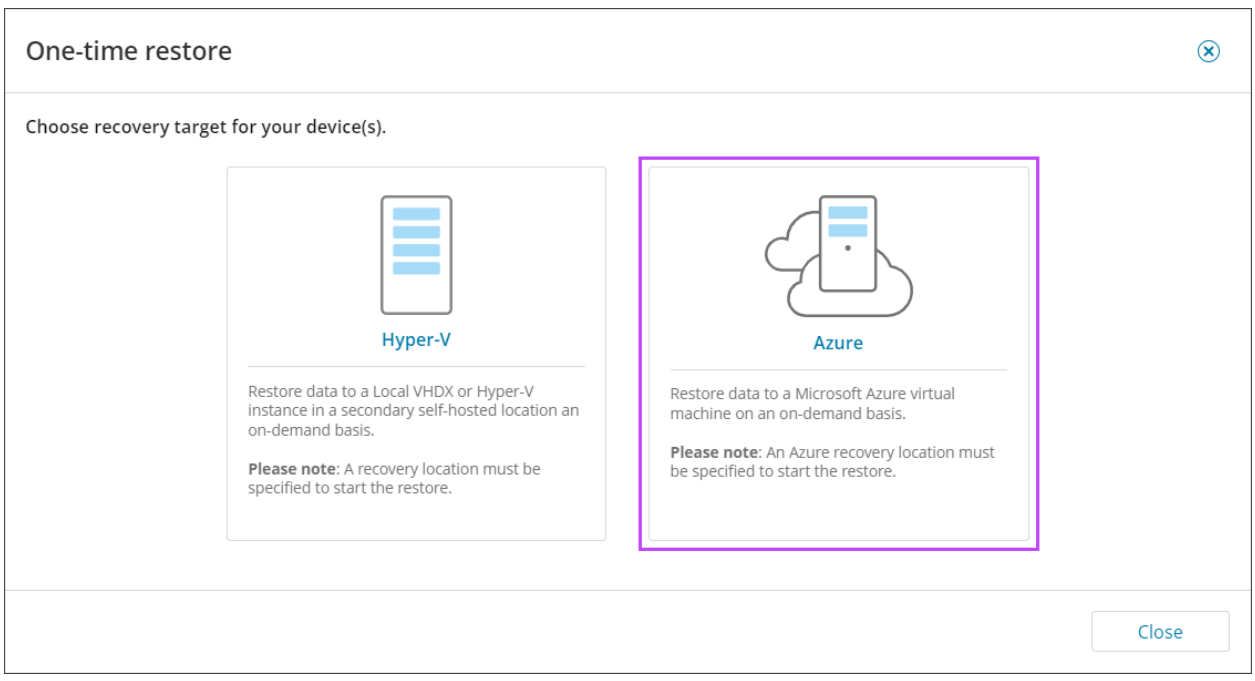
Before starting a One-Time Restore to Azure, ensure you have checked all requirements and limitations, including setting up an Azure recovery location.

From Backup Dashboard

1. Log in to the Management Console under a **SuperUser** account
2. In the Backup Dashboard, tick the checkbox to the left of the device(s) to restore

3. Click **One-Time Restore**

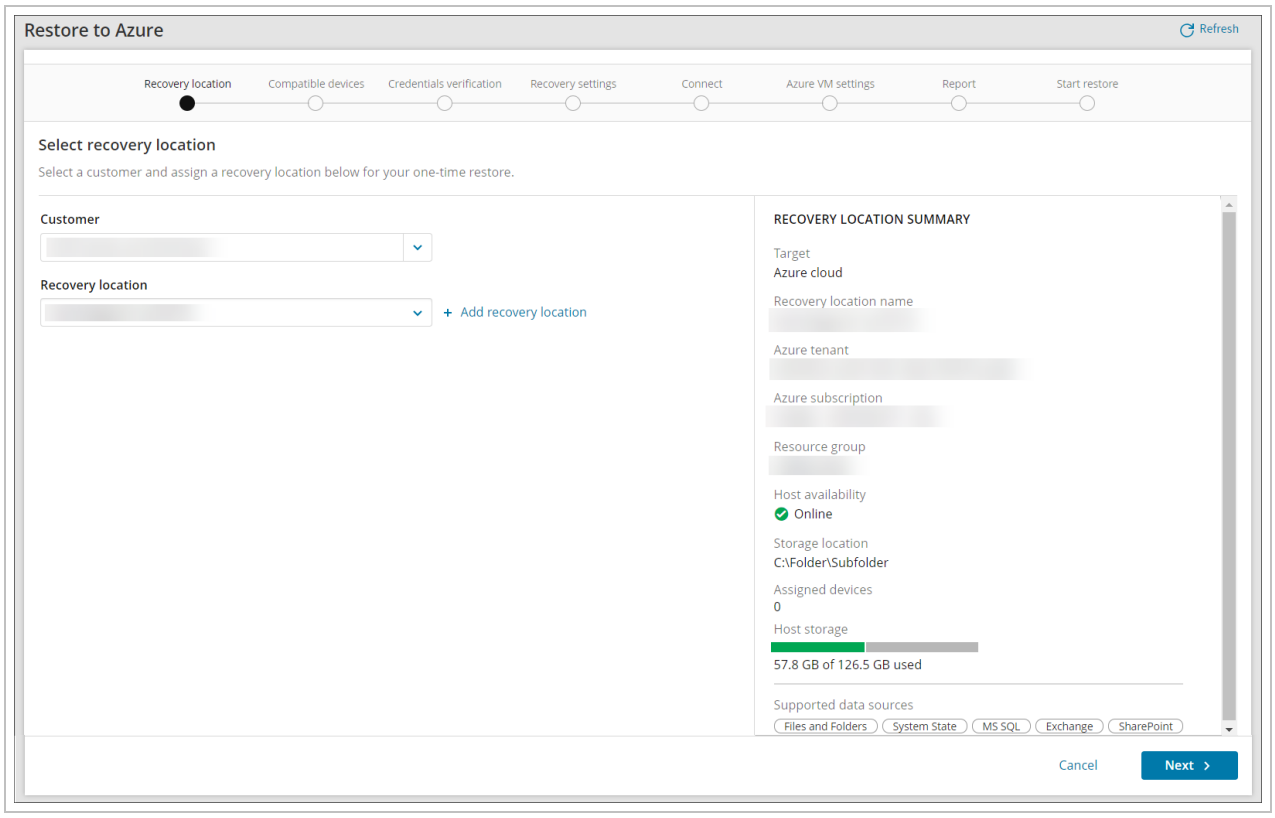
4. Select the **Azure** target



5. Select the Customer

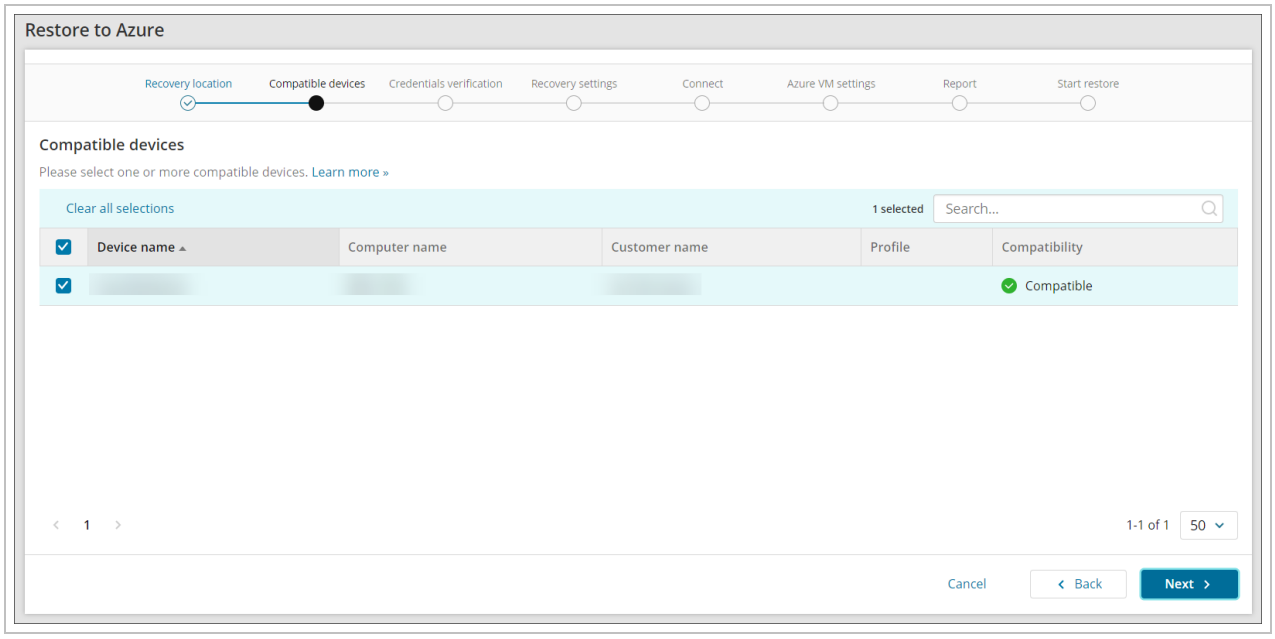
6. Select the Azure Recovery Location for the restore or click **+ Add recovery Location** to follow the steps to create a new Azure Recovery Location

> If adding a recovery location from here, you will be taken to the **Add Azure Recovery Location** wizard, where **Azure** will be automatically selected as the recovery type. Follow the Azure Recovery Location installation instructions from Step #4 onwards.



7. Click **Next**

8. Confirm compatibility of device(s) and click **Next**

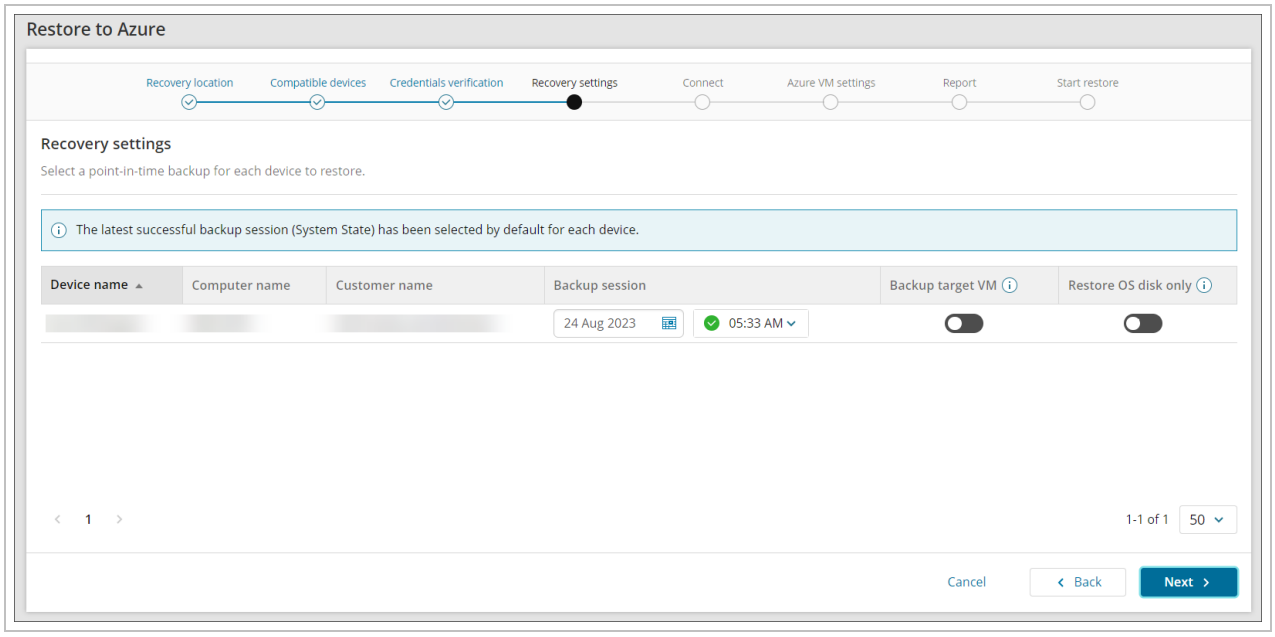


9. Enter the security code/encryption key or passphrase for the device(s). This can be either:
   - **Private encryption key** - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryption
   - **Passphrase encryption** - These are generated on demand for automatically installed devices. You can find information on this here

> If you are logged in as a security officer, this will be detected automatically.

10. Click **Next**

11. Select the date and time of the backup session to restore



> During this step, **all** available sessions for **all devices** listed will be loaded in the backup session column. **Please allow time for these to load**, if the load of sessions fails, a message stating so will be displayed with a refresh button to try again.

12. If you wish to protect the device according to its existing backup schedule, enable **Backup target VM**

> If the **Backup Target VM** option is enabled for one or more devices, be aware that if the backup agent is still running in backup mode on the source VM, this will lead to corrupted backup data for both the source and target VMs.

13. If you wish to skip all data drives, enable **Restore OS disk only**

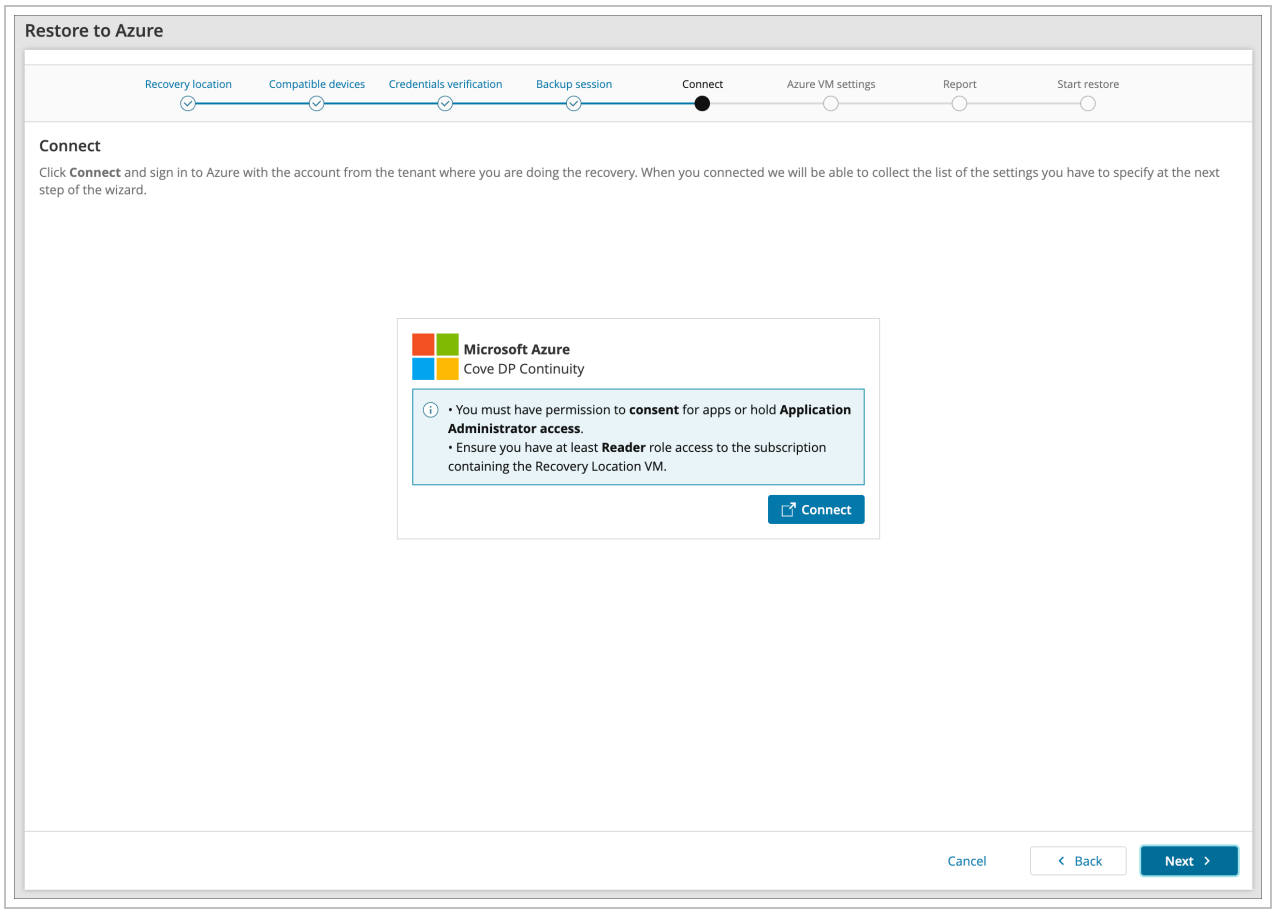
> Enabling **Restore OS disk only** will help to speed up restores as the only thing being restored is the Operating System

14. Click **Next**

15. Connect to Microsoft Azure by either:
    a. Allow permissions to the Azure user account to **consent for apps** access,

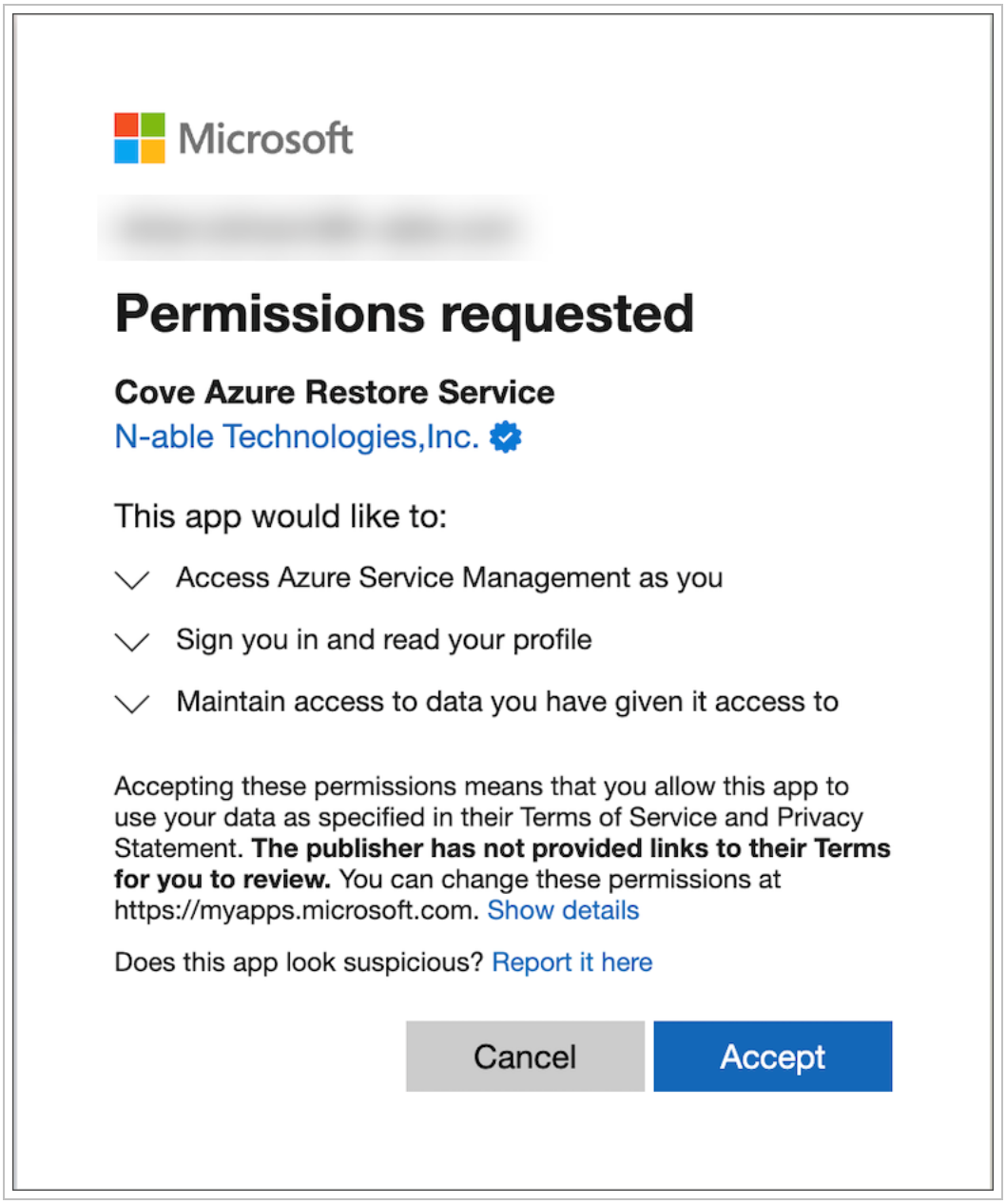
or;

    a. Login using Application Administrator access



> Ensure you have at minimum **Reader** role access to the subscription containing the Recovery Location VM

b. Accept the required permissions



If you do not see the authentication page, make sure your browser is not blocking pop-up windows.

16. Supply the **Azure VM settings**:

AZURE VM SETTINGS

Subscription

Resource group

Virtual machine name

BEN-0079

Region

West Europe

Availability options

VM size

OS disk type

Premium SSD

Data disk(s) type

Premium SSD

Virtual network

Subnet

default

Stop target VM after recovery

Assign NSG and public IP

- Subscription

  > This cannot be changed as the subscription is set in the **Recovery Location** configuration

- Resource Group
- Virtual Machine name
- Region

  > This cannot be changed as the subscription is set in the **Recovery Location** configuration

- Availability options
- VM size

  > If the **VM size** selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either **increase** the **regional vCPU quota** on the Subscription, or **decrease** the **VM size** selected in the Azure VM Settings.

- OS disk type

  > Set to **Premium SSD** to speed up the Azure restore. This can be changed in Azure later

- Data disk(s) type

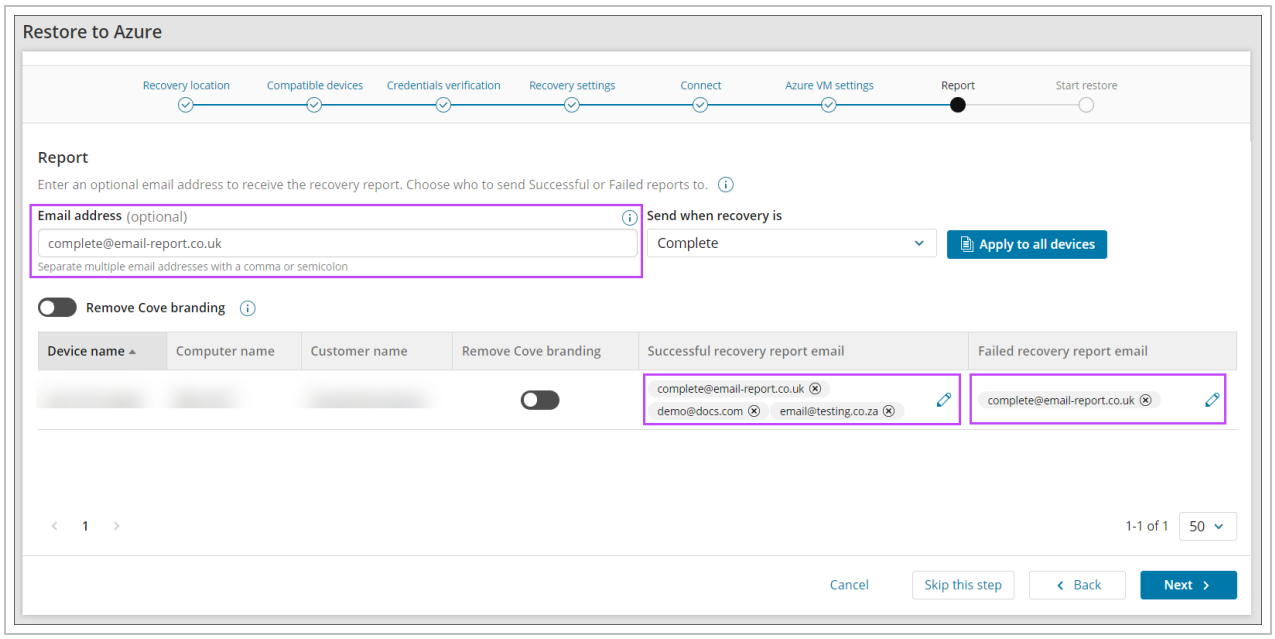
  > Set to **Premium SSD** to speed up the Azure restore. This can be changed in Azure later

- Virtual Network
- Subnet
- Stop target VM after recovery
- Assign NSG and public IP

17. Click **Next**

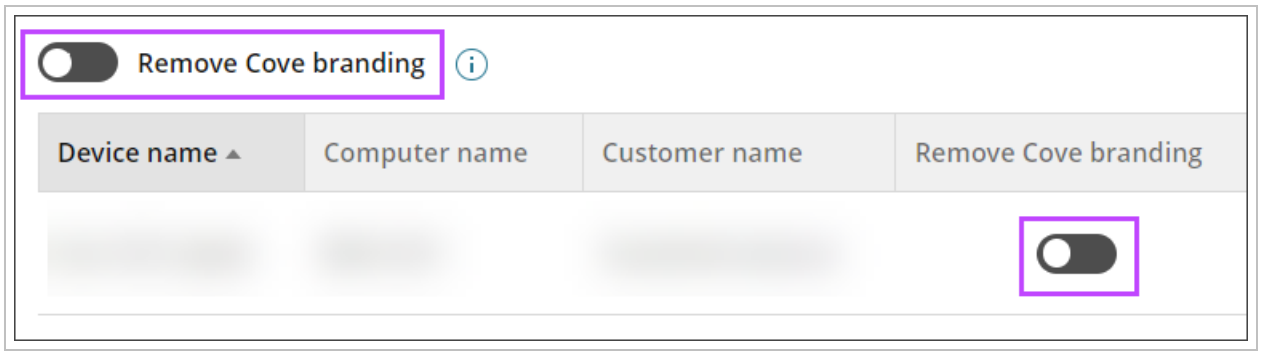
18. Click **Next** to progress to the **Report** window to enter one or more email addresses to receive a report when:
    a. The recovery is complete (Successful or Failed)
    b. The recovery was successful
    c. The recovery failed

> Multiple addresses should be separated using a comma or semi-colon



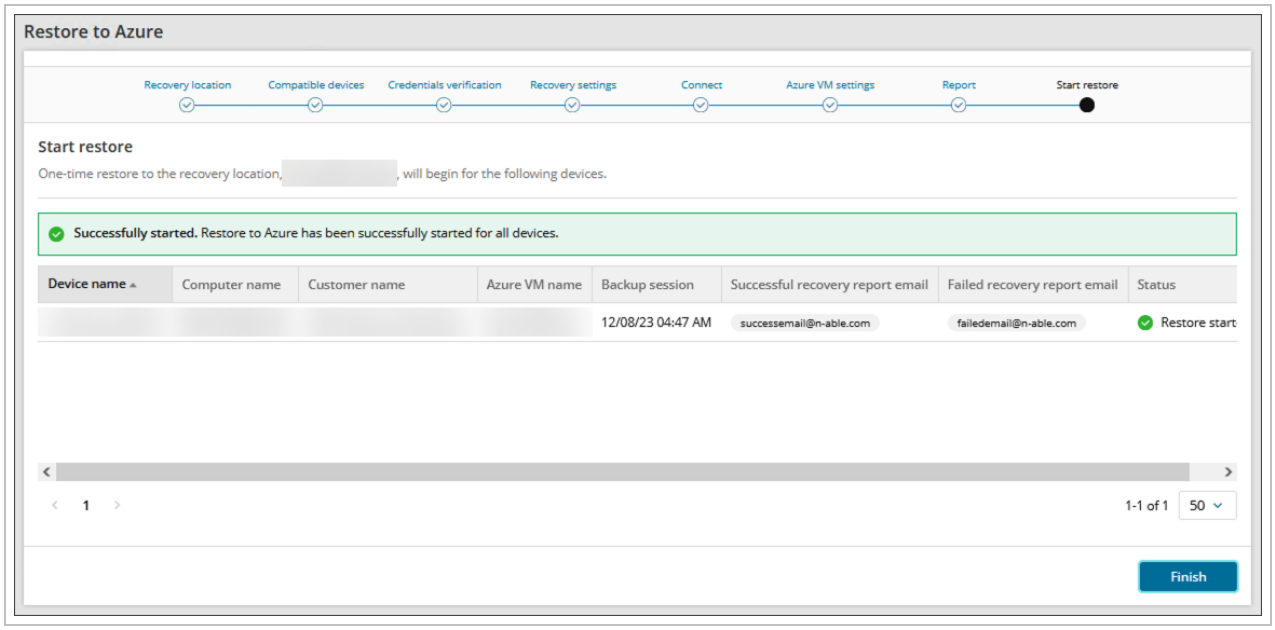
> If you do not want to add an email address to receive reports, click **Skip this step**

19. To remove all branding from the reports, use the **Remove Cove branding** toggle per device, or above the device list to apply the changes to all devices in this window



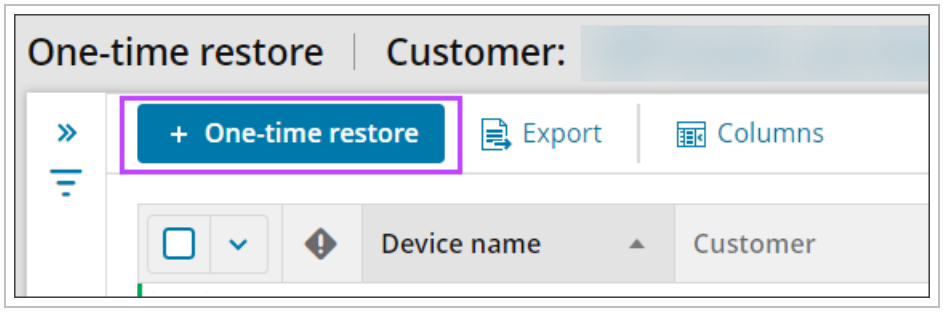
20. Review and confirm the restore details for each device and click **Confirm**

21. Once the restore has been started, a green banner will be displayed and a notification in the top right-hand corner of the screen to confirm. Click **Finish** to close the restore wizard and return to the Dashboard



From One-Time Restore Overview

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to the **One-Time Restore** overview by selecting **Continuity** > **One-time Restore** from the vertical menu on the left hand side
3. Click **One-time restore** from the top bar



4. The wizard will open to target selection window, follow the above steps from Step #4 onwards

Recovery Reports

When the device(s) assigned to the plan have **Successful recovery report email** or **Failed recovery report email** recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox.

Here is an example report **with** Cove branding:

Cove Data Protection

Recovery completed

On demand restore to Microsoft Azure

Last recovery session completed successfully: April 05 2023 7:12:10 PM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Restore to Azure dashboard.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Server
Operating system	Windows Server 2019 Standard Server (17763), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 05 2023 7:12:10 PM
Recovery status	Completed
Recovery duration	40 minutes and 58 seconds
Recovery location	

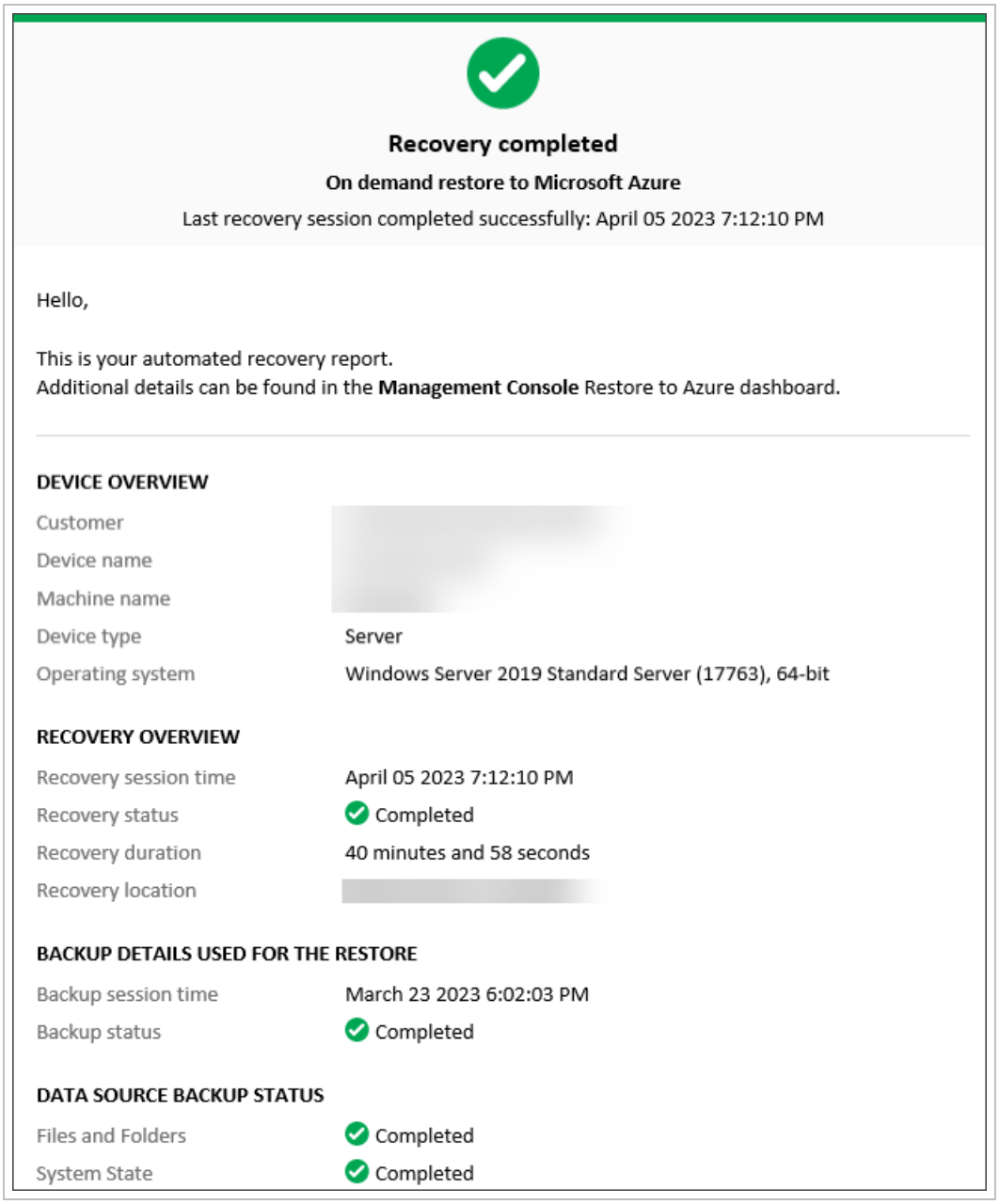
BACKUP DETAILS USED FOR THE RESTORE

Backup session time	March 23 2023 6:02:03 PM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

Here is an example **without** Cove branding:



Recovery completed

On demand restore to Microsoft Azure

Last recovery session completed successfully: April 05 2023 7:12:10 PM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Restore to Azure dashboard.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Server
Operating system	Windows Server 2019 Standard Server (17763), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 05 2023 7:12:10 PM
Recovery status	Completed
Recovery duration	40 minutes and 58 seconds
Recovery location	

BACKUP DETAILS USED FOR THE RESTORE

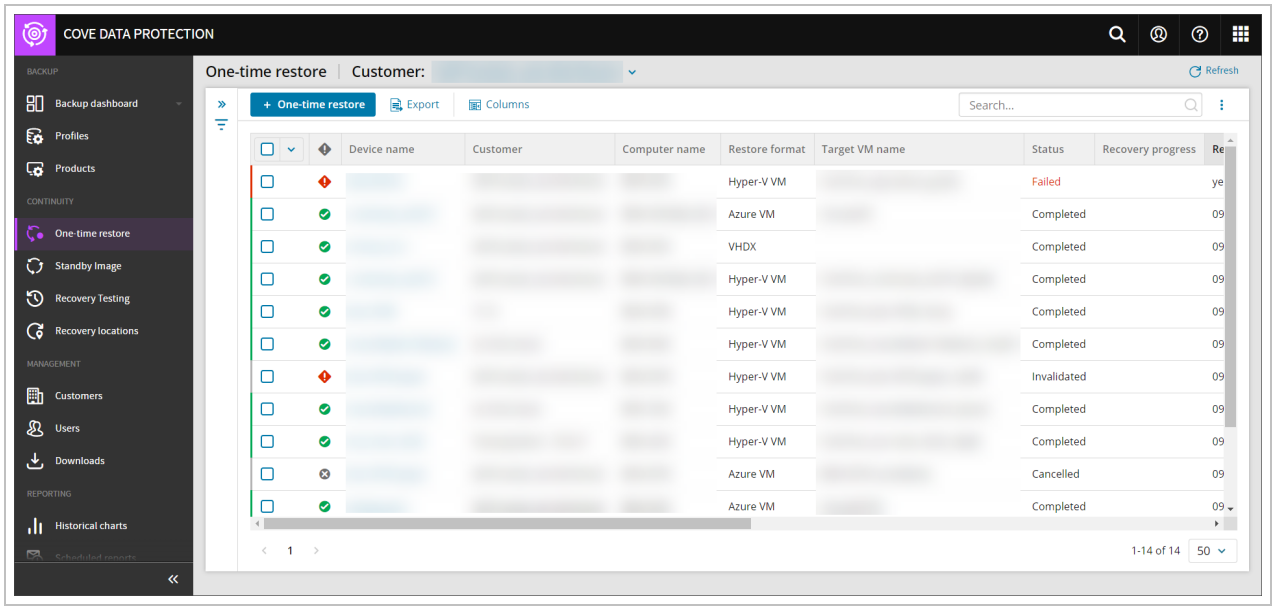
Backup session time	March 23 2023 6:02:03 PM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

Monitor Azure Restore Progress

From the Management Console, you can view the dedicated One-Time Restore overview by selecting **Continuity** > **One-time Restore** from the vertical menu on the left hand side.



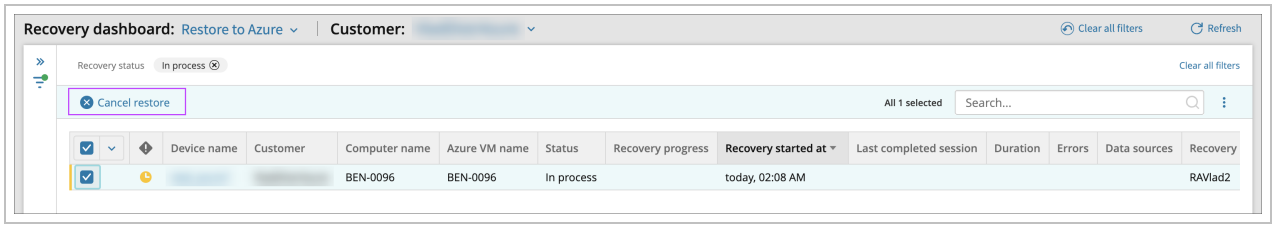
From this dashboard, you will see a specified set of columns detailing information relevant to devices using **One-time Restore**, including the status, restore format and data sources, along with other information relating to Azure and Hyper-V.

If no devices are active, the dashboard will display a message to advise.

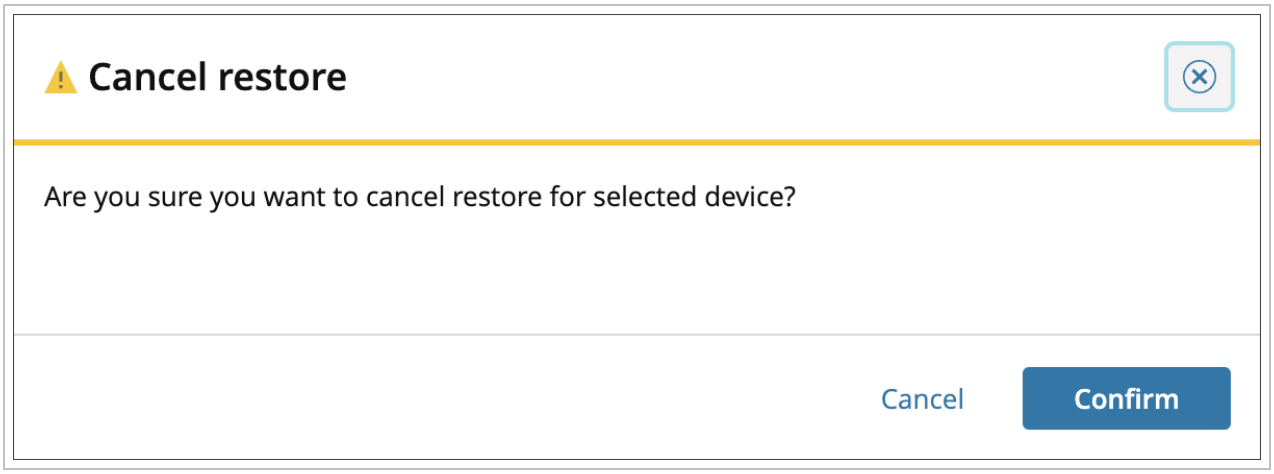
Cancel Restore

From the One-Time Restore overview, it is possible to cancel any recovery currently in progress:

1. Search for or use the filters to find the device in question where the recovery is currently running
2. Select the device
3. Click **Cancel restore** from the top bar



4. Confirm cancellation



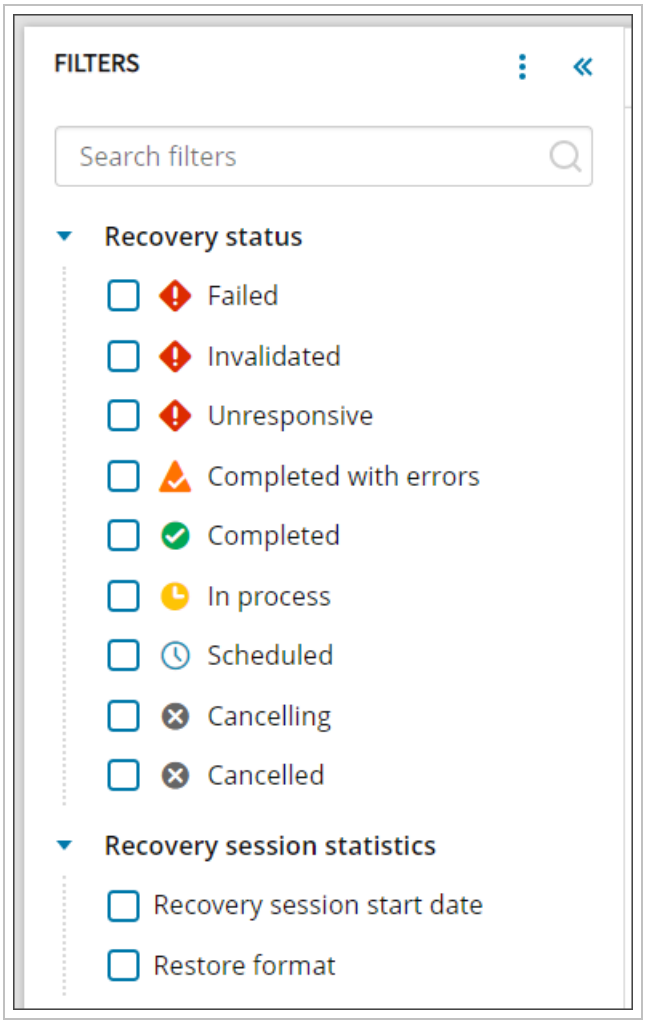
The device will now show in the list with a status of **Cancelled**

Searching

Searching within the One-Time Restore overview can be done by using the search box over to the right hand side of the page, just above the devices list. The search can be performed against any text field.

Filtering

The Standby Image overview also includes functionality to filter devices using the filter menu to the left of the device list and can be displayed or hidden by clicking the double arrows.



From this menu, you can filter by:

Recovery status

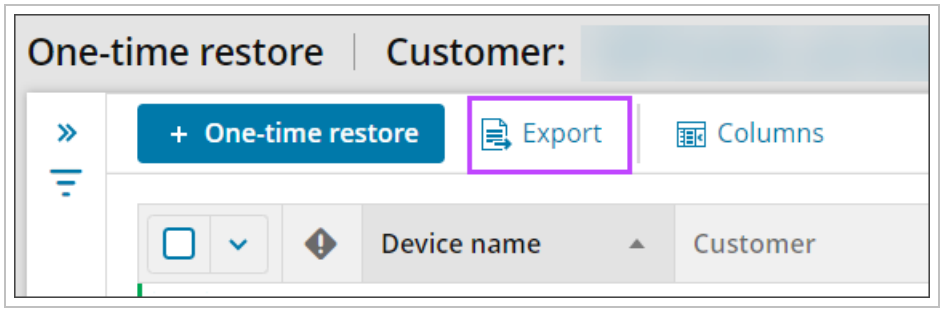
- **Failed** - The recovery session has failed
- **Invalidated** - Device was moved to an inappropriate partner and so the session has failed
- **Unresponsive** - The recovery session was initiated but did not receive updates for at least 30 minutes because the recovery location restarted or was offline.
- **Completed with errors** - The recovery session completed, but encountered errors
- **Completed** - The recovery session completed with no errors
- **In process** - The recovery is currently in progress
- **Scheduled** - Devices just added to a recovery plan and are waiting for their first recovery session or devices where restores were paused and have since been resumed will display as scheduled
- **Cancelling** - The recovery is in process of aborting
- **Cancelled** - The recovery has been cancelled

Recovery Session Statistics

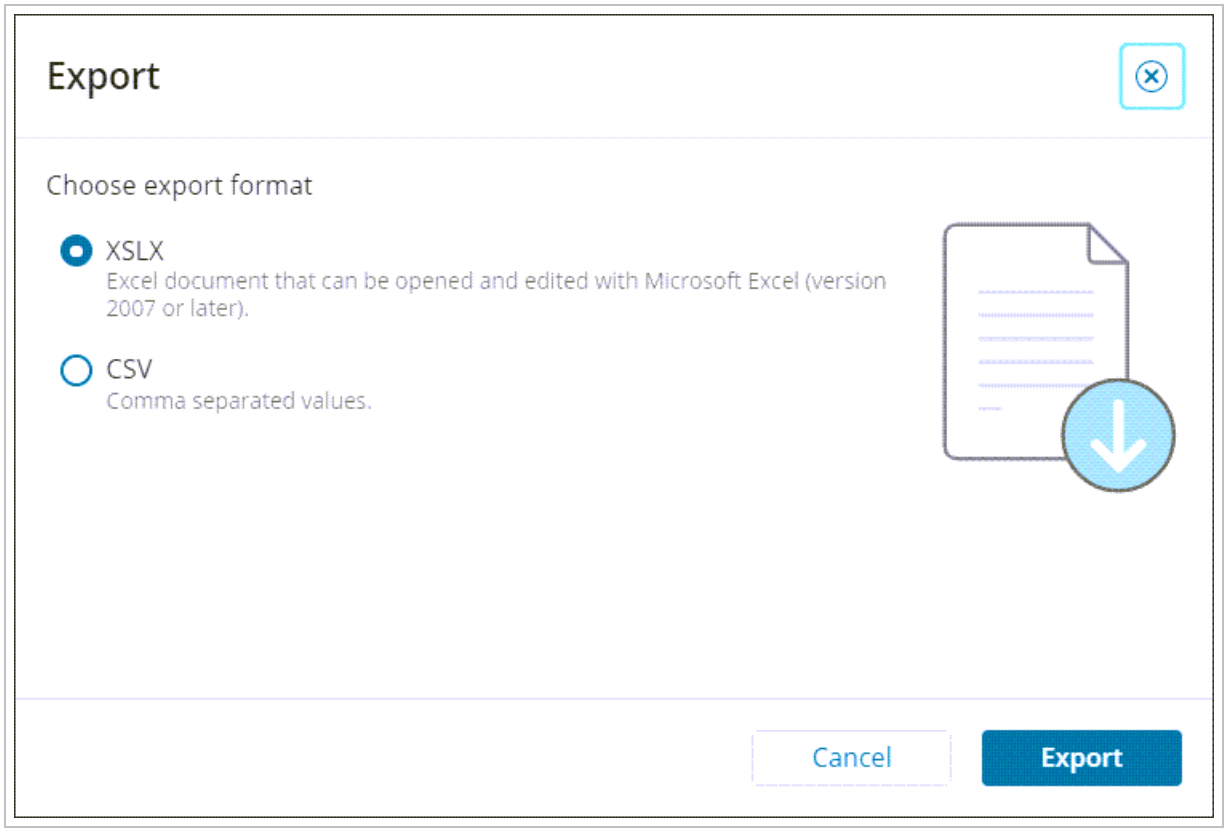
- Recovery session start date
- Restore format
  - Hyper-V VM
  - VHDX
  - Azure VM

Exporting

You may export a list of devices currently assigned a plan by clicking **Export**

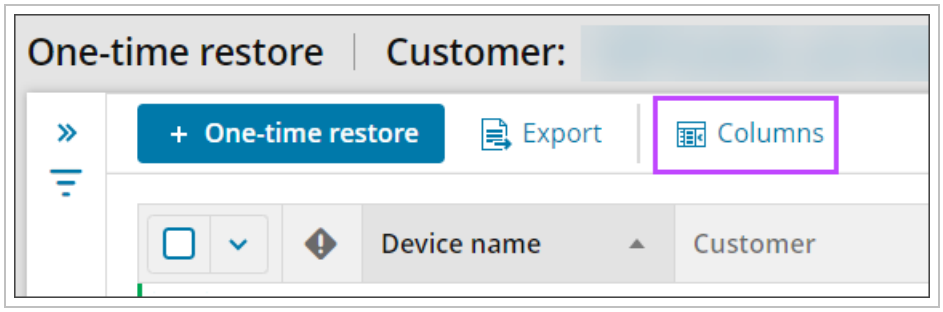


This will then provide a separate dialog where you can choose to export in either XSLX or CSV.

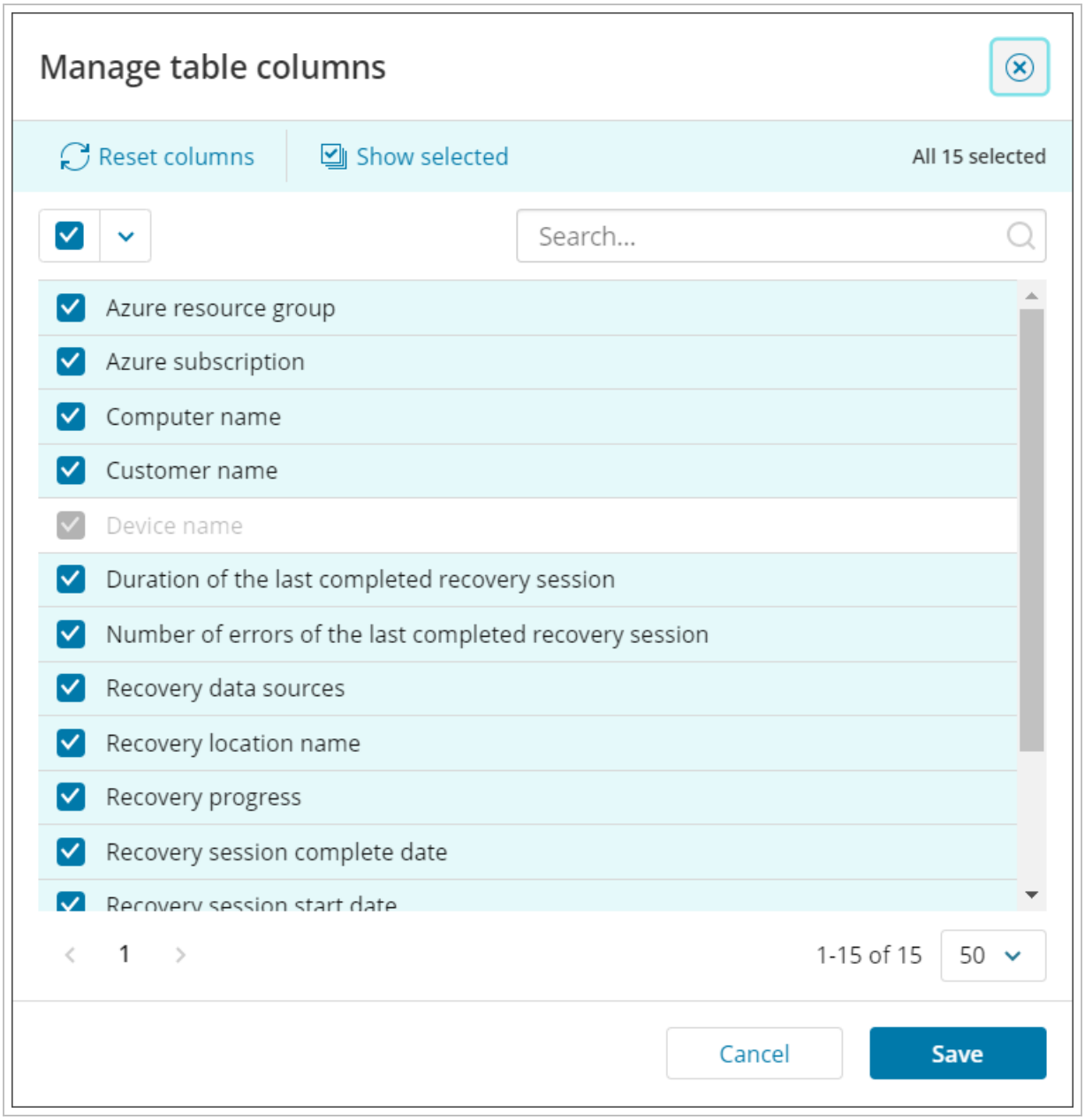


Manage Table Columns

Management Console allows you to manage the tables columns that can be seen within the One-Time Restore overview.



In the Manage table columns dialog, you can select and deselect columns based on the information you wish to view from the overview.



Accessing device properties

The Device Properties window displays several tabs detailing information on the Backup device. Full details of the contents of each tab can be found on the Device management in Management Console page.

This window can be accessed by clicking the **Device Name** from the One-Time Restore overview.

The two that are the most commonly used with One-Time Restore are the **Overview** tab and the **Settings** tab.

Remove Restore Record from Dashboard

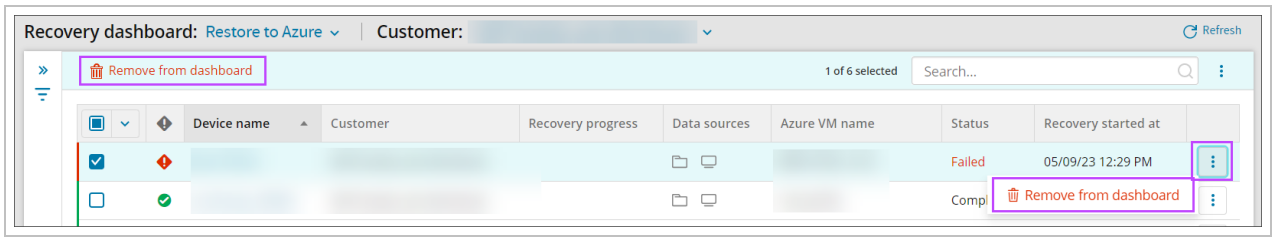
From the **One-Time Restore** overview, you may remove the record of a device's restore history.

This option is available for any restore status.

> This does **not** remove the device from any Standby Image plans or delete the device in Cove.

To remove a device's restore record:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity > One-Time Restore**
3. Using the search or filtering options, find the device(s) for which you need to delete the recovery record
4. Either:

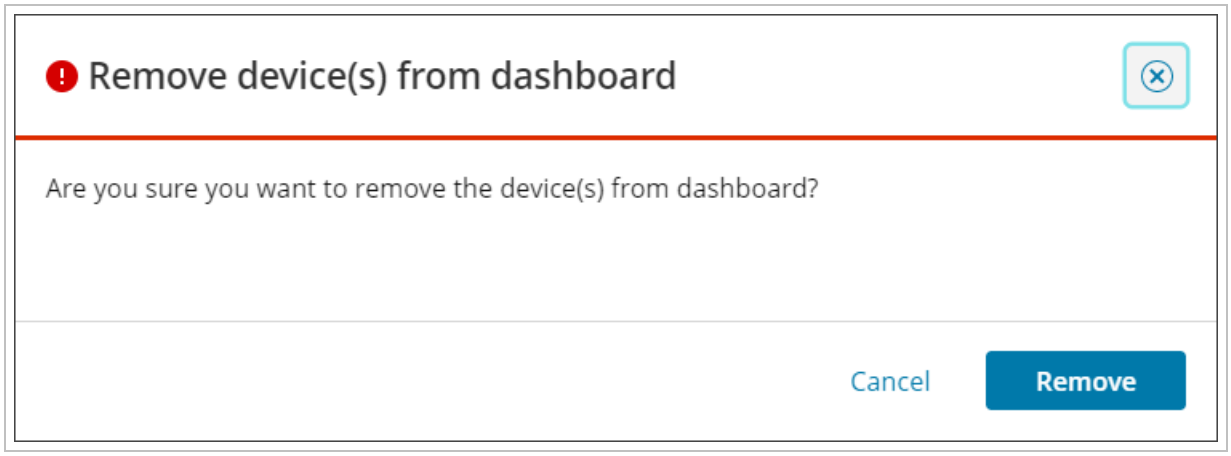


   a. Select the device(s) using the checkbox to the left of the Device Name and click **Remove from Dashboard** from the top bar

   or

   b. Using the action menu (three vertical dots) at the far right of the Device, select **Remove from Dashboard**

5. Confirm removal of the device's history



Standby Image

Cove has three separate methods of running a continuous restore of your data:

- Standby Image to Hyper-V - This service runs a continuous restore of a device to a Hyper-V or Local VHDX as configured in Add Recovery Locations

- Standby Image to Azure - This service runs a continuous restore of your data to Microsoft Azure and boots based on the frequency set during configuration of the plan to an Azure Virtual Machine as configured in Azure Recovery Locations
- Standby Image to ESXi- This service runs a continuous restore of a device to an ESXi server/host as configured in ESXi Recovery Locations

What's inside:

Standby Image to Hyper-V

Cove Data Protection (Cove) offers **self-hosted** Standby Image as a form of disaster recovery. It is a scheduled, automated service to recover critical devices.

> Devices **can** be assigned to **multiple Standby Image plans** at once, i.e. Standby Image to Hyper-V *and* Standby Image to Azure *and* Standby Image to ESXi.

Restores run after each backup session for System State, Files and Folders. After the first restore, a virtual machine is created and kept on the selected Recovery Location, then with each subsequent restore the virtual machine is updated with only new data.

> Restores can be performed to either a Hyper-V instance or to a Local VHDX file. Local VHDX files can be restored to either a Local Drive, or to a Network Share (NAS).

For a Virtual Machine restored to Hyper-V, there is an option to automatically boot it and create a screenshot to check that the Virtual Machine is bootable, then send this screenshot to the Management Console so that users can check it.

> There is no limit to the number of devices that can be added to a recovery location

Standby Image Data Restored:

The following data sources are supported and restored to the Hyper-V recovery location given that they are selected for backup in the Product, or data source selection:

- System State
- Files and Folders
- Exchange
- SharePoint
- MS SQL

Requirements:

- Backup Manager version 17.4 and newer
- Devices and Recovery Locations must belong to the same Customer
- A Cove Data Protection (Cove) SuperUser or Manager account

- Recovery Locations must be added to the Management Console and the Recovery service must be installed on the recovery location **before** Standby Image recovery can occur

> - Recovery Location is an environment where restores will be performed
> - Recovery service is a service which perform restores on that Recovery location

Limitations

- Standby Image cannot be used on the RMM integrated version of Backup (Managed Online Backup) or on the N-central integrated version of Backup (Backup and Recovery)
- Standby Image is **not** available for devices with disabled 'Virtual disaster recovery' feature in an assigned Product
- 32-bit architecture is not supported
- Due to a Microsoft limitation, Hyper-V **does not** support FAT/FAT32/ExFAT formatted drives. For this reason, please use NTFS formatted drives for Standby Image. More information can be found in the Microsoft Documentation for Hyper-V
- Maximum supported capacity for virtual hard disks is **64 TB** per disk
- Devices can only be assigned to **one** Recovery Location

What's inside:

Enable Standby Image to Hyper-V

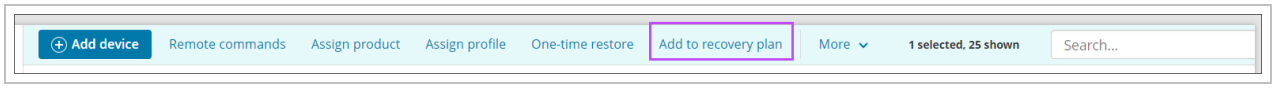
> Devices **cannot** be added to a **Standby Image plan** if already assigned to a **Recovery Testing plan**.

> Devices **can** be assigned to **multiple Standby Image plans** at once, i.e. Standby Image to Hyper-V *and* Standby Image to Azure.

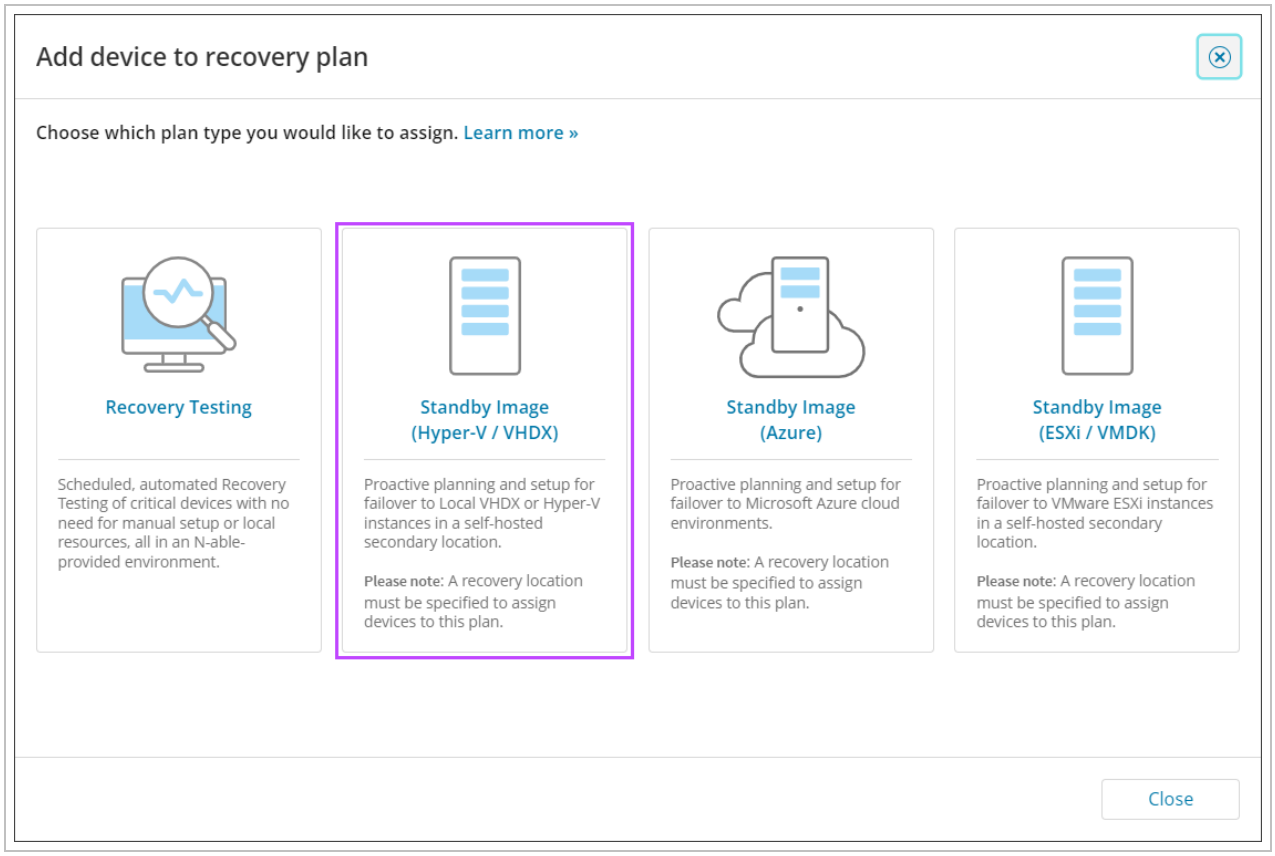
From Main Dashboard

To enable Standby Image to Hyper-V on a device from the Management Console's main Dashboard, follow the steps below:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan to
3. Click **Add to recovery plan** from the Toolbar



4. Select **Standby Image (Hyper-V)**

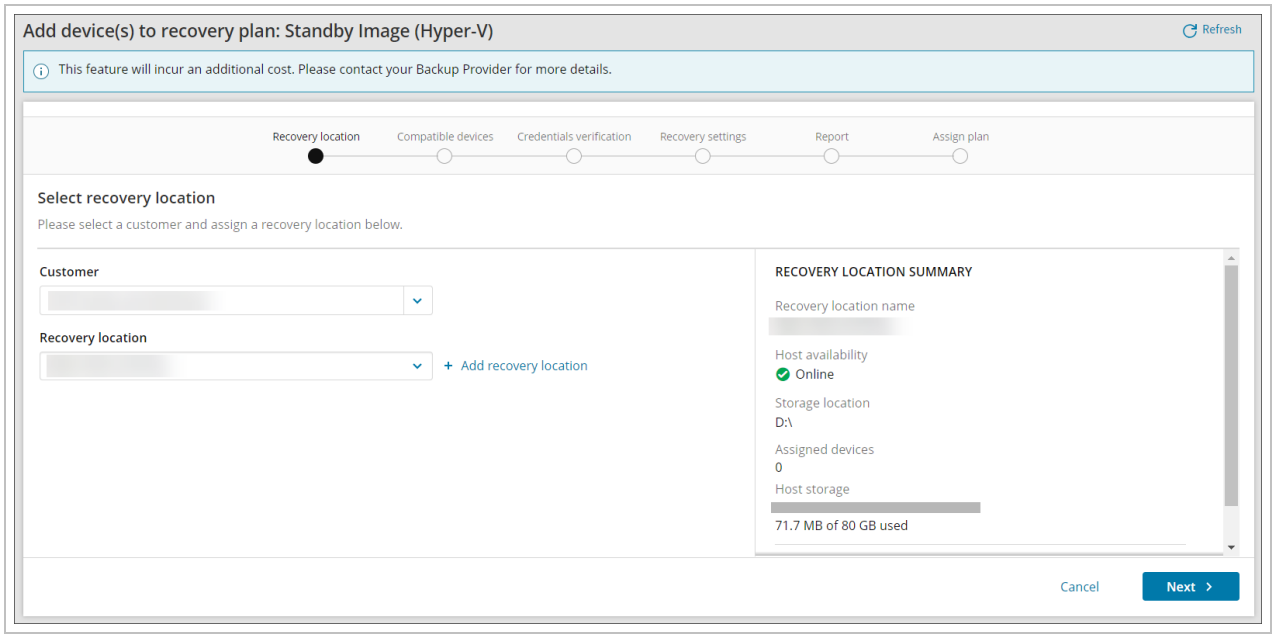


5. Select the customer the device(s) you wish to apply the Standby Image plan belong to

6. Choose the recovery location as was configured in Add Recovery Locations

> If the selected customer does not have any locations, you must add one before continuing by selecting **Add recovery location**. See Add Recovery Locations for full details of adding a location.

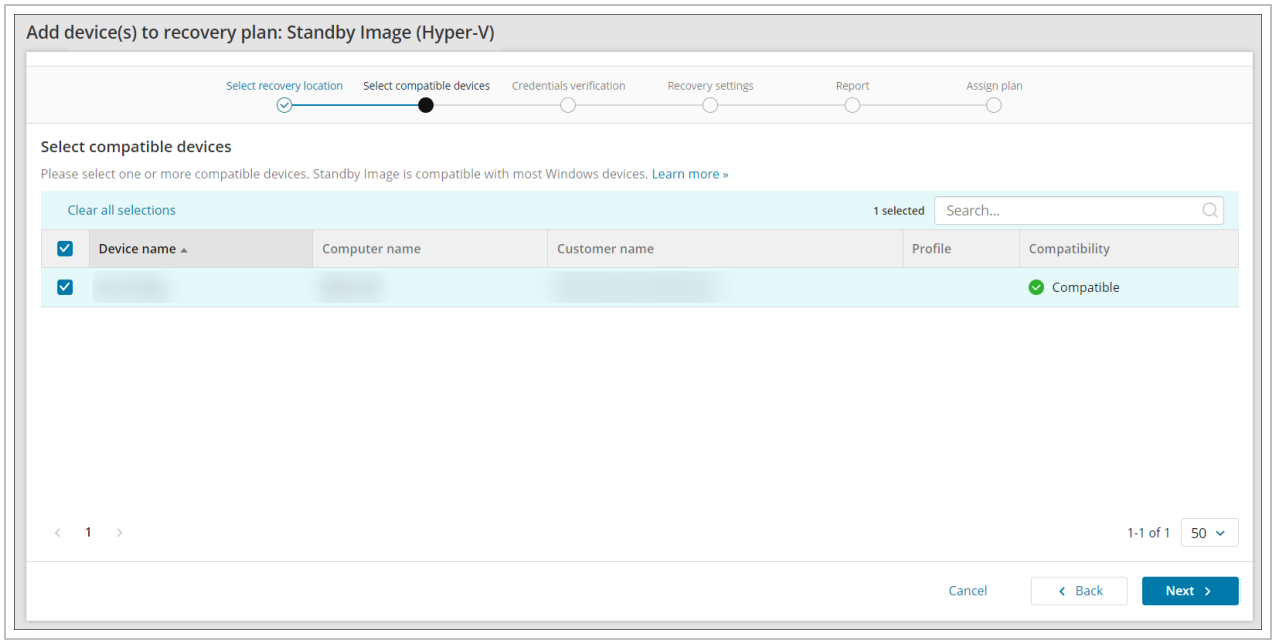
> If the Recovery Location does not have a drive letter, one must be provided before continuing



> It is not possible to assign a location for which the **Host availability** is "**Offline**"

7. Click **Next**

8. Confirm compatibility of the device(s) you want to apply the Standby Image plan on

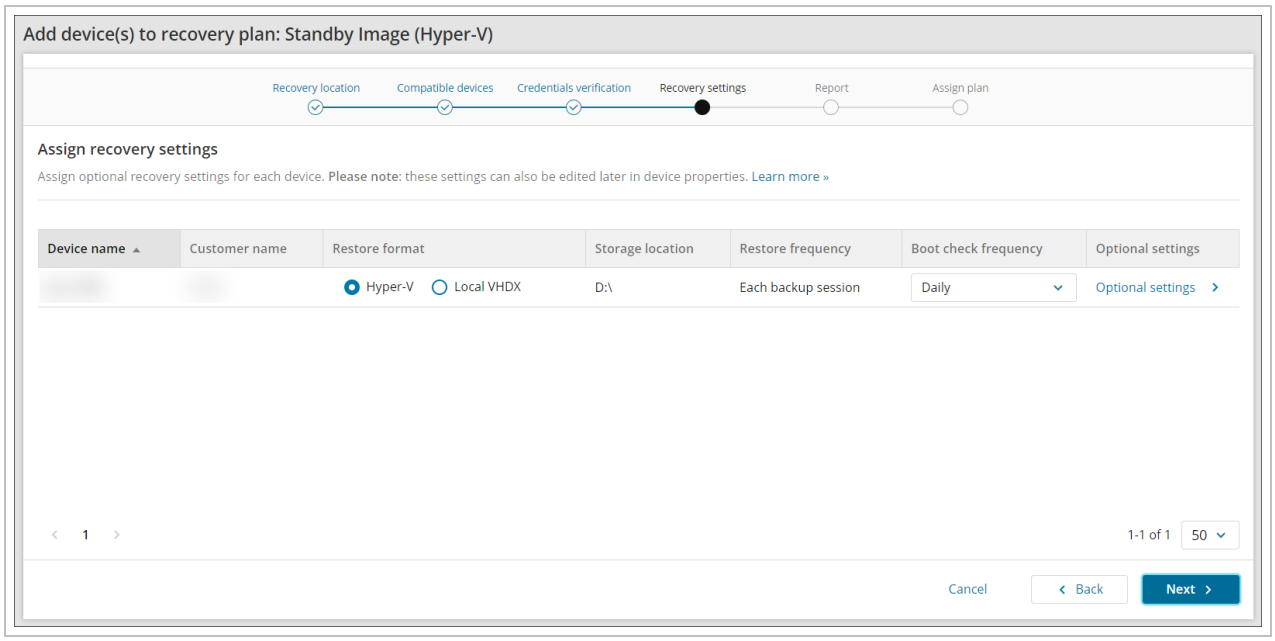


9. Click **Next**
10. Enter the security code/encryption key or passphrase for the device(s). This can be either:
    - **Private encryption key** - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryption
    - **Passphrase encryption** - These are generated on demand for automatically installed devices. You can find information on this here

    > If you are logged in as a security officer, this will be detected automatically.

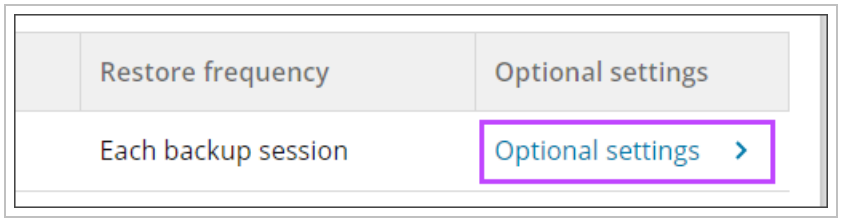
11. Click **Next** to continue

12. Choose the restore format:
    - Hyper-V
    - Local VHDX



13. Choose the boot check frequency:
    - Off
    - Every recovery session
    - Daily
    - Weekly
    - Biweekly
    - Monthly

14. Configure the **Optional Recovery Settings** for the restore format selected by clicking **Optional Settings** to the right of the storage location:



- Hyper-V optional settings:

OPTIONAL RECOVERY SETTINGS

Boot VM after restore and take a screenshot

Restore OS disk only

FRS and DFSR services

Local Speed Vault

CPU cores

4

RAM (GB)

4

Virtual switch

default switch

Enter a virtual switch to enable network settings

VM Subnet mask

255.255.255.0

VM gateway

10.16.10.1

VM DNS server

10.16.10.5.8.8.8.8

Separate multiple DNS servers with a comma or semicolon

VM IP address

10.16.10.24

IP addresses will increment by 1, if applied to all devices

- **Boot VM after restore and take a screenshot** - If this option is enabled, the new virtual machine is booted up after recovery and a confirmation screenshot is created. The results of recovery sessions together with screenshots of the booted systems come in email notifications if an email address was provided to receive a report

  The screenshots are also available in the Management Console see the "Screenshot" column in the Standby Image overview

  > Use the feature carefully if there is another virtual machines in the local network offering the same services (for example, the Active Directory) as it can result in a conflict with subsequent data loss.

- **Restore OS disk only** - Restoring the OS disk only will speed up restores
- **FRS and DFRS services** - If you are restoring Active Directory with multiple domain controllers, you should change the FRS and DFSR services to authoritative in the domain controller that will be started in the first place. Avoid marking several FRS/DFSR services as authoritative in the production environment as it can result in data loss. When the feature is on, the FRS and DFSR services are started on the target VM in the authoritative mode. The NETLOGON and SYSVOL shares become available, so the Active Directory and DNS services become functional again

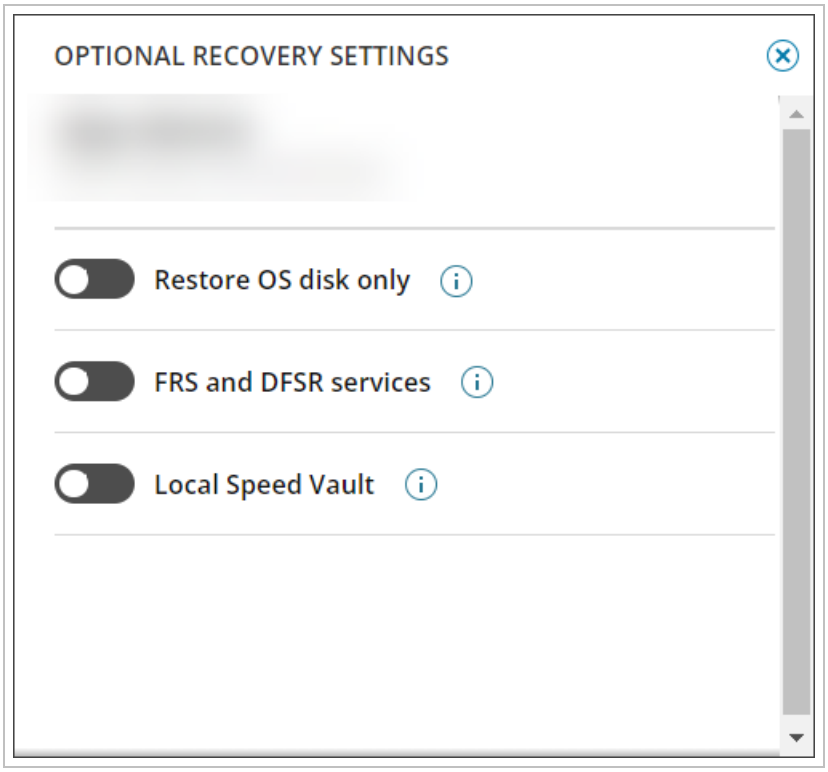
  > More information about FRS/DFSR is available in the Microsoft Knowledge Base. Article IDs: KB2218556 and KB290762

- **LocalSpeedVault** - If a LocalSpeedVault (LSV) is enabled on a backup device, the data is sent to both the LSV and the cloud or private storage location. During a restore, data is automatically downloaded from the LSV first to the local device which makes restore faster. If the LSV is not available or not synchronized, the restore data will be pulled from the cloud or private storage location. This takes place automatically and cannot be reconfigured
- **CPU Cores** - Select the number of CPU Cores to be allocated to the new virtual machine
- **RAM (GB)** - Select the amount of RAM in Gigabytes to be allocated to the new virtual machine
- **Virtual switch** - Enter the Hyper-V network adapter that will be used by your new virtual machine
- **VM subnet mask** - Assign a custom subnet mask to the virtual machine
- **VM gateway** - Assign a custom gateway to the virtual machine
- **VM DNS servers** - Assign the list of custom DNS servers (separated by comma), Example:

  ```
  8.8.8.8 or 8.8.8.8,7.7.7.7
  ```

- **VM IP address** - Assign a custom IP address to the virtual machine

- Local VHDX optional settings:



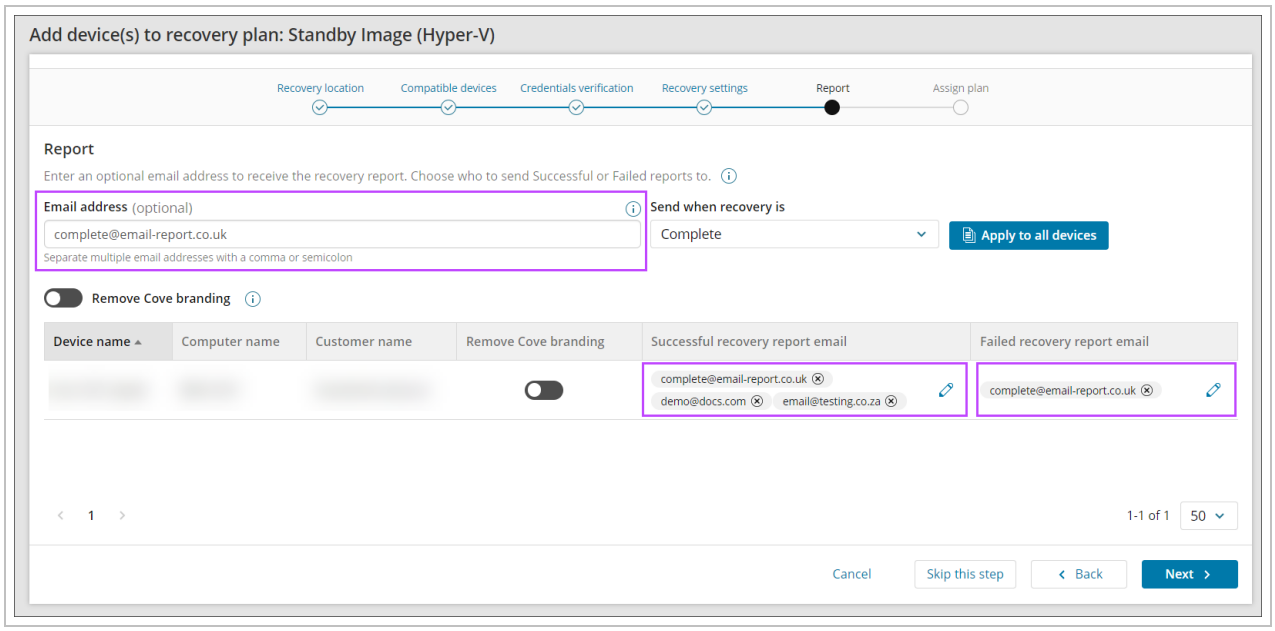
  - **Restore OS disk only** - Restoring the OS disk only will speed up restores
  - **FRS and DFRS services** - If you are restoring Active Directory with multiple domain controllers, you should change the FRS and DFSR services to authoritative in the domain controller that will be started in the first place. Avoid marking several FRS/DFSR services as authoritative in the production environment as it can result in data loss. When the feature is on, the FRS and DFSR services are started on the target VM in the authoritative mode. The NETLOGON and SYSVOL shares become available, so the Active Directory and DNS services become functional again

    > More information about FRS/DFSR is available in the Microsoft Knowledge Base. Article IDs: KB2218556 and KB290762

  - **LocalSpeedVault** - If a LocalSpeedVault (LSV) is enabled on a backup device, the data is sent to both the LSV and the cloud or private storage location. During a restore, data is automatically downloaded from the LSV first to the local device which makes restore faster. If the LSV is not available or not synchronized, the restore data will be pulled from the cloud or private storage location. This takes place automatically and cannot be reconfigured

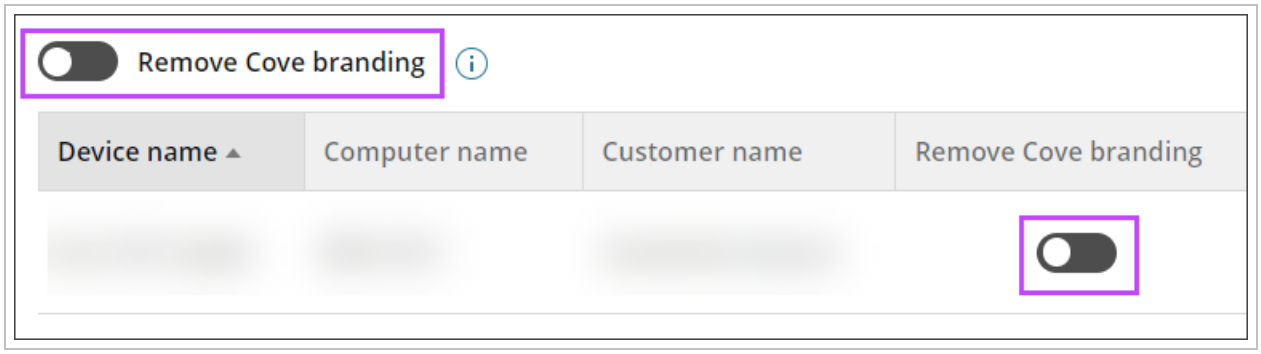
15. Click **Next** to progress to the **Report** window to enter one or more email addresses to receive a report when:
    a. The recovery is complete (Successful or Failed)
    b. The recovery was successful
    c. The recovery failed

> Multiple addresses should be separated using a comma or semi-colon



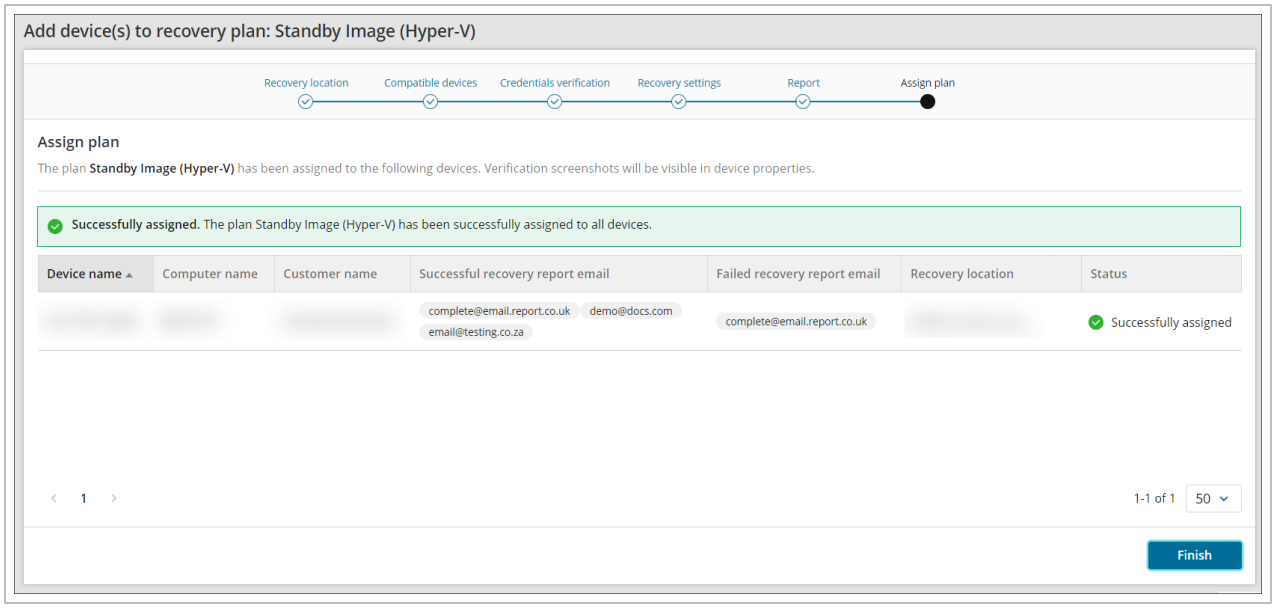
> If you do not want to add an email address to receive reports, click **Skip this step**

16. To remove all branding from the reports, use the **Remove Cove branding** toggle per device, or above the device list to apply the changes to all devices in this window



17. Confirm assigning the plan to the device(s)

18. Wait for the plan to be assigned until you see a confirmation banner on the page

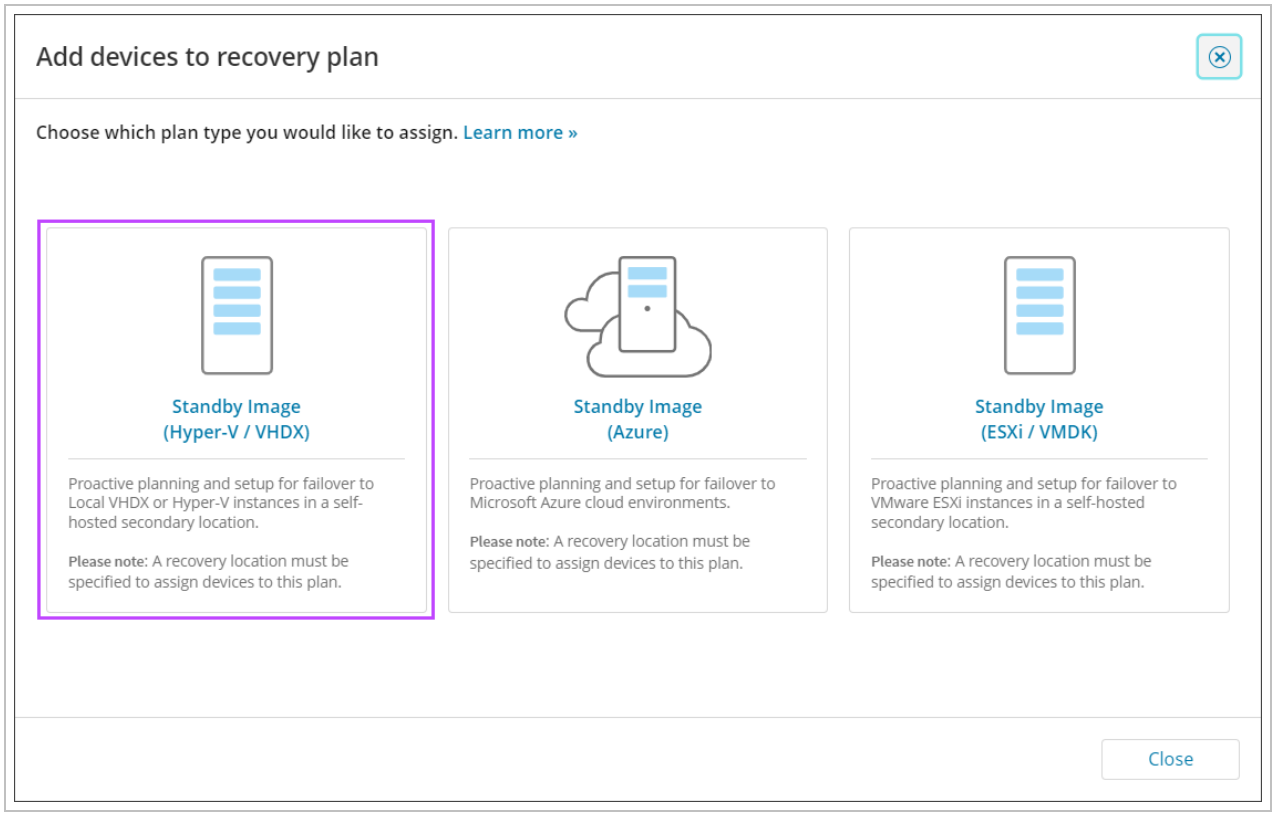


19. Click **Finish**

From Standby Image Overview

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Click **Add to Plan**

4. Select **Standby Image (Hyper-V)**



5. You will now be taken to the **add devices to recovery plan** wizard. Follow the steps from select the customer from the dropdown onwards

From Recovery Locations dashboard

Devices can be added to a Recovery Location from the **Continuity** > **Recovery Locations** page, thereby enabling the Standby Image Plan, using one of three methods:

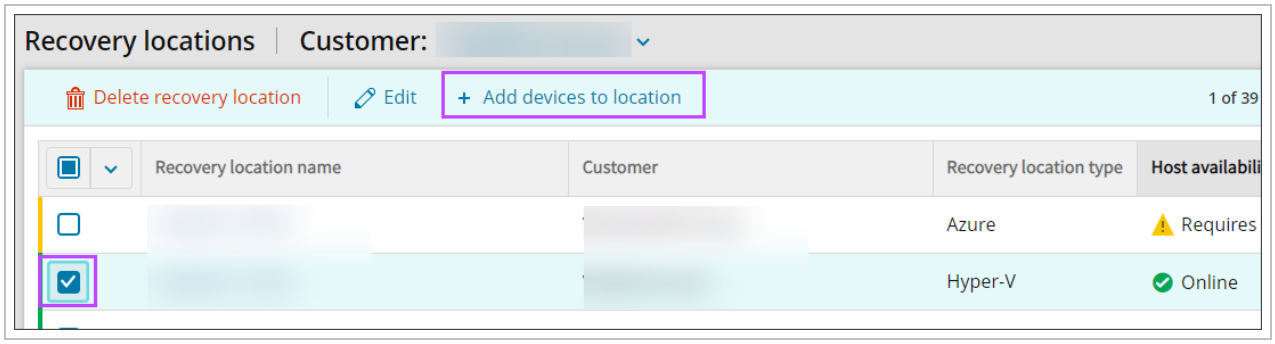
- Top bar menu
- Location context menu
- Right-hand menu

> These will only be available if the Recovery Location is **Online**.

Top bar menu

Available for Hyper-V and ESXi Locations **only**.

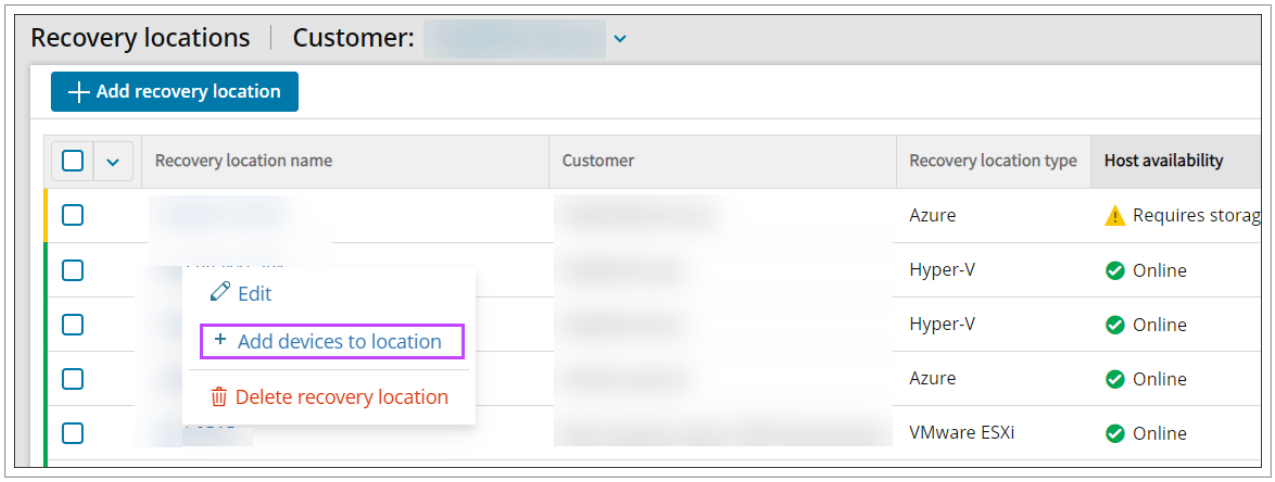
1. Select the checkbox for the Recovery Location to add the device to
2. At the top of the Recovery Locations page, select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
   a. Top bar menu
   b. Top bar menu

Location context menu

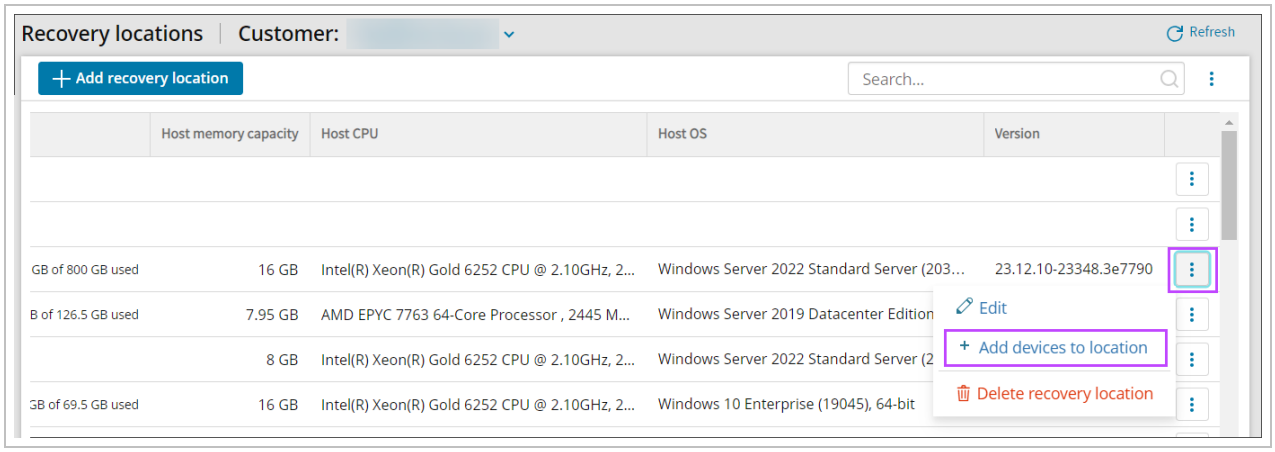
1. Right-click on the Recovery Location to add the device to
2. Select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
    a. Enable Standby Image to AzureDevices cannot be added to a Standby Image plan if already assigned to a Recovery Testing plan.Devices can be assigned to multiple Standby Image plans at once, i.e. Standby Image to Hyper-V and Standby Image to Azure. From Main DashboardTo enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:Log in to the Management Console under a SuperUser or Manager account In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan toClick Add to recovery plan from the Toolbar Select Standby Image (Azure)Select the customer the device(s) you wish to apply the Standby Image plan belong toChoose the recovery location as was configured in Add Recovery LocationsIf the selected customer does not have any locations, you must add one before continuing by selecting Add recovery location. See Add Recovery Locations for full details of adding a location.It is not possible to assign a location for which the Host availability is "Offline"Click NextConfirm the device selected from the Dashboard is compatible and click Next Enter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereClick Next to continueChoose the boot check frequency:OffEvery recovery sessionDailyWeeklyBiweeklyMonthlyIf you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Once connected, click NextClick Azure VM settings towards the right-hand side of the screen to open the settings configuration window:Configure the Azure VM Settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk typeData disk(s) typeVirtual NetworkSubnetAssign NSG and public IPDuring the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend blocking internet access for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.Click Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowConfirm assigning the plan to the device(s)Wait for the plan to be assigned until you see a confirmation banner on the pageClick FinishFrom Standby Image OverviewLog in to the Management Console under a SuperUser or Manager accountNavigate to Continuity > Standby ImageClick Add to PlanSelect Standby Image (Azure)You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the planRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding:
    b. Top bar menu
    c. Top bar menu

Right-hand menu

1. Click the action menu button for the Recovery Location, seen as three dots in a vertical line to the right of the location's version
2. Select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
    a. Enable Standby Image to AzureDevices cannot be added to a Standby Image plan if already assigned to a Recovery Testing plan.Devices can be assigned to multiple Standby Image plans at once, i.e. Standby Image to Hyper-V and Standby Image to Azure. From Main DashboardTo enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:Log in to the Management Console under a SuperUser or Manager account In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan toClick Add to recovery plan from the Toolbar Select Standby Image (Azure)Select the customer the device(s) you wish to apply the Standby Image plan belong toChoose the recovery location as was configured in Add Recovery LocationsIf the selected customer does not have any locations, you must add one before continuing by selecting Add recovery location. See Add Recovery Locations for full details of adding a location.It is not possible to assign a location for which the Host availability is "Offline"Click NextConfirm the device selected from the Dashboard is compatible and click Next Enter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereClick Next to continueChoose the boot check frequency:OffEvery recovery sessionDailyWeeklyBiweeklyMonthlyIf you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Once connected, click NextClick Azure VM settings towards the right-hand side of the screen to open the settings configuration window:Configure the Azure VM Settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk typeData disk(s) typeVirtual NetworkSubnetAssign NSG and public IPDuring the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend blocking internet access for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.Click Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowConfirm assigning the plan to the device(s)Wait for the plan to be assigned until you see a confirmation banner on the pageClick FinishFrom Standby Image OverviewLog in to the Management Console under a SuperUser or Manager accountNavigate to Continuity > Standby ImageClick Add to PlanSelect Standby Image (Azure)You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the planRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding:
    b. Top bar menu
    c. Top bar menu

Recovery Reports

When the device(s) assigned to the plan have **Successful recovery report email** or **Failed recovery report email** recipient

address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox.

Here is an example report with Cove branding:

Cove Data Protection

Recovery completed

Recovery plan: **Standby Image (Hyper-V)**

Last recovery session completed successfully: April 13 2024 9:15:32 PM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Workstation
Operating system	Windows 10 Enterprise (19045), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 13 2024 9:15:32 PM
Recovery status	Completed
Recovery duration	1 hour, 2 minutes and 11 seconds
Recovery location	
Storage location	D:\
Restore frequency	Each backup session
Recovery plan	Standby Image (Hyper-V)

BACKUP DETAILS USED FOR THE RESTORE

Backup session time	April 13 2024 8:45:28 PM
Backup status	Completed

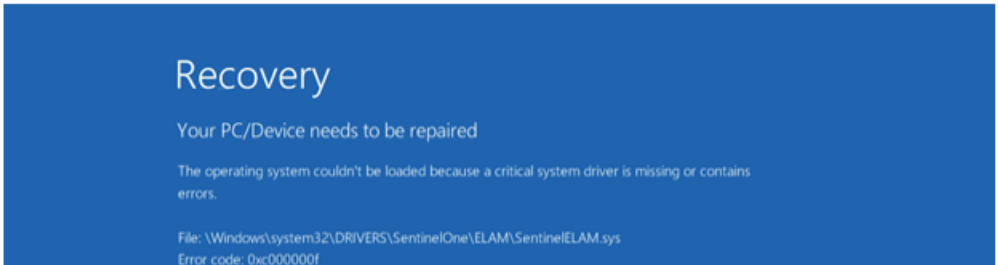
DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

BOOT TEST OVERVIEW

Screenshot verification	Completed
Boot time	April 13 2024 9:15:32 PM
Backup session time	April 13 2024 8:45:28 PM
Boot check frequency	Each recovery session

Below is a screenshot of the virtual machine created during the boot phase of recovery.



Here is an example **without** Cove branding:

Recovery completed

Recovery plan: **Standby Image (Hyper-V)**

Last recovery session completed successfully: April 16 2024 3:45:28 AM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Workstation
Operating system	Windows 10 Enterprise (19045), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 16 2024 3:45:28 AM
Recovery status	Completed
Recovery duration	1 hour, 13 minutes and 6 seconds
Recovery location	Hyper-V.OaNaB
Storage location	D:\
Restore frequency	Each backup session
Recovery plan	Standby Image (Hyper-V)

BACKUP DETAILS USED FOR THE RESTORE

Backup session time	April 16 2024 3:35:44 AM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

BOOT TEST OVERVIEW

Screenshot verification	Not applicable
Boot check frequency	Off

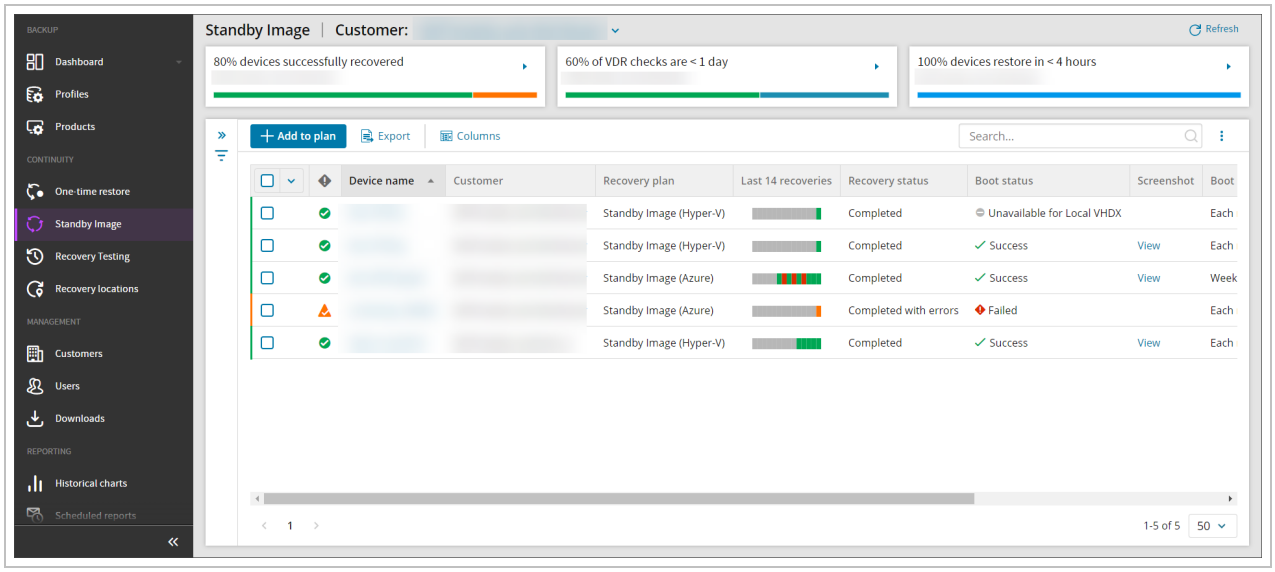
Screenshot verification is not applicable

Monitor Standby Image Devices

From the Management Console, you can view the dedicated Standby Image Overview by selecting **Continuity** > **Standby Image** from the vertical menu on the left hand side.

This page will list devices assigned to the Standby Image plans:

- Standby Image to Hyper-V
- Standby Image to Azure
- Standby Image to ESXi



From this dashboard, you will see a specified set of columns detailing information relevant to devices using the Standby Image plan, including the continuity history of the last 14 recoveries, the recovery status, boot status, and plan assigned, along with some other information.

If no devices are assigned to either Standby Image plan, the dashboard will display a message to advise, along with a button to add devices to a plan.

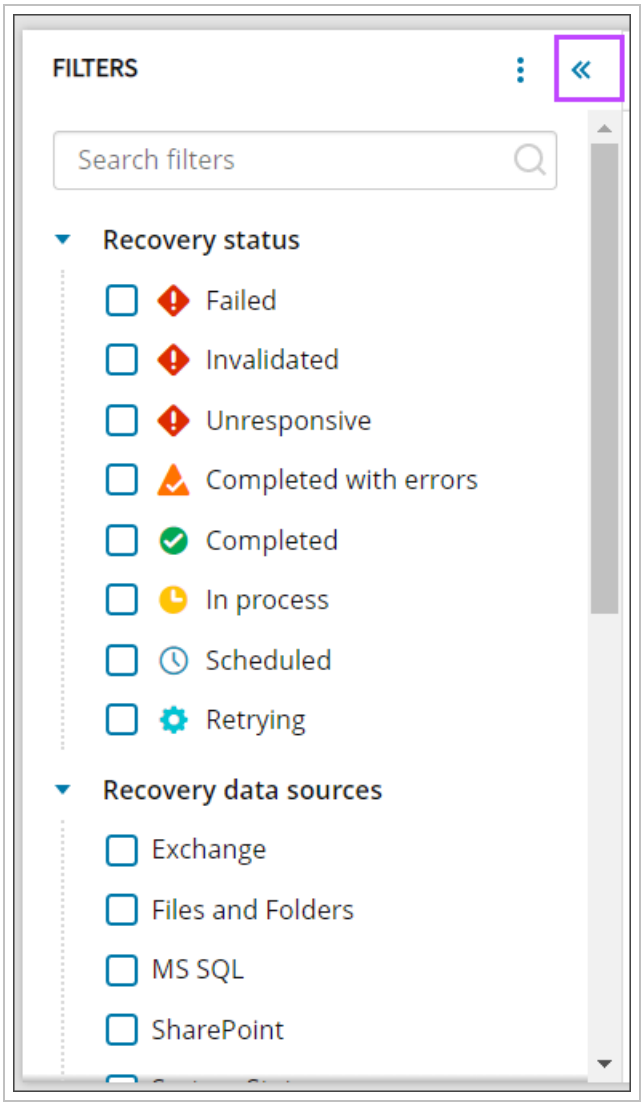
> If a device is assigned to **multiple** plans (i.e. **Standby Image to Hyper-V**, **Standby Image to Azure** and **Standby Image to ESXi**), the device will be listed for each instance of a plan and can be told apart by the **Recovery Plan** column.

Searching

Searching within the Standby Image overview can be done by using the search box over to the right hand side of the page, just above the devices list. The search can be performed by any text field.

Filtering

The Standby Image overview also includes functionality to filter devices using the filter menu to the left of the device list and can be displayed or hidden by clicking the double arrows.



From this menu, you can filter by:

Recovery status

- **Failed** - The recovery session has failed
- **Invalidated** - Device was moved to an inappropriate partner and so the session has failed
- **Unresponsive** - The recovery session was initiated but did not receive updates for at least 30 minutes because the recovery location restarted or was offline.
- **Completed with errors** - The recovery session completed, but encountered errors
- **Completed** - The recovery session completed with no errors
- **In process** - The recovery is currently in progress
- **Scheduled** - Devices just added to a recovery plan and are waiting for their first recovery session or devices where restores were paused and have since been resumed will display as scheduled
- **Retrying** - A restore session was not finished so the system is trying the restore again

Recovery data sources

- Exchange
- Files and Folders
- MS SQL
- SharePoint
- System State

Recovery session statistics

- Boot check frequency
  - Off
  - Every recovery session
  - Daily
  - Weekly
  - Biweekly
  - Monthly
- Boot Check Status
  - Success
  - Failed
  - Off
  - Unavailable for Local VHDX
- Continuous restores
  - Running
  - Paused
- Duration of the last completed recovery session
  - Sliding scale from 0 to unlimited

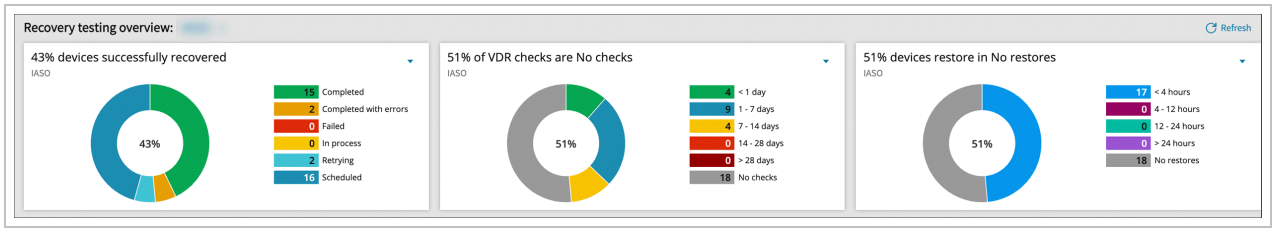
  in minutes
- Number of errors of the last completed recovery session
  - Sliding scale from 0 to unlimited
- Number of restored files
  - Sliding scale from 0 to unlimited
- Number of selected files
  - Sliding scale from 0 to unlimited
- Recovery Location name
  - Select the recovery location from a dropdown
- Recovery Plan
  - Standby Image (Hyper-V)
  - Standby Image (ESXi)
  - Standby Image (Azure)
- Restored size
  - Sliding scale from 0 to unlimited

  in KB and GB

- Recovery testing status of the last completed recovery session
  - Failed
  - Completed with errors
  - Completed
- Screenshot
  - Available
  - Not Available
- Selected size
  - Sliding scale from 0 to unlimited
  in KB and GB
- Timestamp of the last completed recovery session
  - Quick Picks of:
    - Last day
    - 1 - 7 days
    - 7 - 14 days
    - 14 - 28 days
    - > 28 days
  - Custom range, select a stat date and time and an end date and time

Widgets

Three widgets can be maximized at the top of the page, which allow for further filtering:



Device recovery status

This widget allows you to filter the devices by recovery status:

- Completed
- Completed with errors
- Failed
- In process
- Retrying
- Scheduled

VDR checks time frame

This widget allows you to see the percentage of devices whose recovery check completed within the following day ranges:

- < 1 day
- 1 - 7 days
- 7 - 14 days
- 14 - 28 days
- > 28 days
- No checks

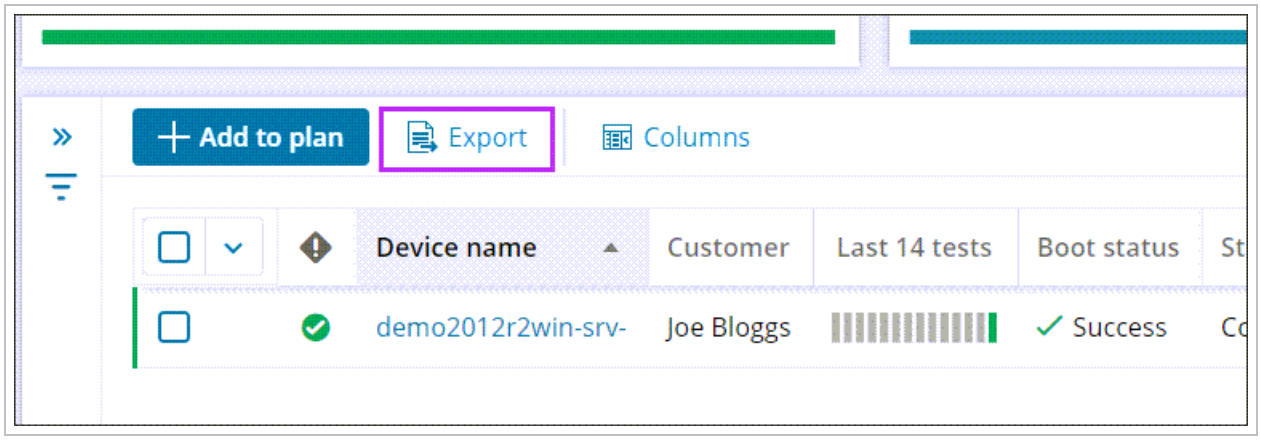
Device restore time frame

From this widget, you can filter devices by the how recent restores are done by the following time frames:

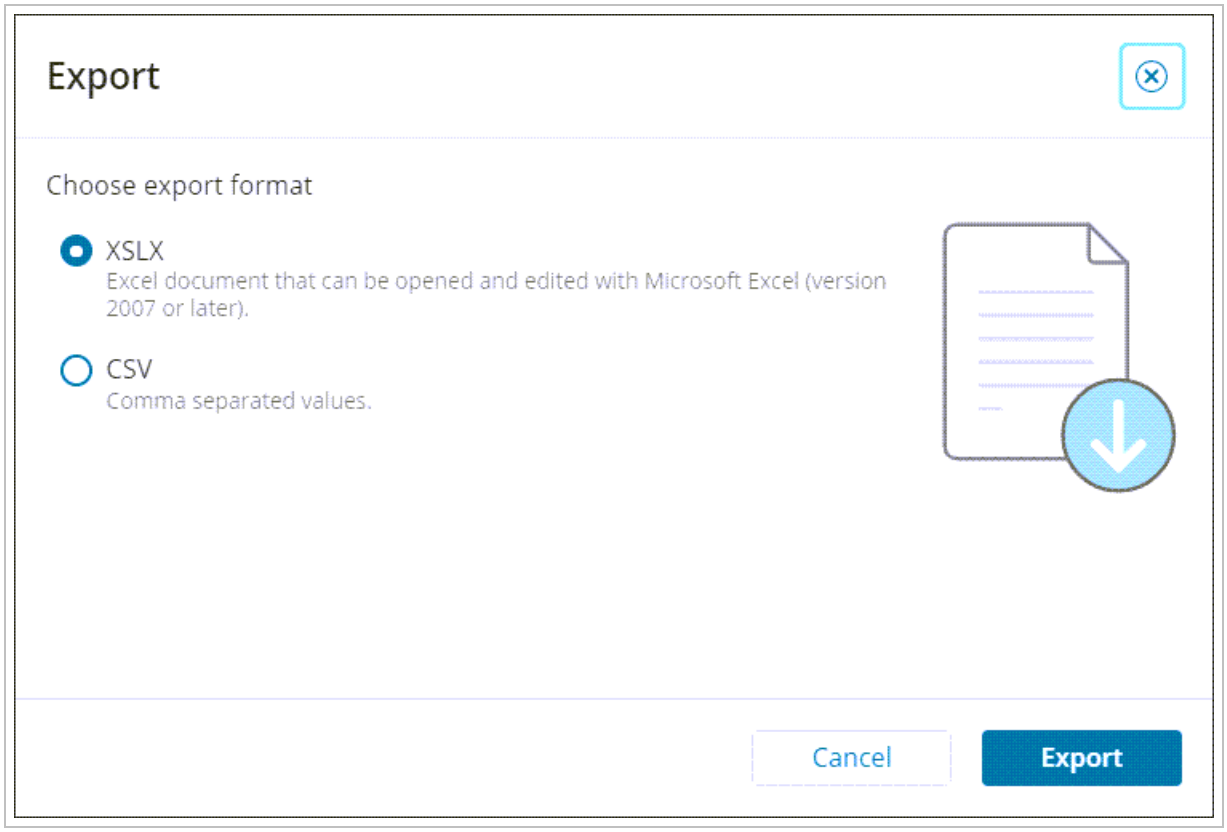
- < 4 hours
- 4 - 12 hours
- 12 - 24 hours
- > 24 hours
- No restores

Exporting

You may export a list of devices currently assigned a plan by clicking **Export**

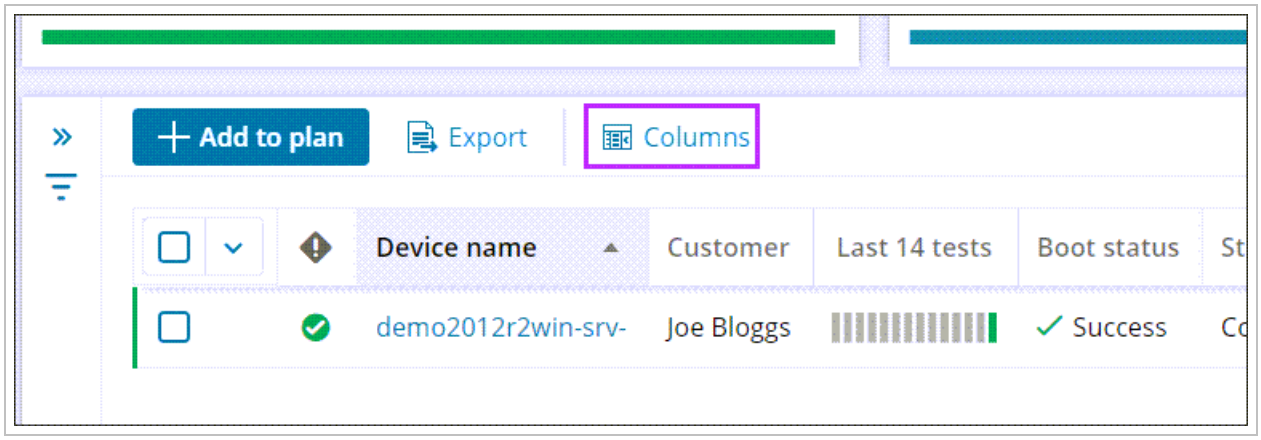


This will then provide a separate dialog where you can choose to export in either XSLX or CSV.

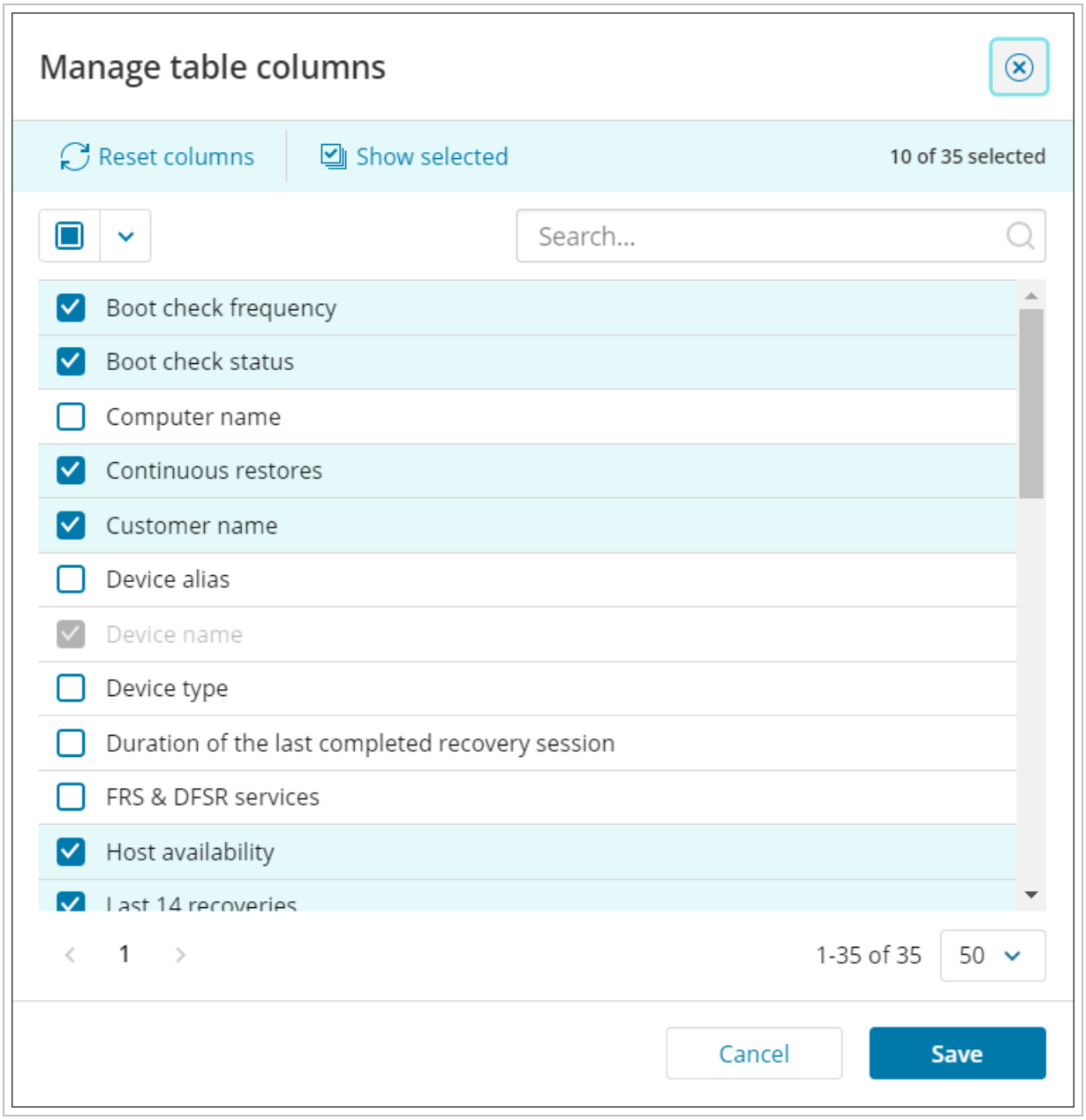


Manage Table Columns

Management Console allows you to manage the tables columns that can be seen within the Standby Image overview.



In the Manage table columns dialog, you can select and deselect columns based on the information you wish to view from the overview.

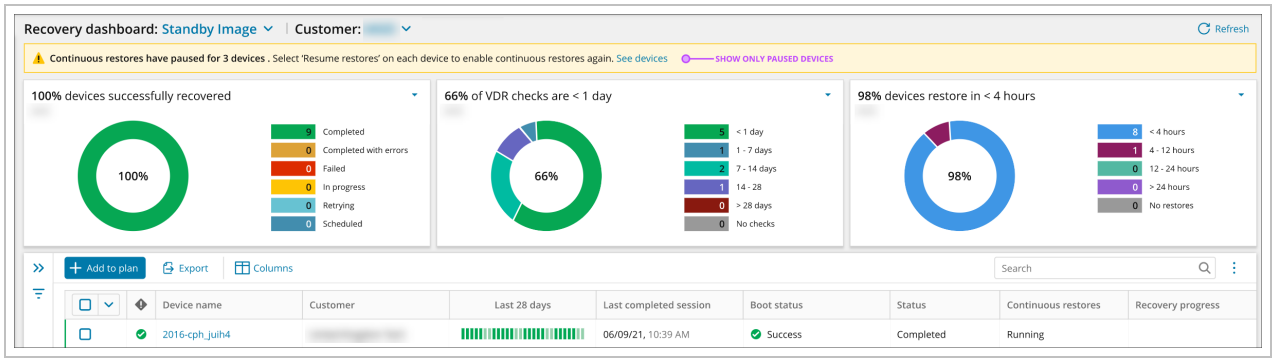


Pause Standby Image recovery

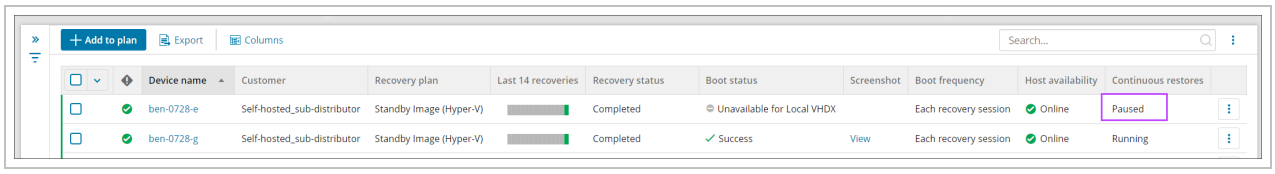
Once a Standby plan has been assigned to a device, the continuous restores can be paused and restarted. Pause or resume restores functionality there to provide a possibility to use the restored machine for failover in case of disaster.

> If a restored Virtual Machine is turned on manually, the Standby Image restore will automatically pause.

Pausing and restarting continuous restores can done be for single or multiple devices at a time. Once devices have been paused, a banner will be displayed at the top of the page to advise.

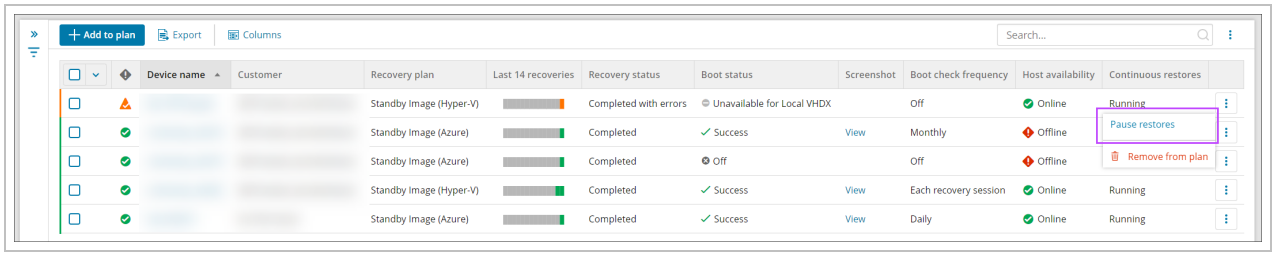


Click **See devices** to filter the devices list by **Continuous Restore: Paused** to only devices which are currently paused.



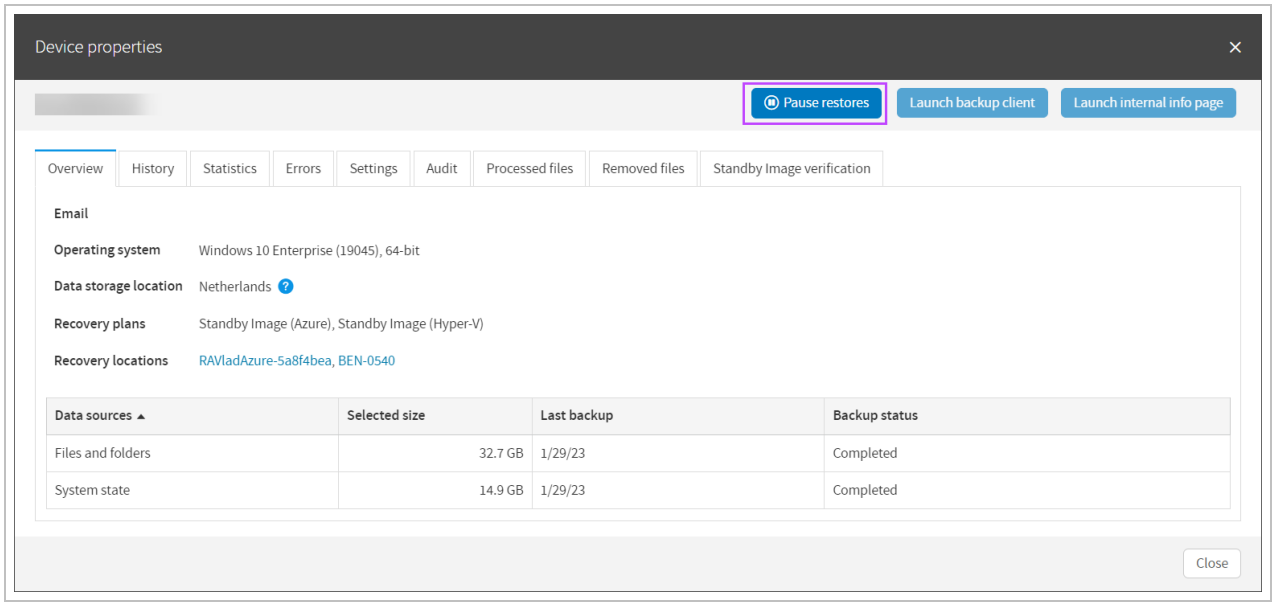
For single devices

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Click the menu action button to the right of the device (Three vertical dots)
4. Select **Pause Restores** or **Resume Restores**



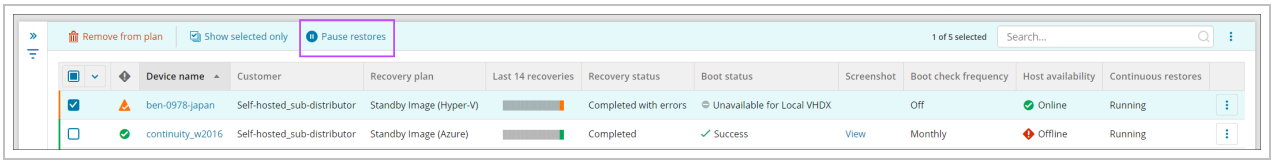
> This will differ depending on whether the plan is currently active, or has been paused already

It is also possible to pause restores from the Device Properties window:



For single or multiple devices

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Tick the checkbox for any devices that need paused from the list
4. In the top panel, select **Pause Restores** or **Resume Restores**



> This will differ depending on whether the plan is currently active, or has been paused already

Accessing device properties

The Device Properties window displays several tabs detailing information on the Backup device. Full details of the contents of each tab can be found on the Device management in Management Console page.

The two that are the most commonly used with Standby Image are the **Settings** tab and the **Standby Image Verification** tab.

Settings Tab

Broken into several sections, this tab contains:

General

This section provides the main device details:

- **customer** - Who device belongs to, can be changed to move the device to a different customer
- **Device name** - Cannot be changed

- **Installation key** - Cannot be changed
- **Creation date** - Cannot be changed
- **Expires on** - Can be amended to a date in the future, or set to **'no expiration'** if required

> You may also see the Request Passphrase button here if the device is set up to use this instead of its own security code/encryption key

Backup

This section contains:

- **Backup product** - Use the dropdown to change the Product used by the device
- **Profile** - Use the dropdown to change the Profile applied to the device

Recovery

On a device assigned to the Standby Image plan, this section will allow you to see plan in use and amend some details of this:

- **Recovery Plan** - Standby Image (Each backup session)
- **Recovery Location** - Cannot be changed from this panel. To change this, see Add Device to Recovery Location
- **Successful recovery report email** - Specify the email address(es) that will receive reports when the most recent Recovery as per the assigned plan has been successful
- **Failed recovery report email** - Specify the email address(es) that will receive reports when the most recent Recovery as per the assigned plan has failed
- **Remove Cove branding** - toggle branding of the email reports on or off
- **Restore format** - This option will not be available for Standby Image to Azure.
  - For **Standby Image to Hyper-V**, this is a choice between **Hyper-V** or **Local VHDX**
  - For **Standby Image to ESXi**, this is a choice between **ESXi** and Local **VHDX**

    > Further settings displayed are dependent on the Restore Format selected for the device. These settings can be changed as required.

> All Recovery Plans associate to the device will be included here, and can be minimized or expanded by clicking the arrow to the left of the plan name.

Device properties

Launch backup client | Launch internal info page

Overview | History | Statistics | Errors | Settings | Audit | Processed files | Removed files | Standby Image verification

General

Customer

Device name

Installation key

Creation date 2/21/23

Expires on 04/18/24 No expiration

Backup

Product _test

Profile -servers

Recovery

Standby Image (ESXi)

Recovery plan Standby Image (ESXi)

Recovery location ESXiRA

Successful recovery report email e.g email@email.com

Failed recovery report email e.g email@email.com

Remove Cove branding OFF

Restore format ESXi VMDK

Boot check frequency Daily

FRS and DFSR services OFF

Local Speed Vault OFF

CPU cores 4

RAM (GB) 4

VM Subnet mask Enter a custom subnet mask to the new virtual mac

VM gateway Enter a custom gateway to the new virtual machine

VM DNS server Enter a DNS server to be used on the restored mach

Separate multiple DNS servers with a comma or semicolon

VM IP address Enter a custom IP address to the new virtual machir

Standby Image (Hyper-V)

Recovery plan Standby Image (Hyper-V)

Recovery location BEN-6478

Successful recovery report email e.g email@email.com

Failed recovery report email e.g email@email.com

Remove Cove branding OFF

Restore format Hyper-V Local VHDX

Boot check frequency Daily

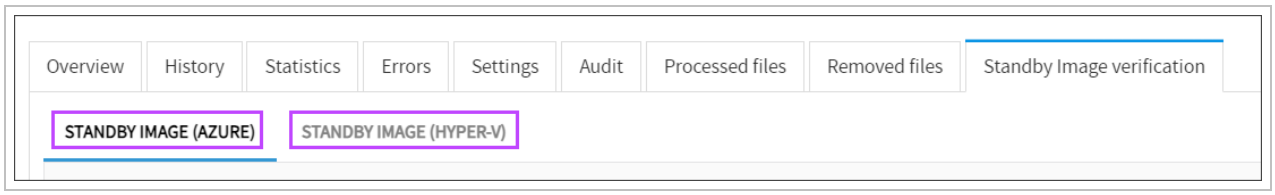
FRS and DFSR services OFF

Local Speed Vault OFF

Standby Image Verification Tab

To view statistics of the Standby Image and check the screenshots to ensure this has been successful, you can view this by following one of the below methods.

All plans associated to the device will have their own sub-tabs that can be selected to view the appropriate screenshot:



From Device Properties

1. Log in to the Management Console
2. Click the device name on either the Backup Dashboard or the Standby Image overview to open the Device Properties
3. Navigate to the **Standby Image Verification** tab

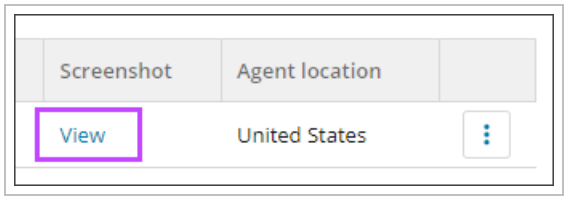
From Standby Image Overview

The Standby Image Verification tab can be viewed from the Standby Image overview in one of two ways:

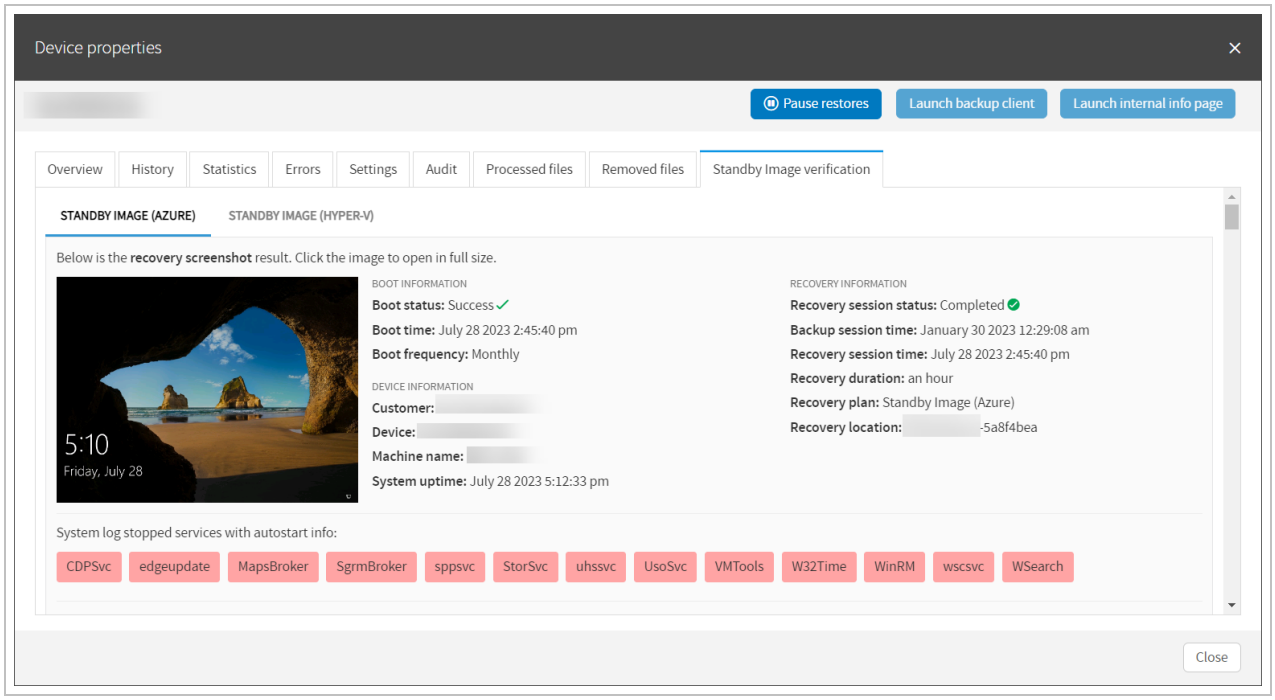
- Via theScreenshot column
- Via the Last 14 recoveries column

Screenshot column

1. Log in to the Management Console
2. Navigate to **Continuity** > **Standby Image**
3. Click **View** under the Screenshot column

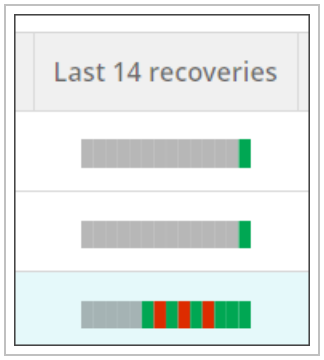


4. This will take you in to the Device Properties dialogue, where you will now see the **Standby Image Verification** tab:

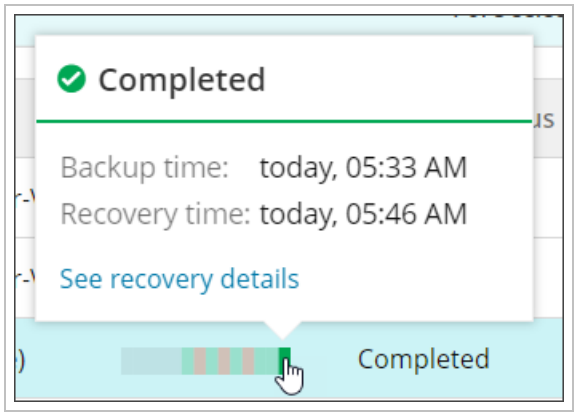


Last 14 recoveries column

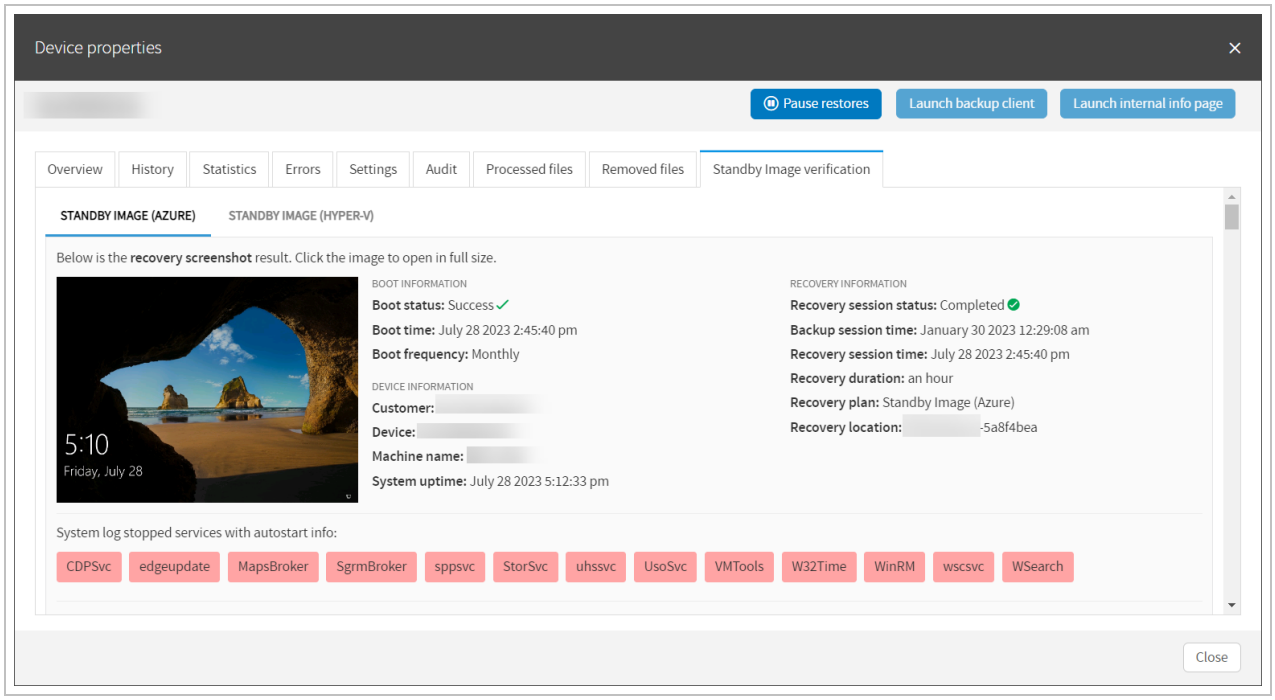
1. Log in to the Management Console
2. Navigate to **Continuity** > **Standby Image**
3. Hover your mouse over the most recent colored bar in the Last 14 recoveries column



4. Click **See recovery details** in the popup box that appears



5. This will take you in to the Device Properties dialogue, where you will now see the **Standby Image Verification** tab:



Standby Image to Azure

Cove Data Protection (Cove)'s Standby Image to Azure service runs a continuous restore of your data to Microsoft Azure and boots based on the frequency set during configuration of the plan.

> Devices **can** be assigned to **multiple Standby Image plans** at once, i.e. Standby Image to Hyper-V *and* Standby Image to Azure *and* Standby Image to ESXi.

Standby Image Data Restored:

Standby Image restores the following data sources:

- System State
- Files and Folders
- Exchange
- SharePoint
- MS SQL

Requirements

- Backup Manager version 17.4 and above
- The target VM **must** have access to Azure storage in order to successfully perform boot test
- A pre-created virtual network and subnet in the Azure resource group where you plan to do the restore
- The Recovery Location VM **must** be assigned the **Owner role** in the **Azure resource group** where you are placing standby image
- The Recovery Location VM **must** be assigned the **Owner role** for the **resource group of the Virtual Network** being used for the restore

What's inside:

Enable Standby Image to Azure

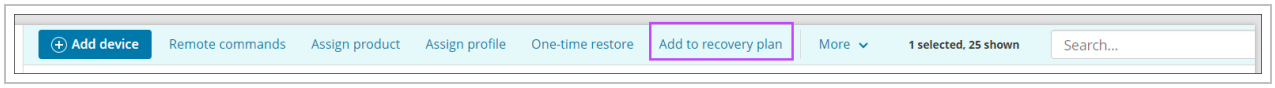
> Devices **cannot** be added to a **Standby Image plan** if already assigned to a **Recovery Testing plan**.

> Devices **can** be assigned to **multiple Standby Image plans** at once, i.e. Standby Image to Hyper-V *and* Standby Image to Azure.

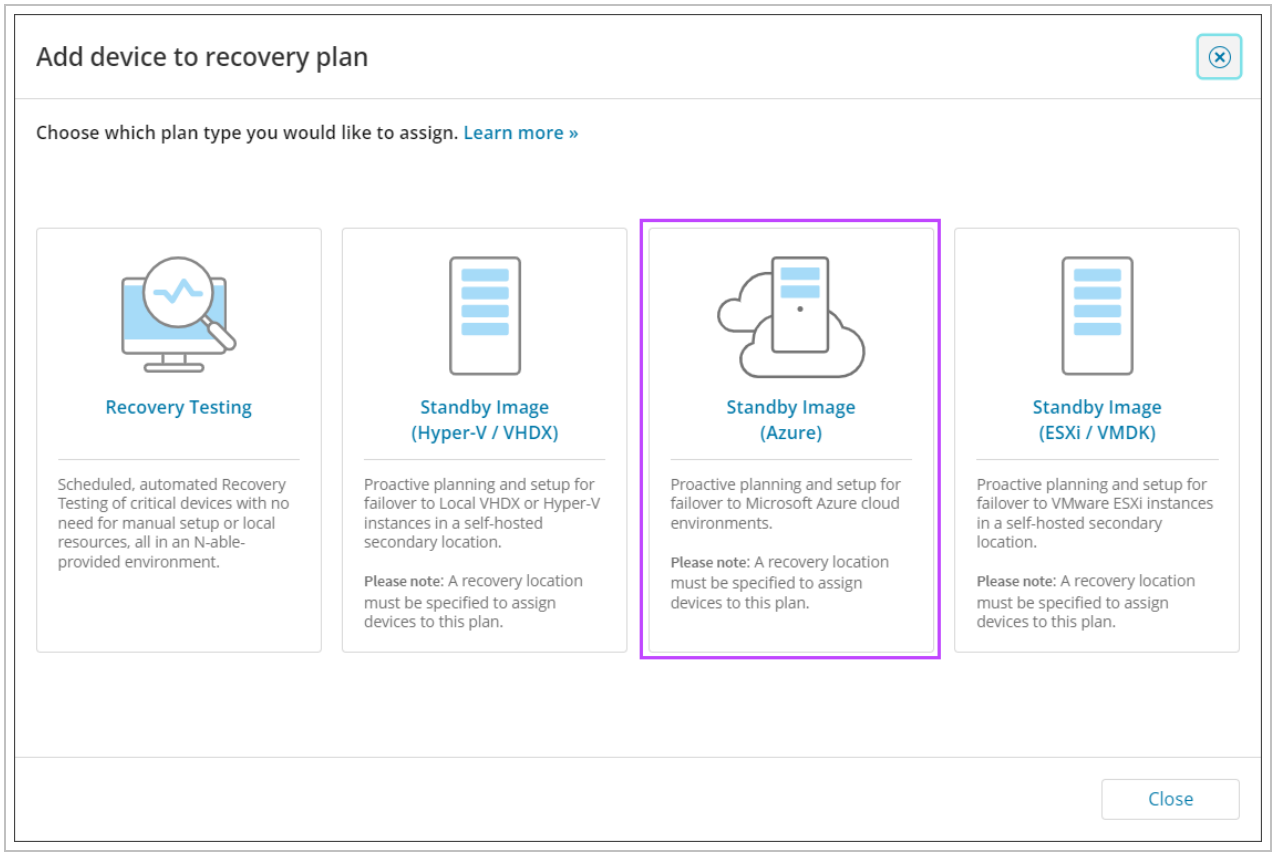
From Main Dashboard

To enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan to
3. Click **Add to recovery plan** from the Toolbar



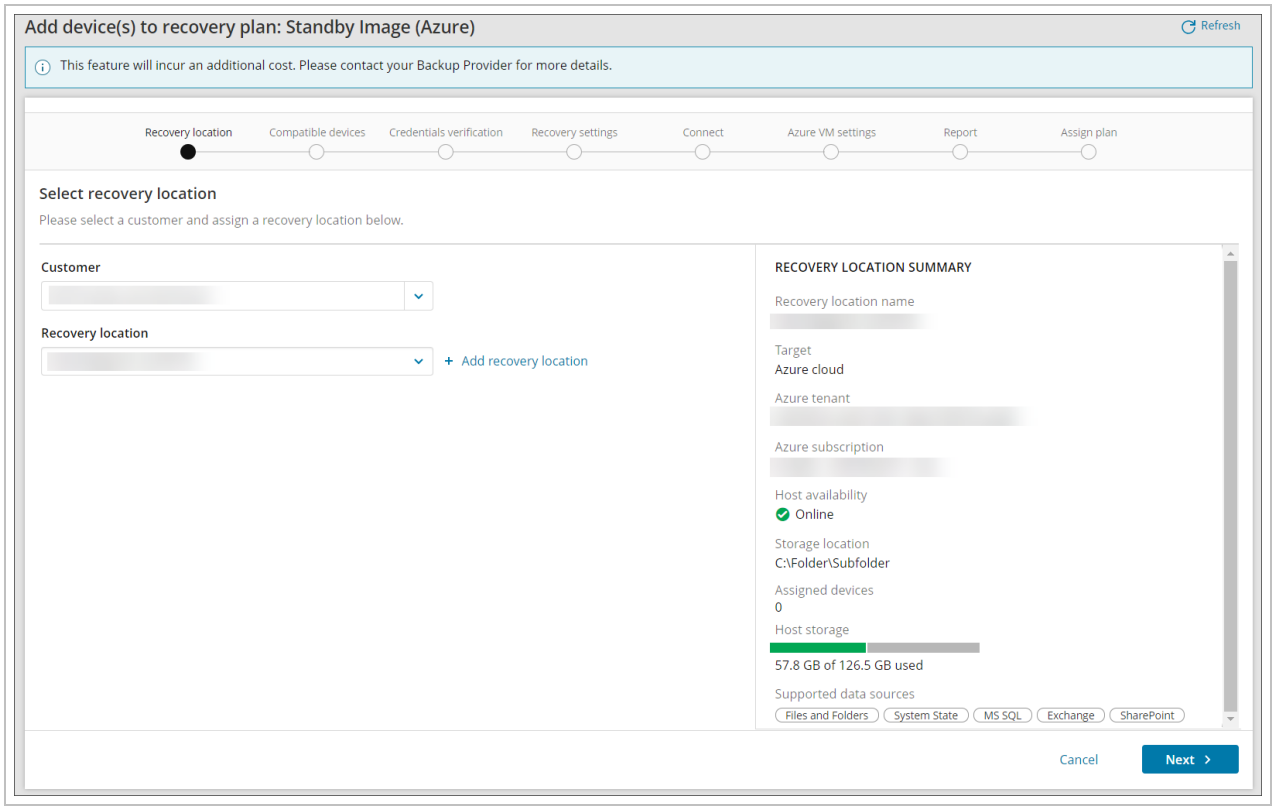
4. Select **Standby Image (Azure)**



5. Select the customer the device(s) you wish to apply the Standby Image plan belong to

6. Choose the recovery location as was configured in Add Recovery Locations

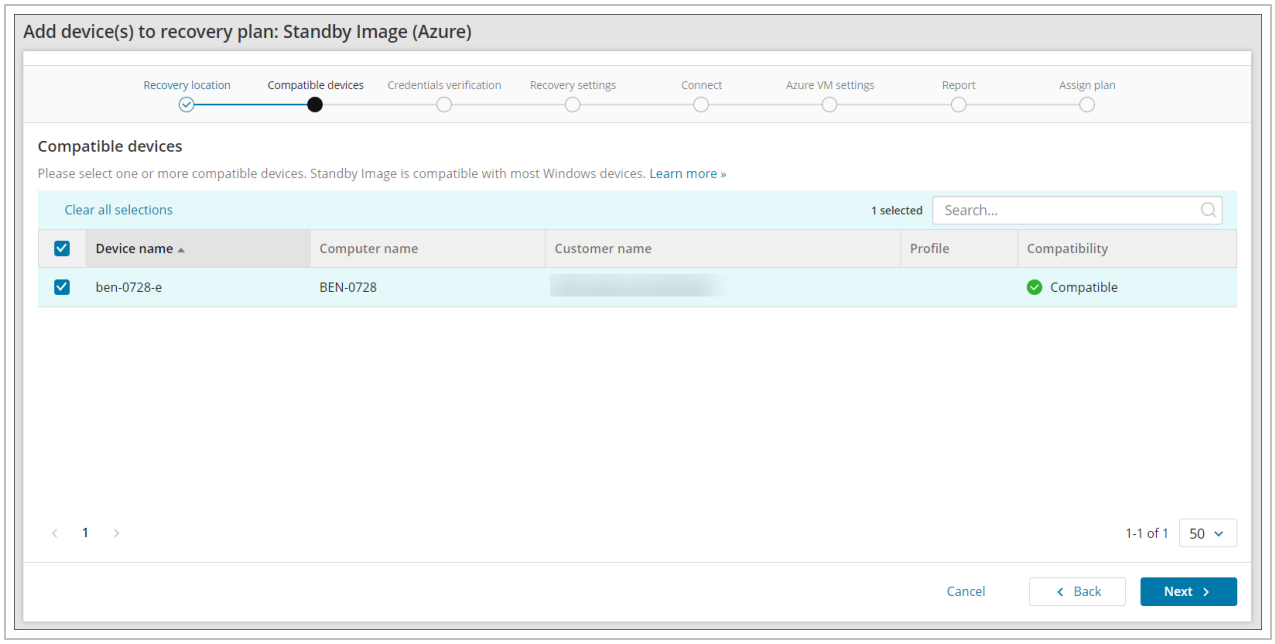
> If the selected customer does not have any locations, you must add one before continuing by selecting **Add recovery location**. See Add Recovery Locations for full details of adding a location.



> It is not possible to assign a location for which the **Host availability** is "**Offline**"

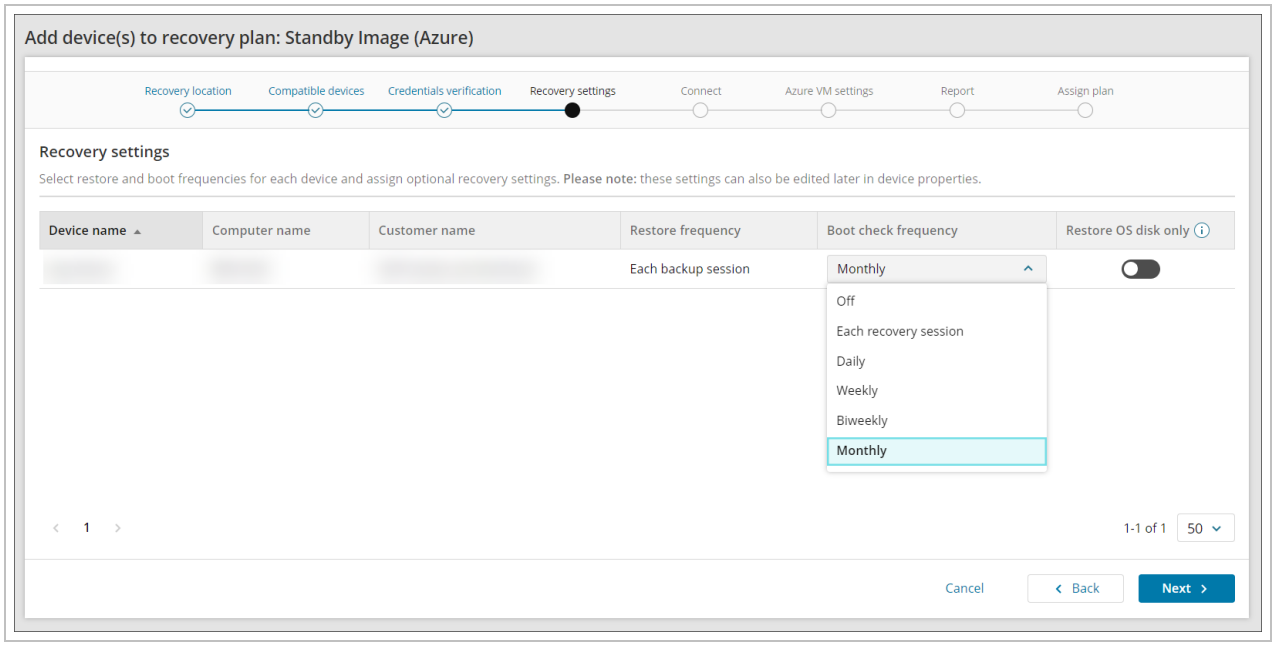
7. Click **Next**

8. Confirm the device selected from the Dashboard is compatible and click **Next**

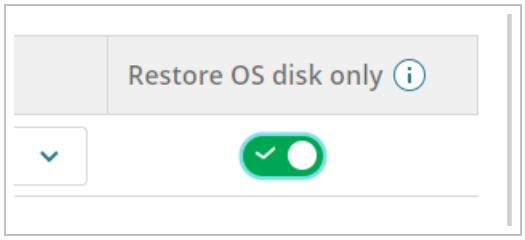


9. Enter the security code/encryption key or passphrase for the device(s). This can be either:
   - **Private encryption key** - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryption
   - **Passphrase encryption** - These are generated on demand for automatically installed devices. You can find information on this here
10. Click **Next** to continue

11. Choose the boot check frequency:
    - Off
    - Every recovery session
    - Daily
    - Weekly
    - Biweekly
    - Monthly



12. If you wish to skip all data drives, enable **Restore OS disk only**



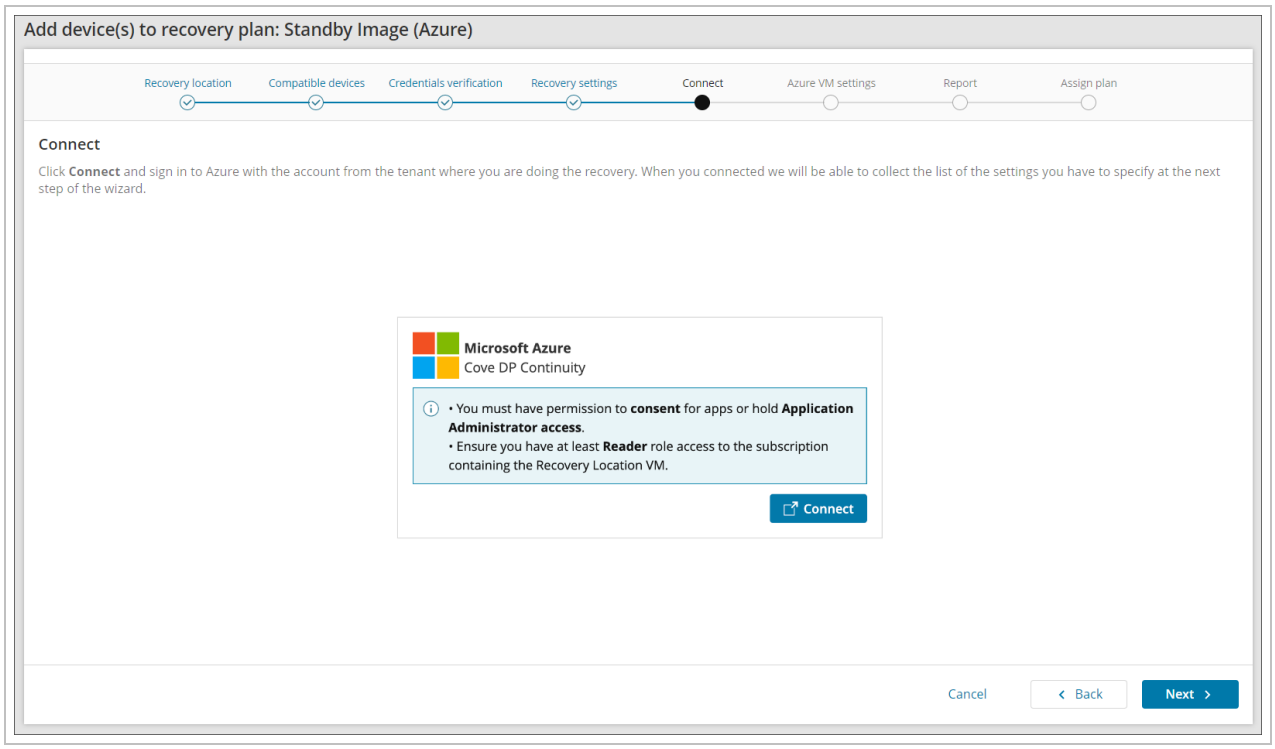
> Enabling **Restore OS disk only** will help to speed up restores as the only thing being restored is the Operating System

13. Click **Next**

14. Connect to Microsoft Azure by either:
    a. Allow permissions to the Azure user account to **consent for apps** access,

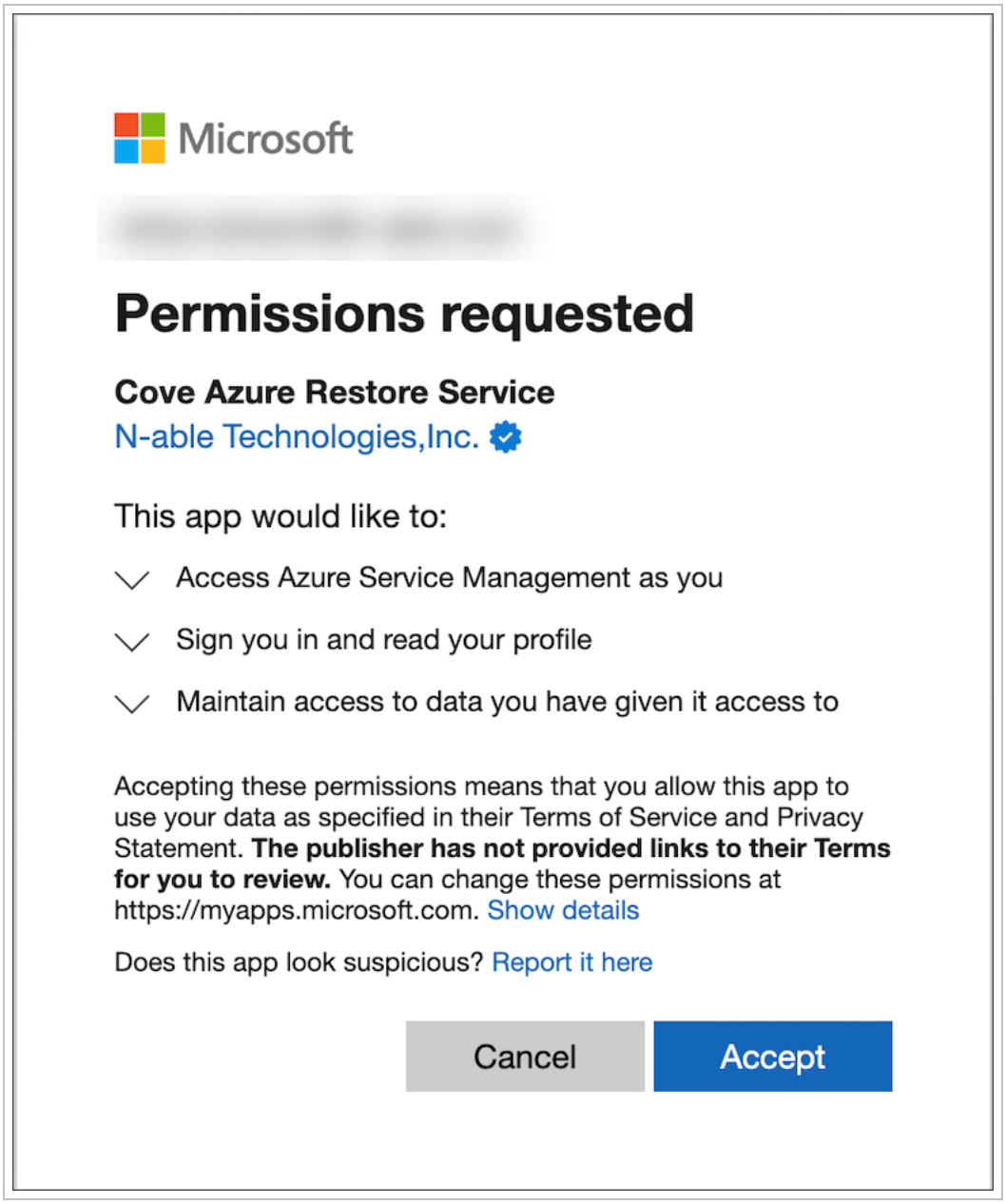
or;

    a. Login using Application Administrator access



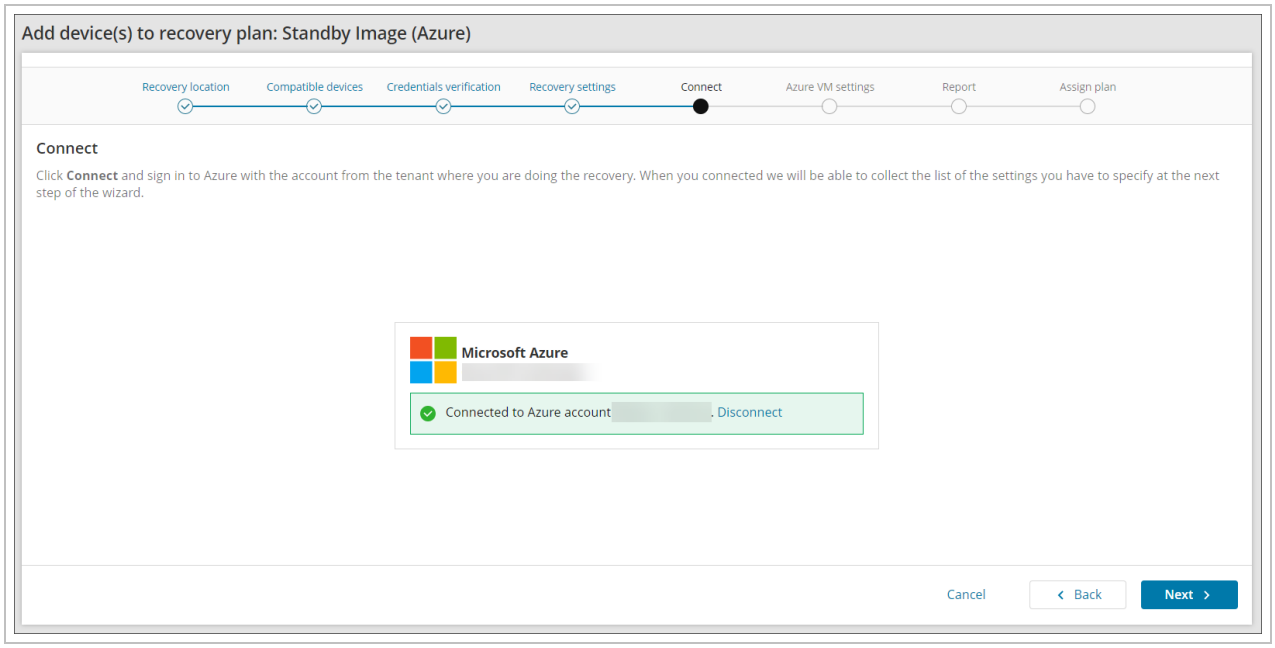
> Ensure you have at minimum **Reader** role access to the subscription containing the Recovery Location VM

b. Accept the required permissions



If you do not see the authentication page, make sure your browser is not blocking pop-up windows.

15. Once connected, click **Next**



16. Click **Azure VM settings** towards the right-hand side of the screen to open the settings configuration window:

17. Configure the **Azure VM Settings:**

AZURE VM SETTINGS

Subscription

Resource group

Virtual machine name

Region

West Europe

Availability options

VM size

OS disk type

Premium SSD

Data disk(s) type

Premium SSD

Virtual network

Subnet

default

Assign NSG and public IP

- Subscription

  > This cannot be changed as the subscription is set in the **Recovery Location** configuration

- Resource Group
- Virtual Machine name
- Region

  > This cannot be changed as the subscription is set in the **Recovery Location** configuration

- Availability options
- VM size

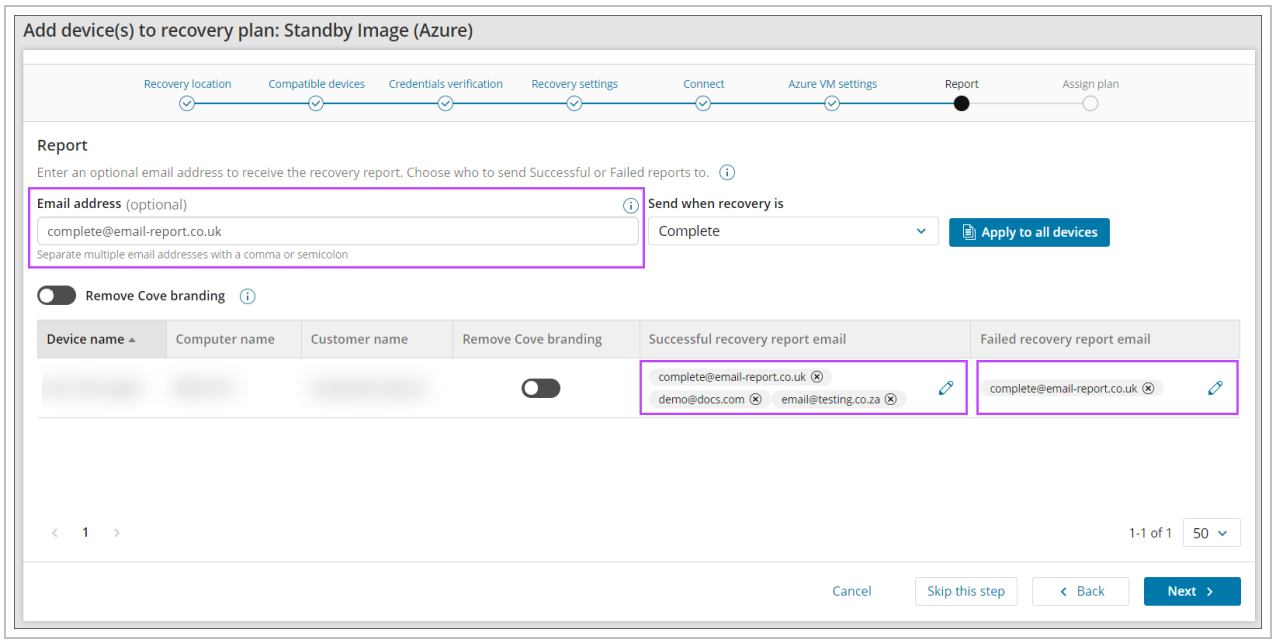
  > If the **VM size** selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either **increase** the **regional vCPU quota** on the Subscription, or **decrease** the **VM size** selected in the Azure VM Settings.

- OS disk type
- Data disk(s) type
- Virtual Network
- Subnet
- Assign NSG and public IP

> During the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend **blocking internet access** for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.

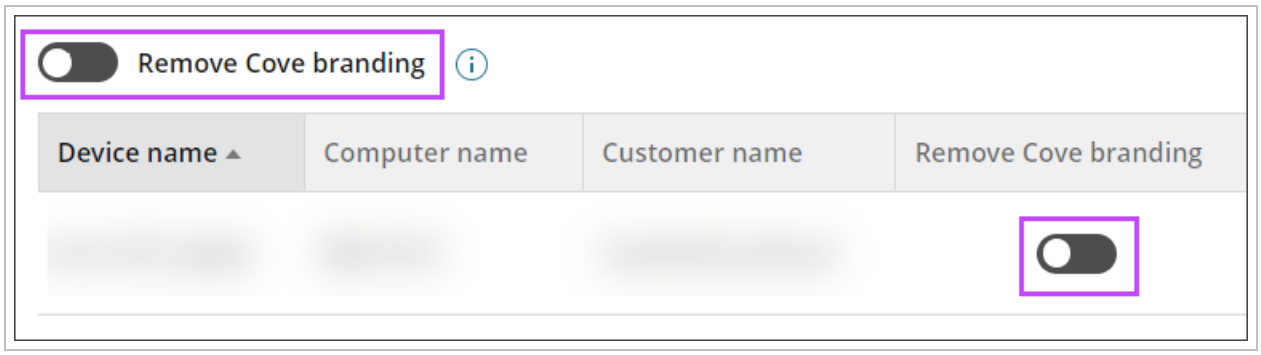
18. Click **Next** to progress to the **Report** window to enter one or more email addresses to receive a report when:
    a. The recovery is complete (Successful or Failed)
    b. The recovery was successful
    c. The recovery failed

> Multiple addresses should be separated using a comma or semi-colon



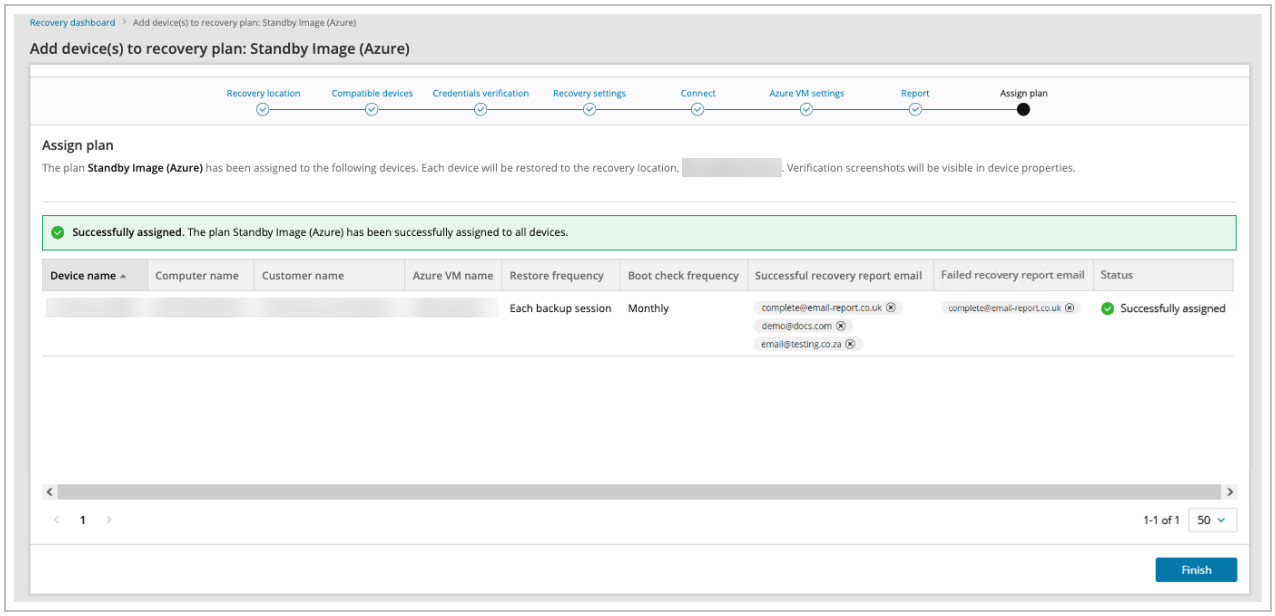
> If you do not want to add an email address to receive reports, click **Skip this step**

19. To remove all branding from the reports, use the **Remove Cove branding** toggle per device, or above the device list to apply the changes to all devices in this window



20. Confirm assigning the plan to the device(s)

21. Wait for the plan to be assigned until you see a confirmation banner on the page

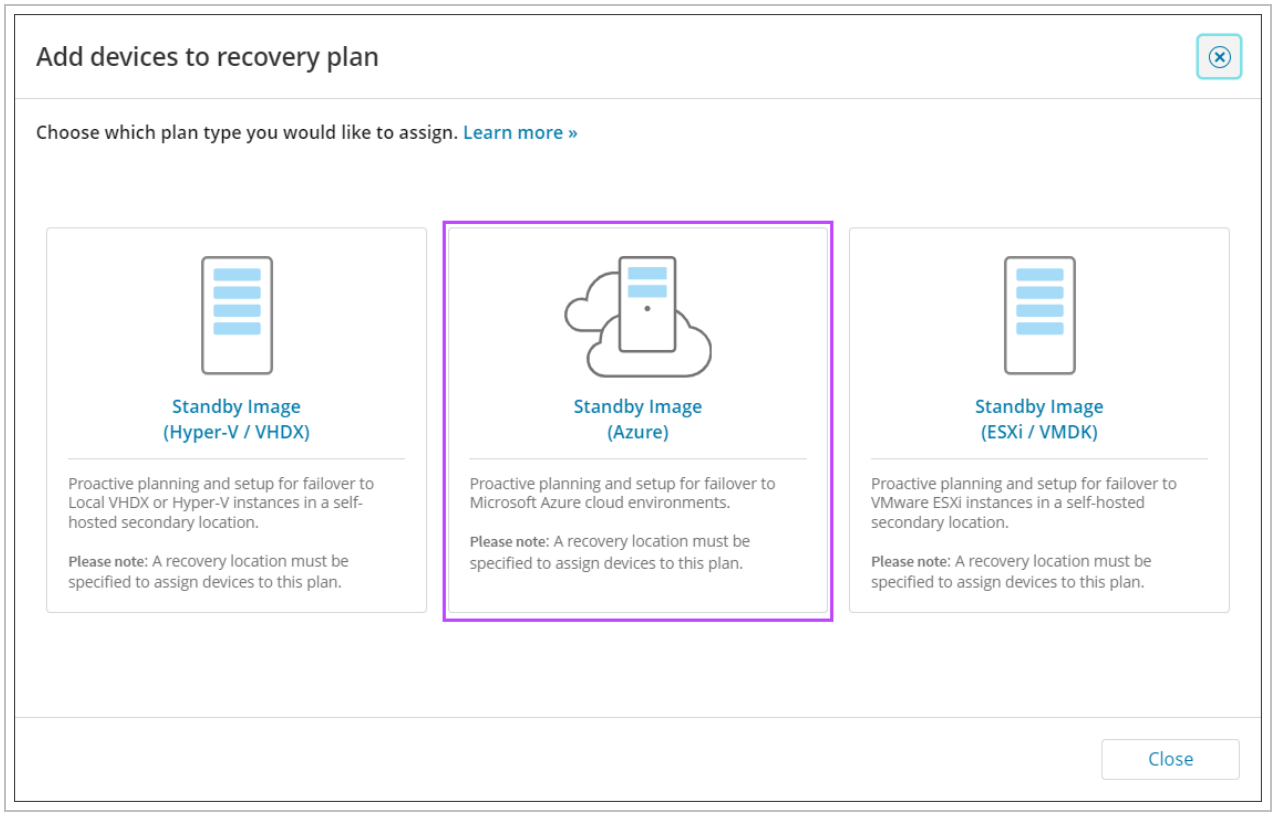


22. Click **Finish**

From Standby Image Overview

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Click **Add to Plan**

4. Select **Standby Image (Azure)**



5. You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the plan

Recovery Reports

When the device(s) assigned to the plan have **Successful recovery report email** or **Failed recovery report email** recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox.

Here is an example report **with** Cove branding:

Cove Data Protection

Recovery completed

Recovery plan: **Standby Image (Azure)**

Last recovery session completed successfully: April 05 2023 2:16:28 AM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Workstation
Operating system	Windows 10 Pro (19044), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 05 2023 2:16:28 AM
Recovery status	Completed
Recovery duration	1 minute and 57 seconds
Recovery location	pt-az-recovery-agent-1-0e70b668
Boot frequency	Each recovery session
Restore frequency	Each backup session
Recovery plan	Standby Image (Azure)
Screenshot verification	Completed

BACKUP DETAILS USED FOR THE RESTORE

Backup session time	April 05 2023 2:01:02 AM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

Below is a screenshot of the virtual machine created during the boot phase of recovery.

Here is an example **without** Cove branding:

Recovery completed

Recovery plan: **Standby Image (Azure)**

Last recovery session completed successfully: April 05 2023 2:16:28 AM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Workstation
Operating system	Windows 10 Pro (19044), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 05 2023 2:16:28 AM
Recovery status	Completed
Recovery duration	1 minute and 57 seconds
Recovery location	pt-az-recovery-agent-1-0e70b668
Boot frequency	Each recovery session
Restore frequency	Each backup session
Recovery plan	Standby Image (Azure)
Screenshot verification	Completed

BACKUP DETAILS USED FOR THE RESTORE

Backup session time	April 05 2023 2:01:02 AM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

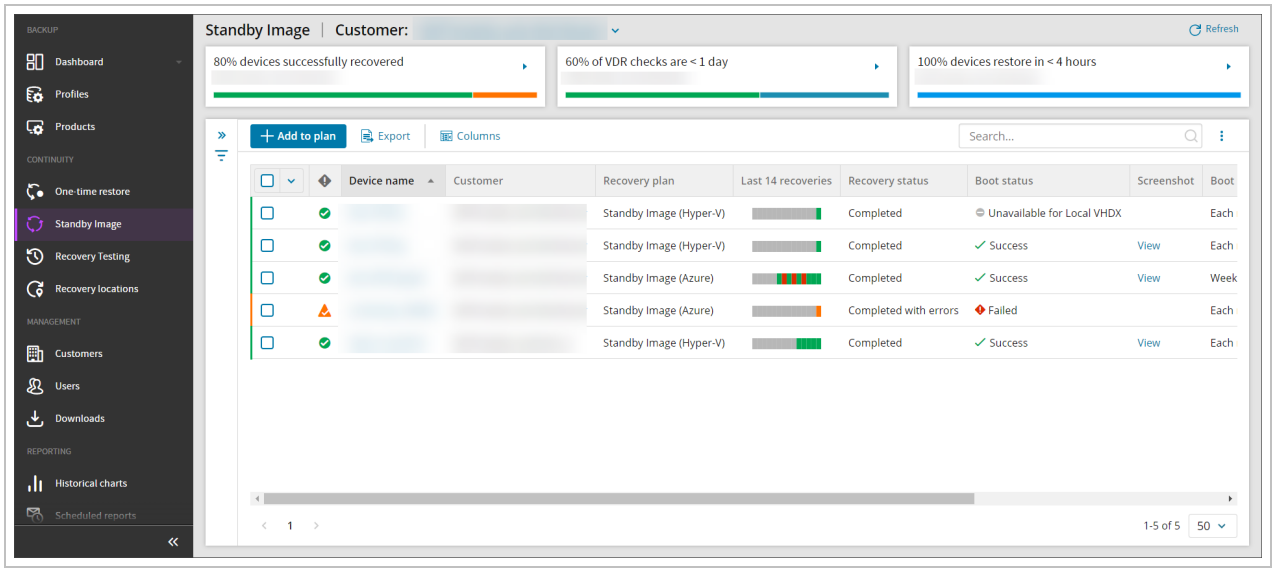
Below is a screenshot of the virtual machine created during the boot phase of recovery.

Monitor Standby Image Devices

From the Management Console, you can view the dedicated Standby Image Overview by selecting **Continuity** > **Standby Image** from the vertical menu on the left hand side.

This page will list devices assigned to the Standby Image plans:

- Standby Image to Hyper-V
- Standby Image to Azure
- Standby Image to ESXi



From this dashboard, you will see a specified set of columns detailing information relevant to devices using the Standby Image plan, including the continuity history of the last 14 recoveries, the recovery status, boot status, and plan assigned, along with some other information.

If no devices are assigned to either Standby Image plan, the dashboard will display a message to advise, along with a button to add devices to a plan.

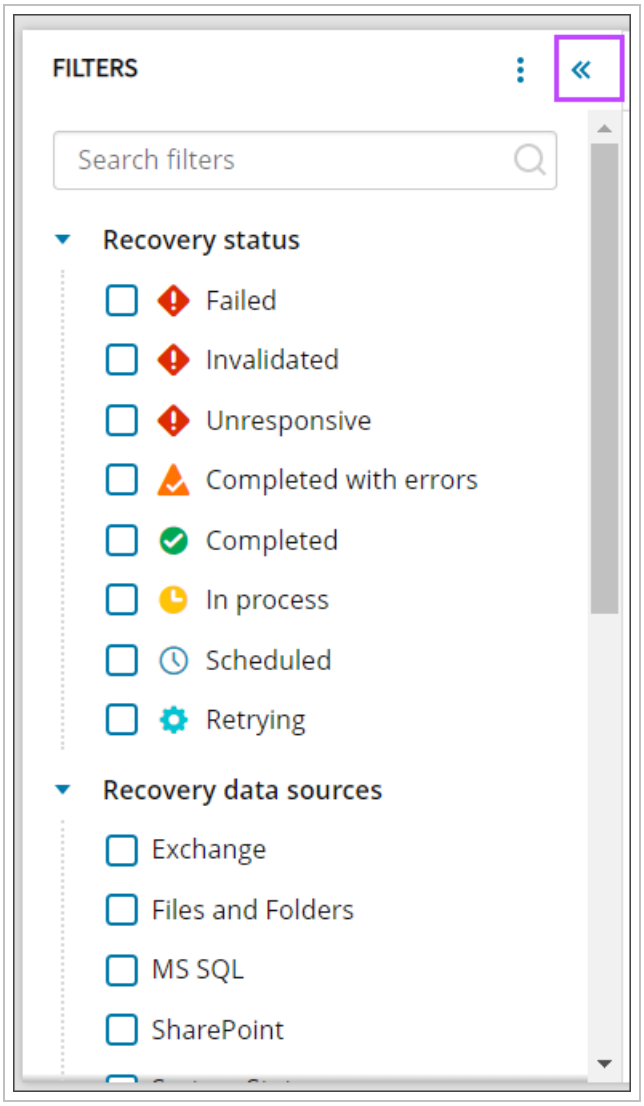
> If a device is assigned to **multiple** plans (i.e. **Standby Image to Hyper-V**, **Standby Image to Azure** and **Standby Image to ESXi**), the device will be listed for each instance of a plan and can be told apart by the **Recovery Plan** column.

Searching

Searching within the Standby Image overview can be done by using the search box over to the right hand side of the page, just above the devices list. The search can be performed by any text field.

Filtering

The Standby Image overview also includes functionality to filter devices using the filter menu to the left of the device list and can be displayed or hidden by clicking the double arrows.



From this menu, you can filter by:

Recovery status

- **Failed** - The recovery session has failed
- **Invalidated** - Device was moved to an inappropriate partner and so the session has failed
- **Unresponsive** - The recovery session was initiated but did not receive updates for at least 30 minutes because the recovery location restarted or was offline.
- **Completed with errors** - The recovery session completed, but encountered errors
- **Completed** - The recovery session completed with no errors
- **In process** - The recovery is currently in progress
- **Scheduled** - Devices just added to a recovery plan and are waiting for their first recovery session or devices where restores were paused and have since been resumed will display as scheduled
- **Retrying** - A restore session was not finished so the system is trying the restore again

Recovery data sources

- Exchange
- Files and Folders
- MS SQL
- SharePoint
- System State

Recovery session statistics

- Boot check frequency
  - Off
  - Every recovery session
  - Daily
  - Weekly
  - Biweekly
  - Monthly
- Boot Check Status
  - Success
  - Failed
  - Off
  - Unavailable for Local VHDX
- Continuous restores
  - Running
  - Paused
- Duration of the last completed recovery session
  - Sliding scale from 0 to unlimited

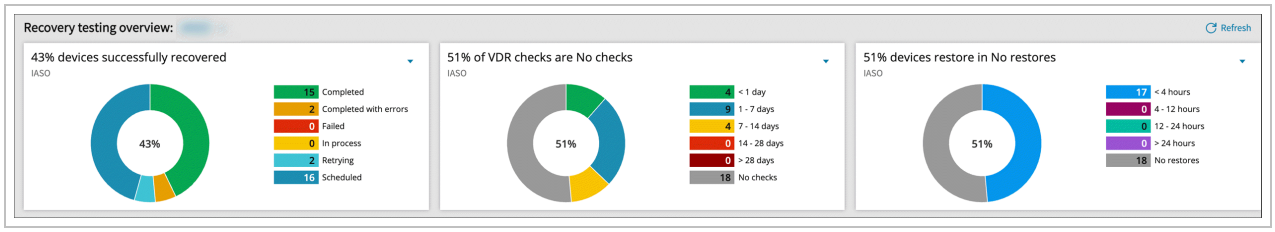
  in minutes
- Number of errors of the last completed recovery session
  - Sliding scale from 0 to unlimited
- Number of restored files
  - Sliding scale from 0 to unlimited
- Number of selected files
  - Sliding scale from 0 to unlimited
- Recovery Location name
  - Select the recovery location from a dropdown
- Recovery Plan
  - Standby Image (Hyper-V)
  - Standby Image (ESXi)
  - Standby Image (Azure)
- Restored size
  - Sliding scale from 0 to unlimited

  in KB and GB

- Recovery testing status of the last completed recovery session
  - Failed
  - Completed with errors
  - Completed
- Screenshot
  - Available
  - Not Available
- Selected size
  - Sliding scale from 0 to unlimited
  in KB and GB
- Timestamp of the last completed recovery session
  - Quick Picks of:
    - Last day
    - 1 - 7 days
    - 7 - 14 days
    - 14 - 28 days
    - > 28 days
  - Custom range, select a stat date and time and an end date and time

Widgets

Three widgets can be maximized at the top of the page, which allow for further filtering:



Device recovery status

This widget allows you to filter the devices by recovery status:

- Completed
- Completed with errors
- Failed
- In process
- Retrying
- Scheduled

VDR checks time frame

This widget allows you to see the percentage of devices whose recovery check completed within the following day ranges:

- < 1 day
- 1 - 7 days
- 7 - 14 days
- 14 - 28 days
- > 28 days
- No checks

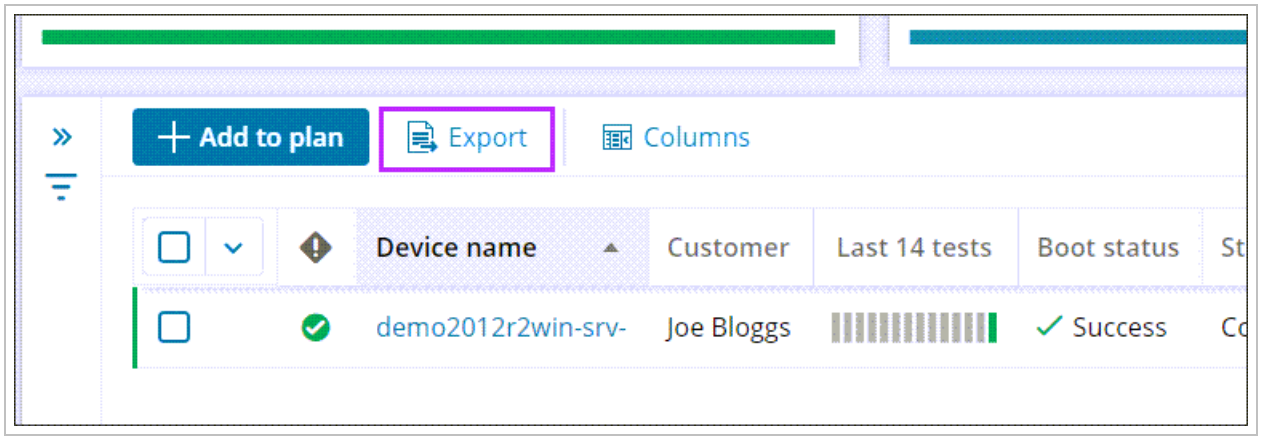
Device restore time frame

From this widget, you can filter devices by the how recent restores are done by the following time frames:

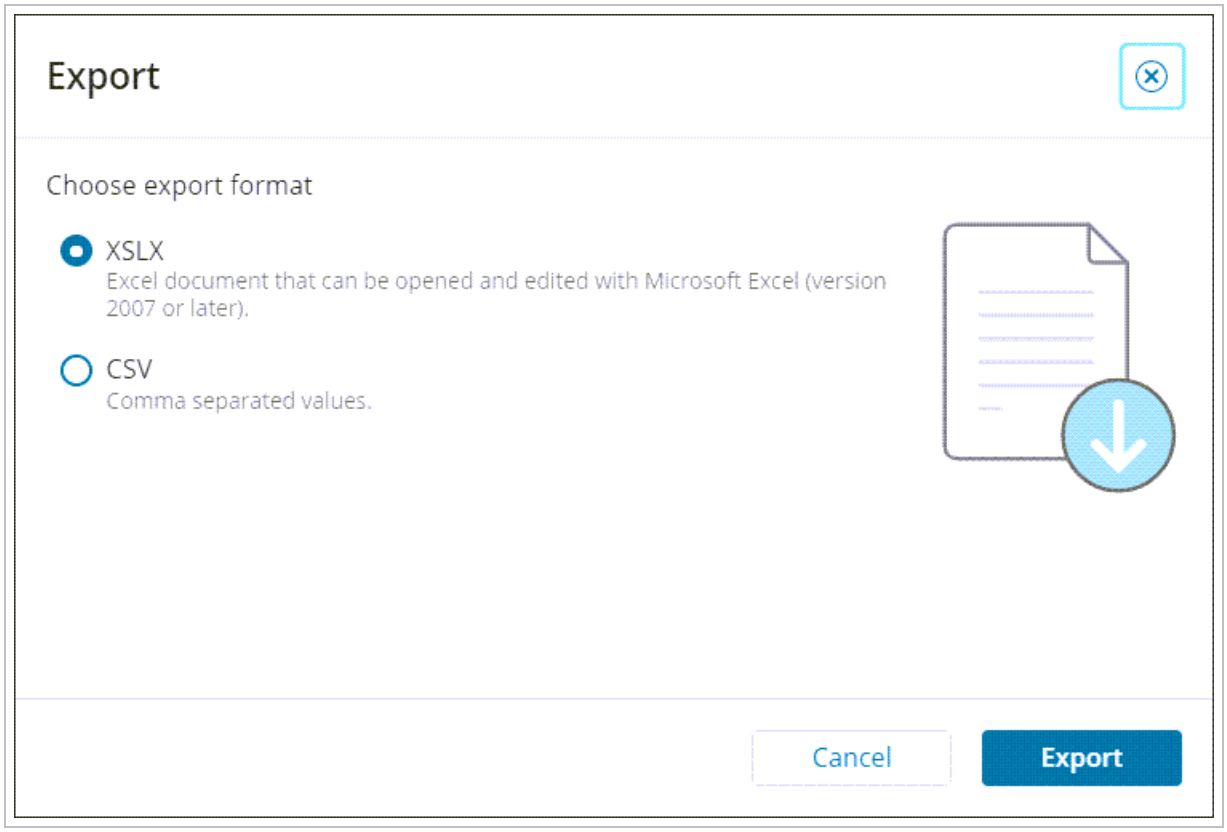
- < 4 hours
- 4 - 12 hours
- 12 - 24 hours
- > 24 hours
- No restores

Exporting

You may export a list of devices currently assigned a plan by clicking **Export**

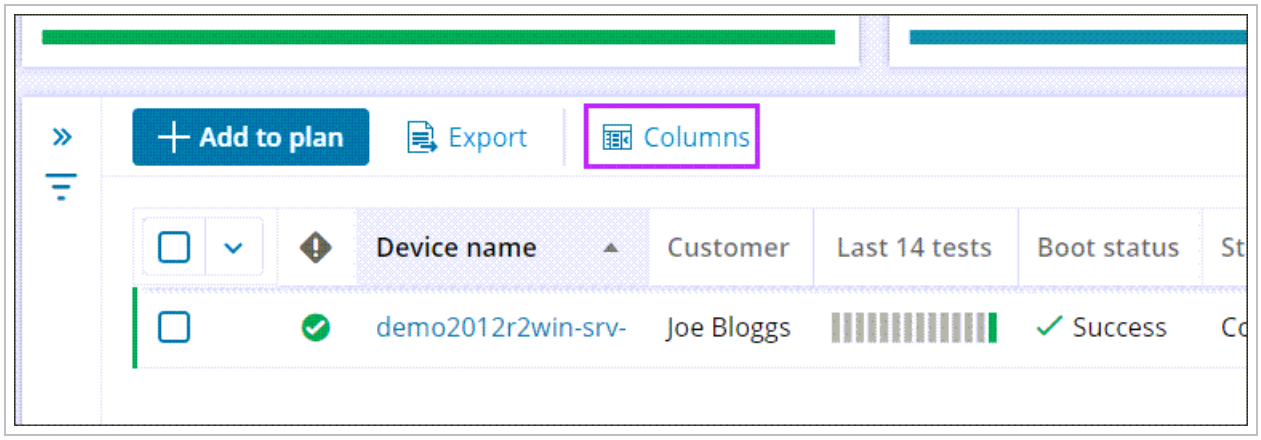


This will then provide a separate dialog where you can choose to export in either XSLX or CSV.

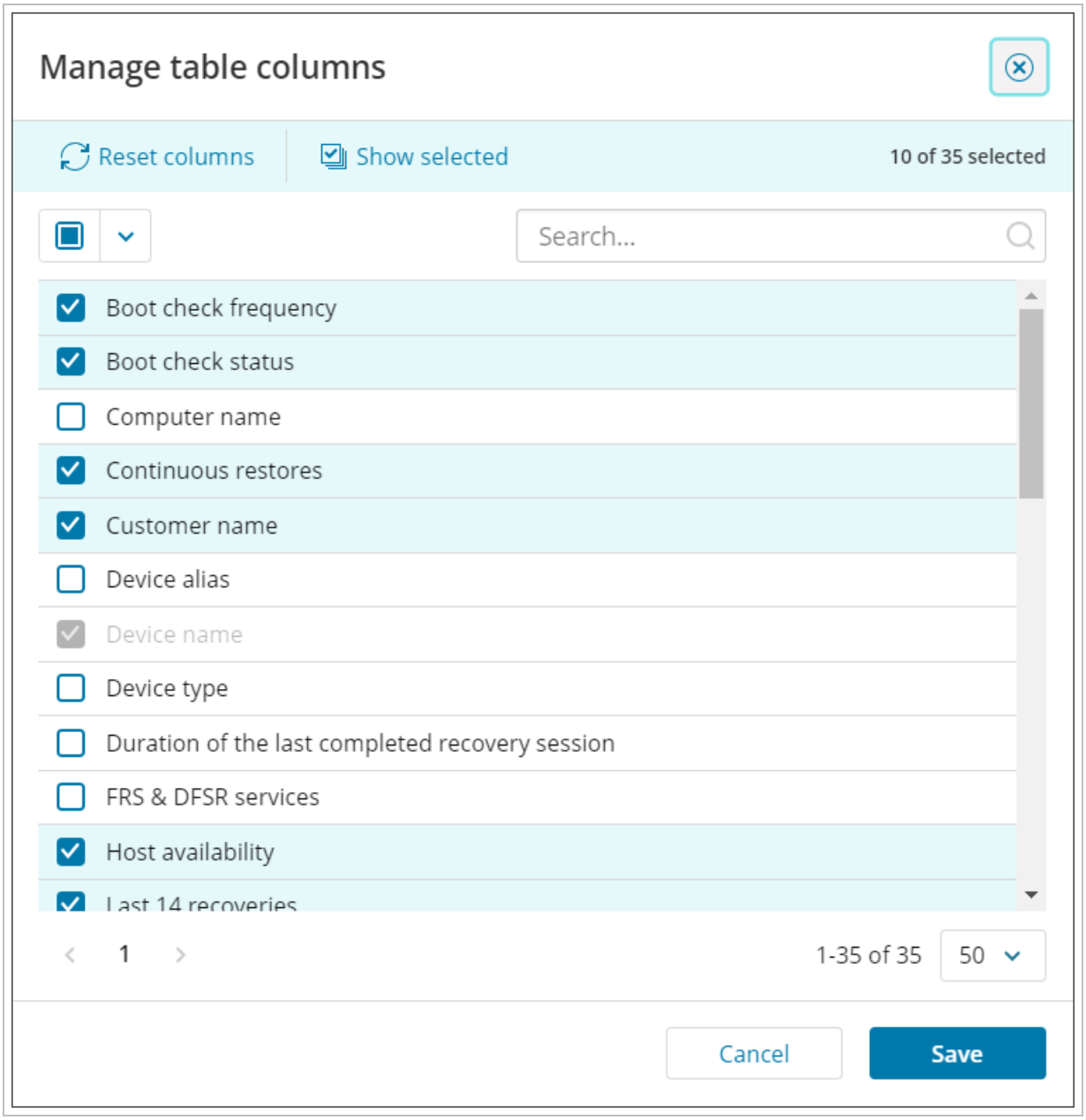


Manage Table Columns

Management Console allows you to manage the tables columns that can be seen within the Standby Image overview.



In the Manage table columns dialog, you can select and deselect columns based on the information you wish to view from the overview.

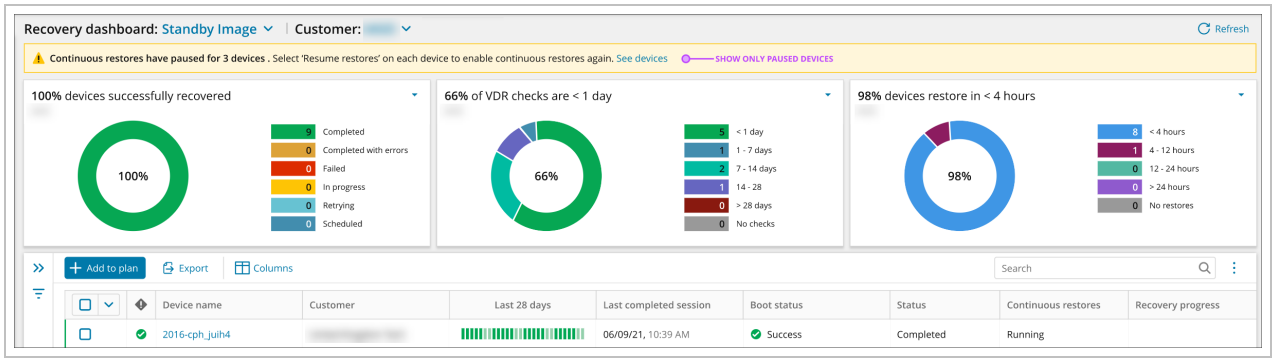


Pause Standby Image recovery

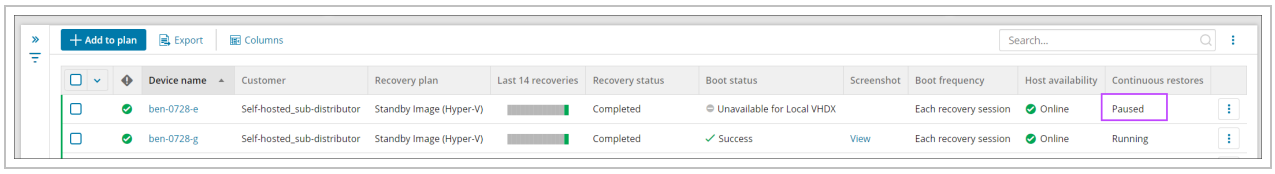
Once a Standby plan has been assigned to a device, the continuous restores can be paused and restarted. Pause or resume restores functionality there to provide a possibility to use the restored machine for failover in case of disaster.

> If a restored Virtual Machine is turned on manually, the Standby Image restore will automatically pause.

Pausing and restarting continuous restores can done be for single or multiple devices at a time. Once devices have been paused, a banner will be displayed at the top of the page to advise.

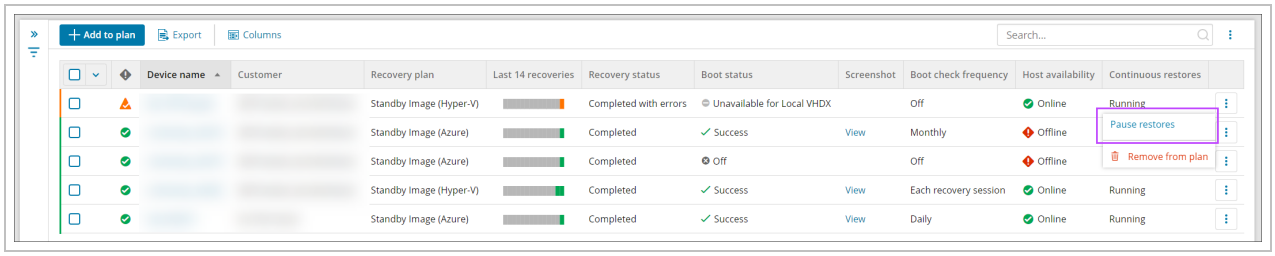


Click **See devices** to filter the devices list by **Continuous Restore: Paused** to only devices which are currently paused.



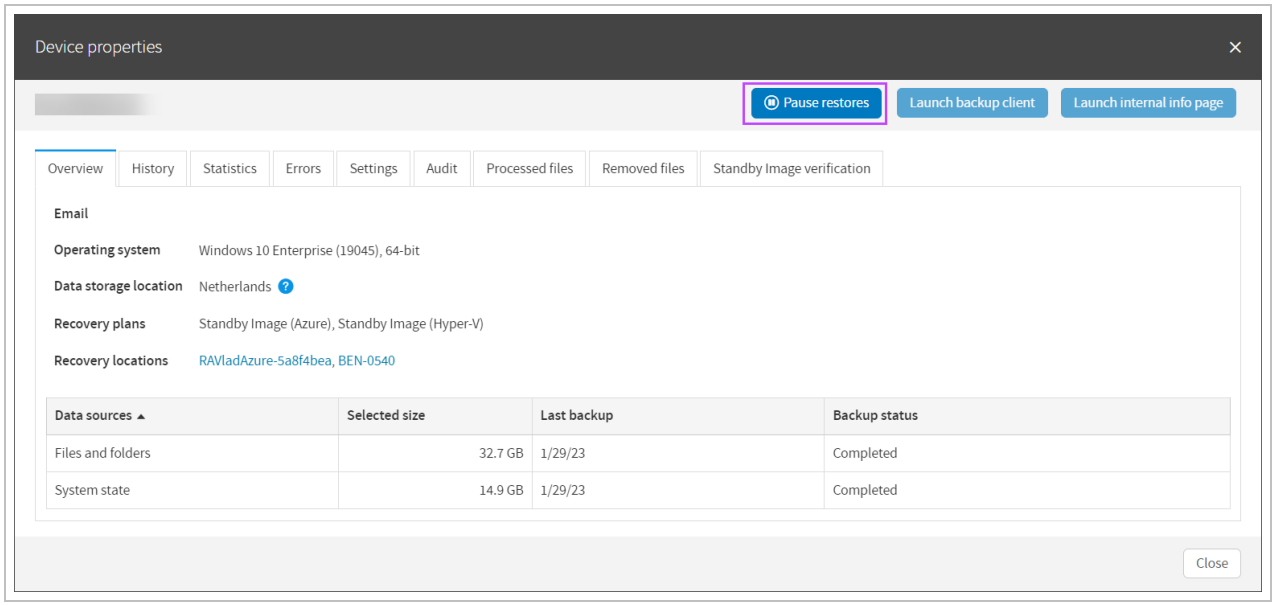
For single devices

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Click the menu action button to the right of the device (Three vertical dots)
4. Select **Pause Restores** or **Resume Restores**



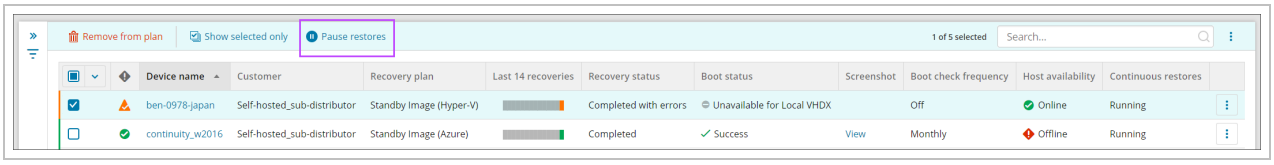
> This will differ depending on whether the plan is currently active, or has been paused already

It is also possible to pause restores from the Device Properties window:



For single or multiple devices

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Tick the checkbox for any devices that need paused from the list
4. In the top panel, select **Pause Restores** or **Resume Restores**



> This will differ depending on whether the plan is currently active, or has been paused already

Accessing device properties

The Device Properties window displays several tabs detailing information on the Backup device. Full details of the contents of each tab can be found on the Device management in Management Console page.

The two that are the most commonly used with Standby Image are the **Settings** tab and the **Standby Image Verification** tab.

Settings Tab

Broken into several sections, this tab contains:

General

This section provides the main device details:

- **customer** - Who device belongs to, can be changed to move the device to a different customer
- **Device name** - Cannot be changed

- **Installation key** - Cannot be changed
- **Creation date** - Cannot be changed
- **Expires on** - Can be amended to a date in the future, or set to **'no expiration'** if required

> You may also see the Request Passphrase button here if the device is set up to use this instead of its own security code/encryption key

Backup

This section contains:

- **Backup product** - Use the dropdown to change the Product used by the device
- **Profile** - Use the dropdown to change the Profile applied to the device

Recovery

On a device assigned to the Standby Image plan, this section will allow you to see plan in use and amend some details of this:

- **Recovery Plan** - Standby Image (Each backup session)
- **Recovery Location** - Cannot be changed from this panel. To change this, see Add Device to Recovery Location
- **Successful recovery report email** - Specify the email address(es) that will receive reports when the most recent Recovery as per the assigned plan has been successful
- **Failed recovery report email** - Specify the email address(es) that will receive reports when the most recent Recovery as per the assigned plan has failed
- **Remove Cove branding** - toggle branding of the email reports on or off
- **Restore format** - This option will not be available for Standby Image to Azure.
  - For **Standby Image to Hyper-V**, this is a choice between **Hyper-V** or **Local VHDX**
  - For **Standby Image to ESXi**, this is a choice between **ESXi** and Local **VHDX**

    > Further settings displayed are dependent on the Restore Format selected for the device. These settings can be changed as required.

> All Recovery Plans associate to the device will be included here, and can be minimized or expanded by clicking the arrow to the left of the plan name.

Device properties

Launch backup client | Launch internal info page

Overview | History | Statistics | Errors | Settings | Audit | Processed files | Removed files | Standby Image verification

General

Customer

Device name

Installation key

Creation date 2/21/23

Expires on 04/18/24 No expiration

Backup

Product _test

Profile -servers

Recovery

Standby Image (ESXi)

Recovery plan Standby Image (ESXi)

Recovery location ESXiRA

Successful recovery report email e.g email@email.com

Failed recovery report email e.g email@email.com

Remove Cove branding OFF

Restore format ESXi VMDK

Boot check frequency Daily

FRS and DFSR services OFF

Local Speed Vault OFF

CPU cores 4

RAM (GB) 4

VM Subnet mask Enter a custom subnet mask to the new virtual mac

VM gateway Enter a custom gateway to the new virtual machine

VM DNS server Enter a DNS server to be used on the restored mach

Separate multiple DNS servers with a comma or semicolon

VM IP address Enter a custom IP address to the new virtual machir

Standby Image (Hyper-V)

Recovery plan Standby Image (Hyper-V)

Recovery location BEN-6478

Successful recovery report email e.g email@email.com

Failed recovery report email e.g email@email.com

Remove Cove branding OFF

Restore format Hyper-V Local VHDX

Boot check frequency Daily

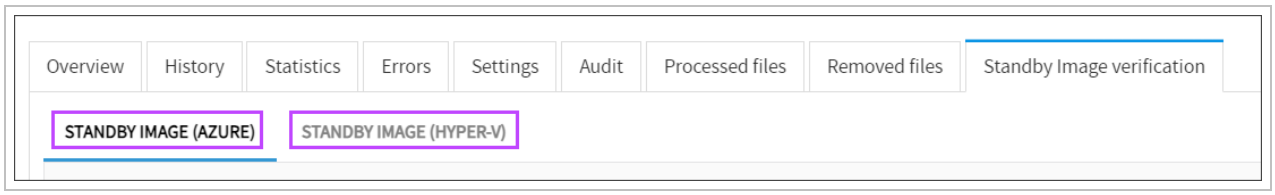
FRS and DFSR services OFF

Local Speed Vault OFF

Standby Image Verification Tab

To view statistics of the Standby Image and check the screenshots to ensure this has been successful, you can view this by following one of the below methods.

All plans associated to the device will have their own sub-tabs that can be selected to view the appropriate screenshot:



From Device Properties

1. Log in to the Management Console
2. Click the device name on either the Backup Dashboard or the Standby Image overview to open the Device Properties
3. Navigate to the **Standby Image Verification** tab

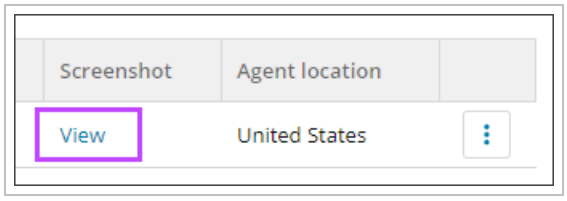
From Standby Image Overview

The Standby Image Verification tab can be viewed from the Standby Image overview in one of two ways:

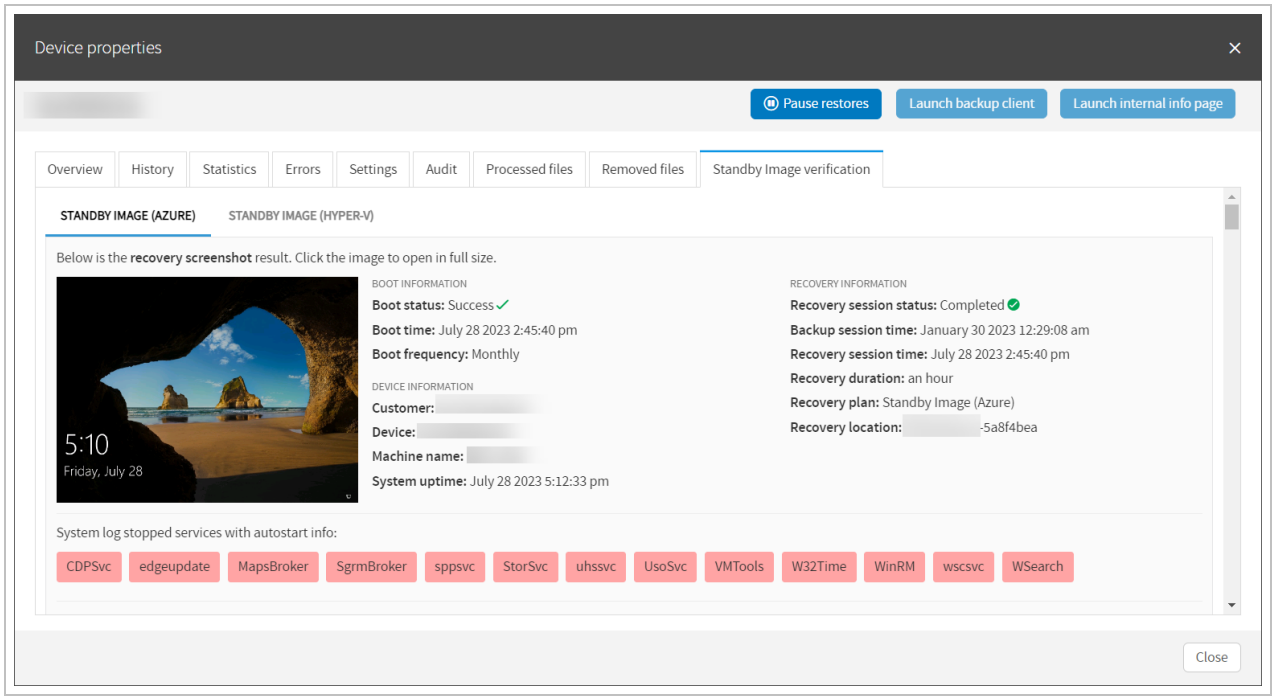
- Via theScreenshot column
- Via the Last 14 recoveries column

Screenshot column

1. Log in to the Management Console
2. Navigate to **Continuity** > **Standby Image**
3. Click **View** under the Screenshot column

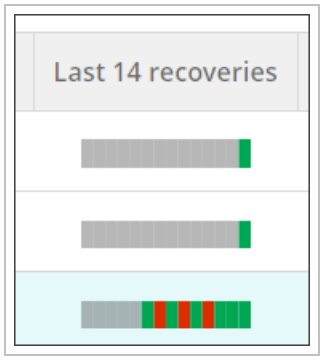


4. This will take you in to the Device Properties dialogue, where you will now see the **Standby Image Verification** tab:

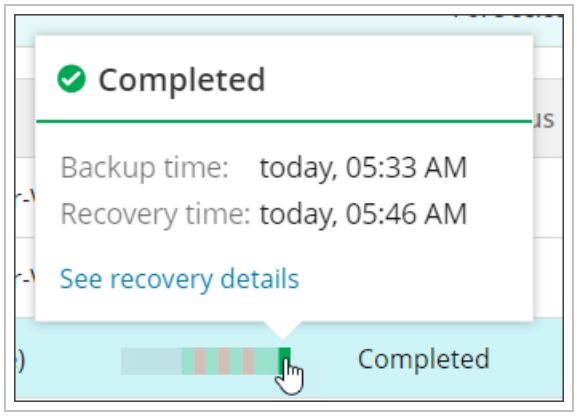


Last 14 recoveries column

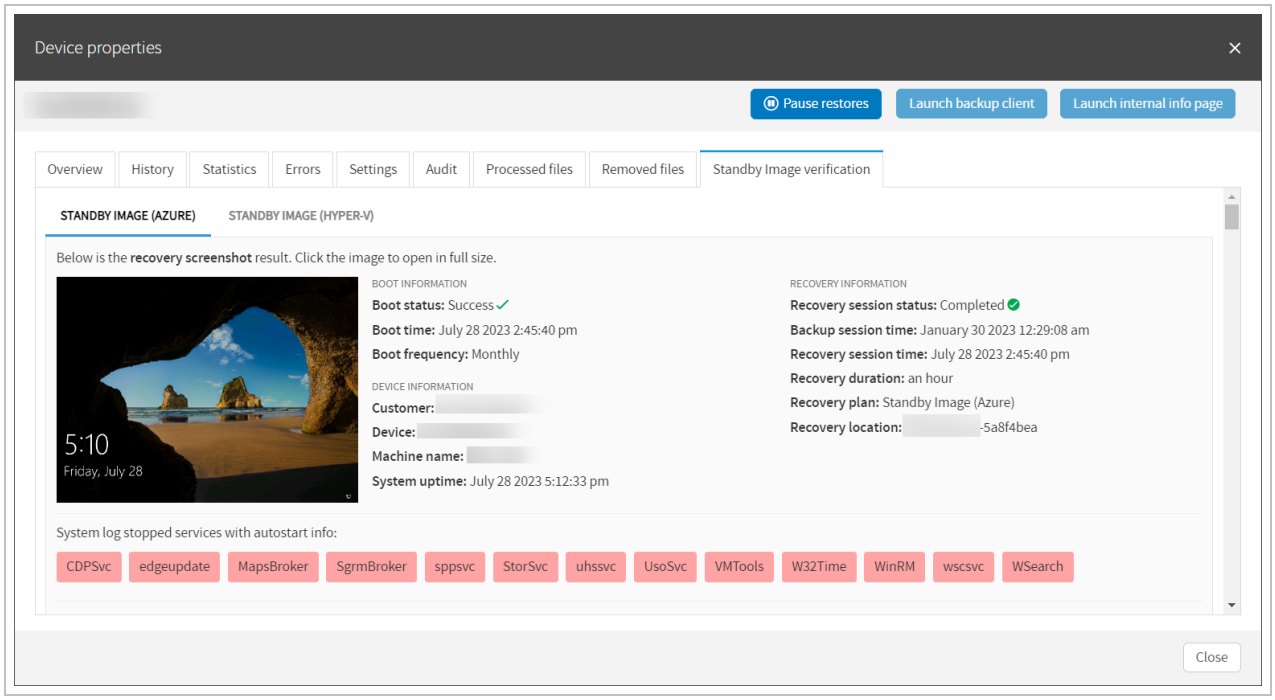
1. Log in to the Management Console
2. Navigate to **Continuity** > **Standby Image**
3. Hover your mouse over the most recent colored bar in the Last 14 recoveries column



4. Click **See recovery details** in the popup box that appears



5. This will take you in to the Device Properties dialogue, where you will now see the **Standby Image Verification** tab:



Standby Image to ESXi

Cove Data Protection (Cove)'s Standby Image to ESXi service runs a continuous restore of your data to VMWare ESXi and boots based on the frequency set during configuration of the plan.

> Devices **can** be assigned to **multiple Standby Image plans** at once, i.e. Standby Image to Hyper-V *and* Standby Image to Azure *and* Standby Image to ESXi.

> Restores can be performed to either a VMWare ESXi instance or to a Local VMDK file. Local VMDK files can be restored to either a Local Drive, or to a Network Share (NAS).

Standby Image Data Restored:

The following data sources are supported and restored to the ESXi recovery location given that they are selected for backup in the Product, or data source selection:

- System State
- Files and Folders
- Exchange
- SharePoint
- MS SQL

Requirements:

- Backup Manager version 17.4 and newer
- Devices and Recovery Locations must belong to the same Customer
- A Cove Data Protection (Cove) SuperUser or Manager account
- Recovery Locations must be added to the Management Console and the Recovery service must be installed on the recovery location **before** Standby Image recovery can occur

  - Recovery Location is a machine with the recovery service installed
  - Recovery service is a service which orchestrates all the recovery jobs for Standby Images

Limitations

- Standby Image cannot be used on the RMM integrated version of Backup (Managed Online Backup) or on the N-central integrated version of Backup (Backup and Recovery)
- Standby Image is **not** available for devices with disabled 'Virtual disaster recovery' feature in an assigned Product
- 32-bit architecture is not supported
- Restores run after each backup session for System State and Files and Folders. After the first restore, a virtual machine is created and kept on the selected host/storage, then with each subsequent restore the virtual machine is updated with only new data
- For a Virtual Machine restored to ESXi host, there is an option to automatically boot it and create a screenshot to check that the Virtual Machine is bootable, then send this screenshot to the Management Console so that users can check it
- Maximum supported capacity for virtual hard disks is **64 TB** per disk
- Devices can only be assigned to **one** Recovery Location

What's inside:

Enable Standby Image to ESXi

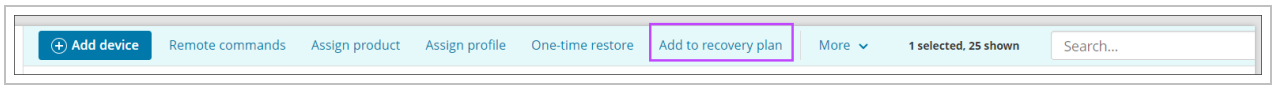
Devices **cannot** be added to a **Standby Image plan** if already assigned to a **Recovery Testing plan**.

Devices **can** be assigned to **multiple Standby Image plans** at once, i.e. Standby Image to Azure, to Hyper-V *and* to ESXi.

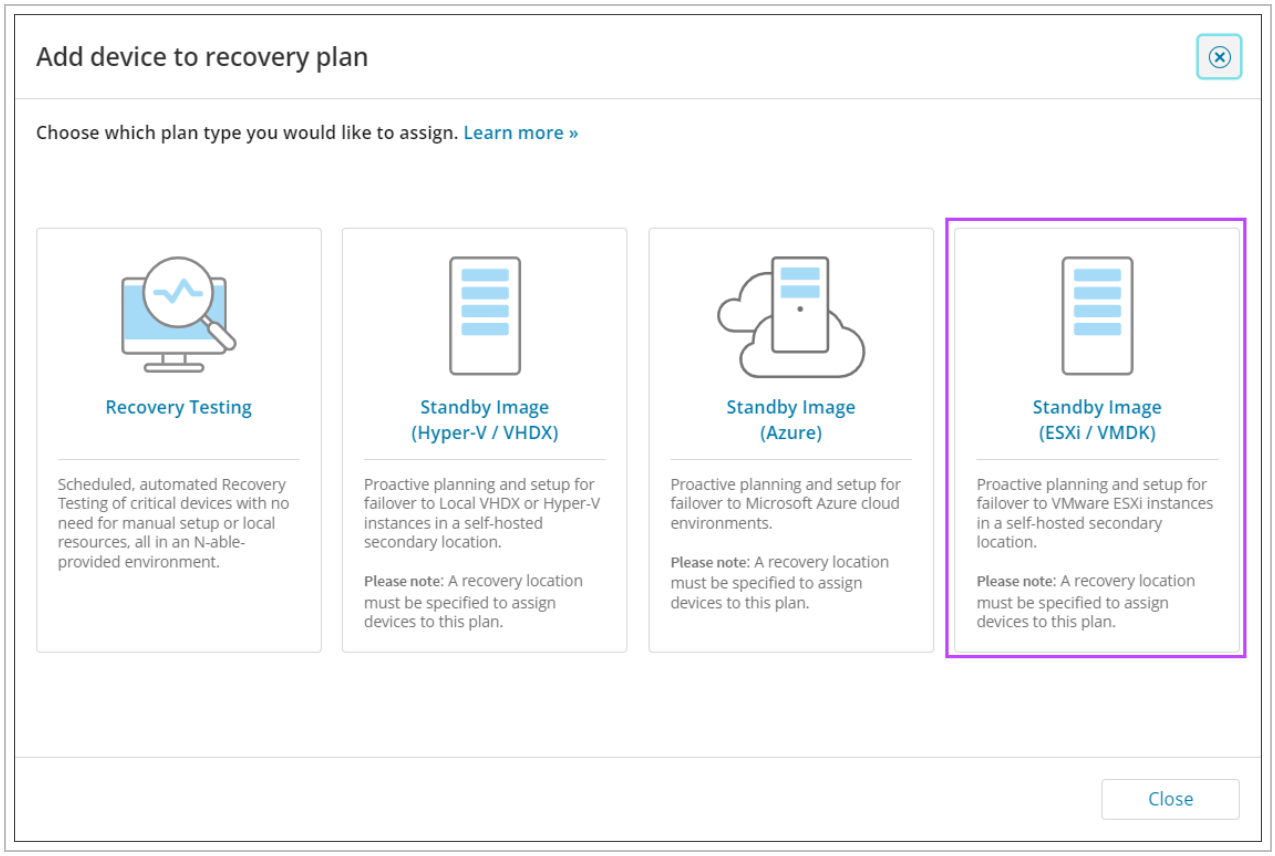
From Main Dashboard

To enable Standby Image to ESXi on a device from the Management Console's main Dashboard, follow the steps below:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan to
3. Click **Add to recovery plan** from the Toolbar



4. Select **Standby Image (ESXi)**

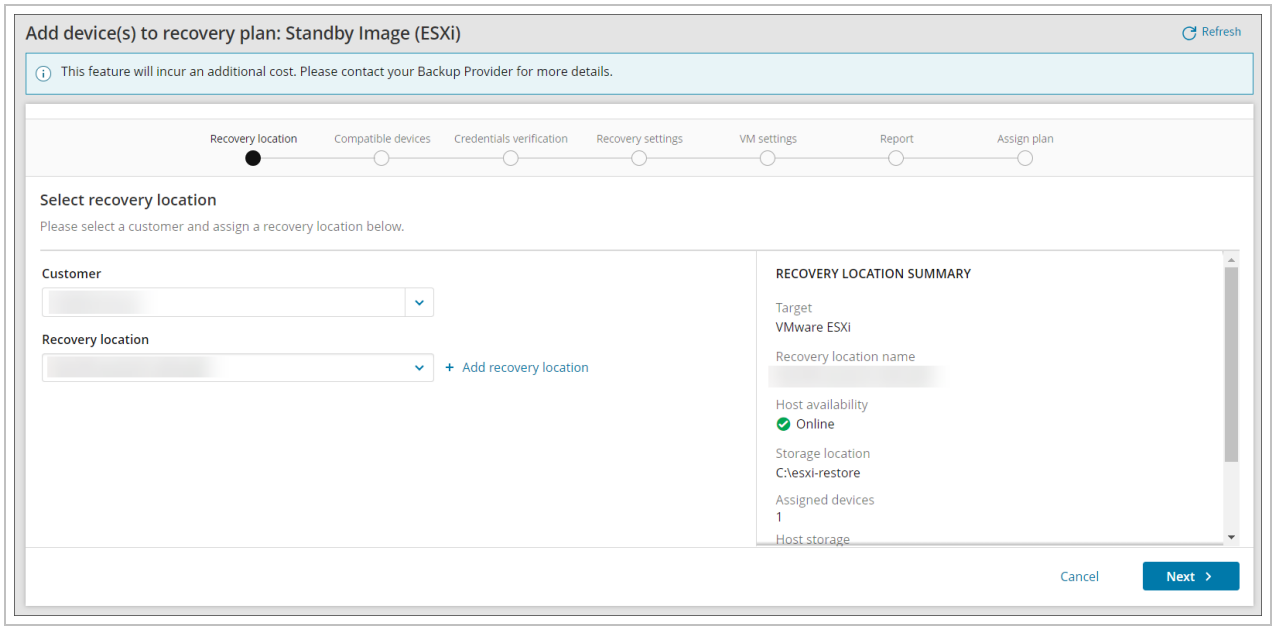


5. Select the customer the device(s) you wish to apply the Standby Image plan belong to

6. Choose the recovery location as was configured in Add Recovery Locations (ESXi)

> If the selected customer does not have any locations, you must add one before continuing by selecting **Add recovery location**.

> If the Recovery Location does not have a Storage Location, one must be provided before continuing



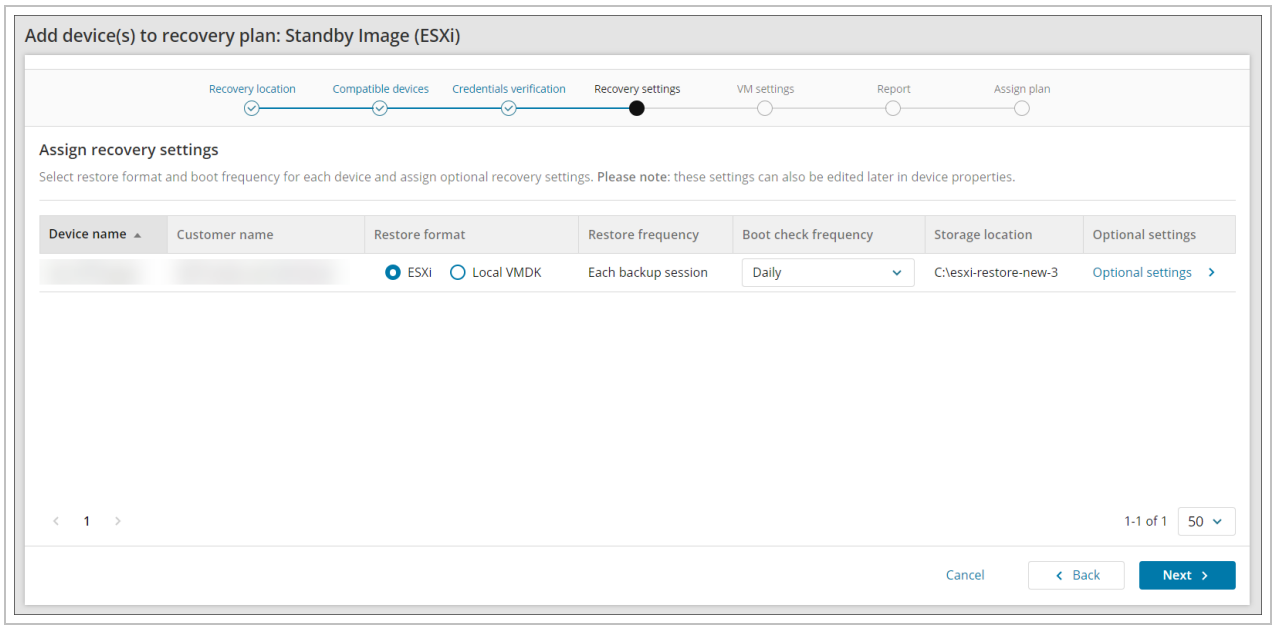
> It is not possible to assign a location for which the **Host availability** is "**Offline**"

7. Click **Next**
8. Confirm compatibility of the device(s) you want to apply the Standby Image plan on
9. Click **Next**
10. Enter the security code/encryption key or passphrase for the device(s). This can be either:
    - **Private encryption key** - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryption
    - **Passphrase encryption** - These are generated on demand for automatically installed devices. You can find information on this here

> If you are logged in as a security officer, this will be detected automatically.

11. Click **Next** to continue

12. Choose the restore format:
    - ESXi
    - Local VMDK



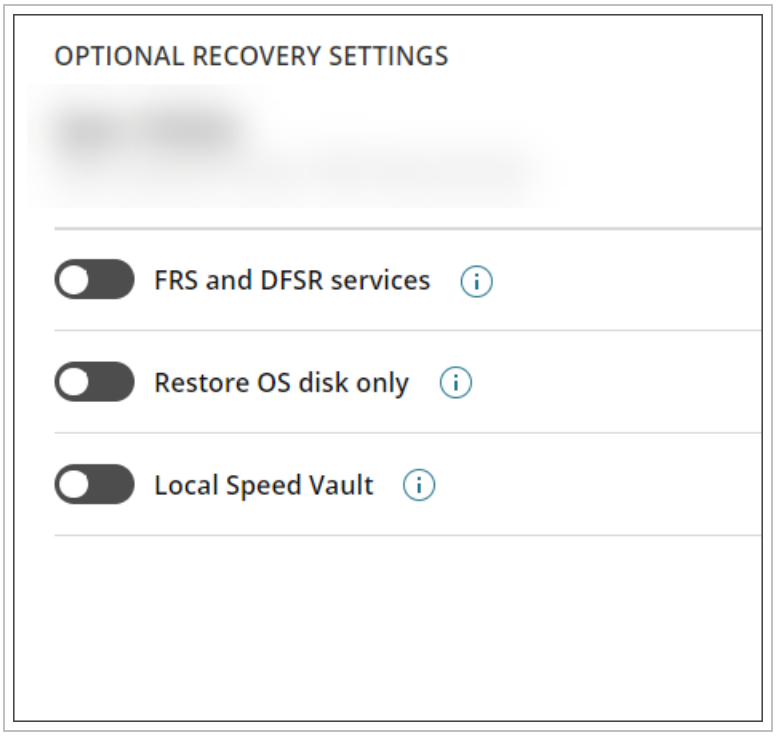
> If the Storage Location was configured as a Network Share, you will only be able to select Local VMDK as the restore format

13. Choose the boot check frequency:

> Available for **ESXi** restore format **only**, these are not available if Local VMDK is selected

    - Off
    - Every recovery session
    - Daily
    - Weekly
    - Biweekly
    - Monthly

14. Configure the **Optional Recovery Settings** for ESXi by clicking **Optional Settings** to the right of the storage location:



- **FRS and DFRS services** - If you are restoring Active Directory with multiple domain controllers, you should change the FRS and DFSR services to authoritative in the domain controller that will be started in the first place. Avoid marking several FRS/DFSR services as authoritative in the production environment as it can result in data loss. When the feature is on, the FRS and DFSR services are started on the target VM in the authoritative mode. The NETLOGON and SYSVOL shares become available, so the Active Directory and DNS services become functional again

  > More information about FRS/DFSR is available in the Microsoft Knowledge Base. Article IDs: KB2218556 and KB290762

- **Restore OS disk only** - Restoring the OS disk only will speed up restores
- **LocalSpeedVault** - If a LocalSpeedVault (LSV) is enabled on a backup device, the data is sent to both the LSV and the cloud or private storage location. During a restore, data is automatically downloaded from the LSV first to the local device which makes restore faster. If the LSV is not available or not synchronized, the restore data will be pulled from the cloud or private storage location. This takes place automatically and cannot be reconfigured

15. Click **Next** to configure the **Virtual Machine Settings**:

> Available for **ESXi** restore format **only**, these are not available if Local VMDK is selected

- **Connected Server(s)** - Select the server where the Virtual Machine will be allocated as added in Step 5: Add Storage Location and Server Connections
- **Data Center**
- **Host**
- **Storage**
- **Resource Pool**
- **Network**
- **Connect on startup** - connect to the selected network on startup
- **CPU Cores** - Select the number of CPU Cores to be allocated to the new virtual machine
- **RAM (GB)** - Select the amount of RAM in Gigabytes to be allocated to the new virtual machine
- **Source VM configuration** - When enabled, the same CPU and RAM settings as used on the source VM will be applied
- **VM IP address** – Assign a custom IP address to the virtual machine
- **VM subnet mask** – Assign a custom subnet mask to the virtual machine
- **VM gateway** – Assign a custom gateway to the virtual machine
- **VM DNS servers** – Assign the list of custom DNS servers (separated by comma), Example:

```
8.8.8.8 or 8.8.8.8,7.7.7.7
```

Connected server(s)

Data center

Host

Storage

Resource pool

Resources

Network

VIRTUAL

Connect on startup

CPU cores

4

RAM (GB)

4

Source VM configuration

VM IP address

Enter a custom IP address to the new virtual machine

IP addresses will increment by 1, if applied to all devices

VM Subnet mask

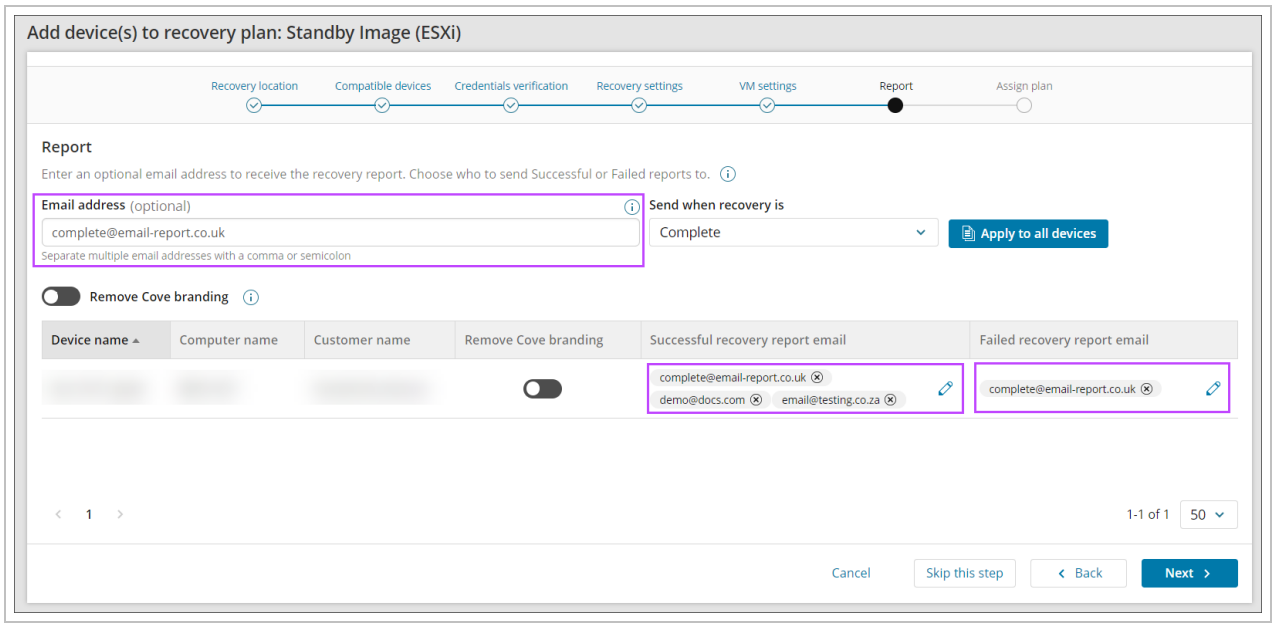
Enter a custom subnet mask to the new virtual machine

VM gateway

Enter a custom gateway to the new virtual machine

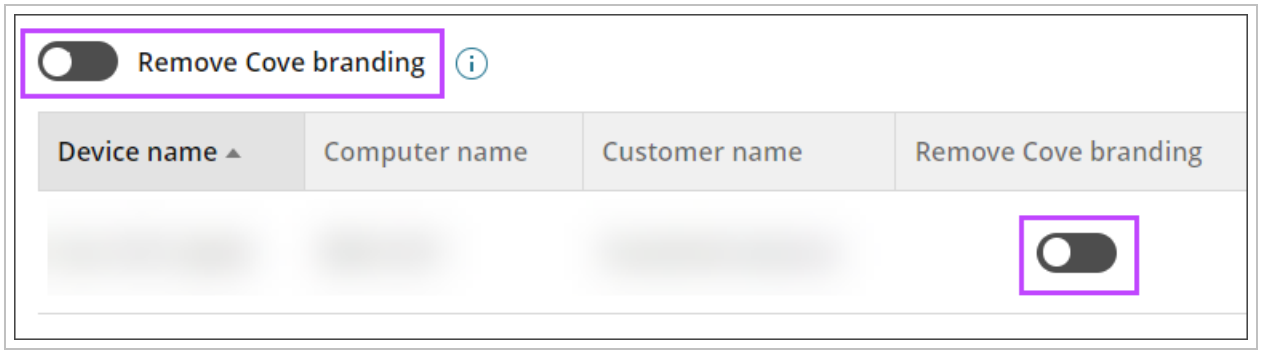
16. Click **Next** to progress to the **Report** window to enter one or more email addresses to receive a report when:
    a. The recovery is complete (Successful or Failed)
    b. The recovery was successful
    c. The recovery failed

> Multiple addresses should be separated using a comma or semi-colon



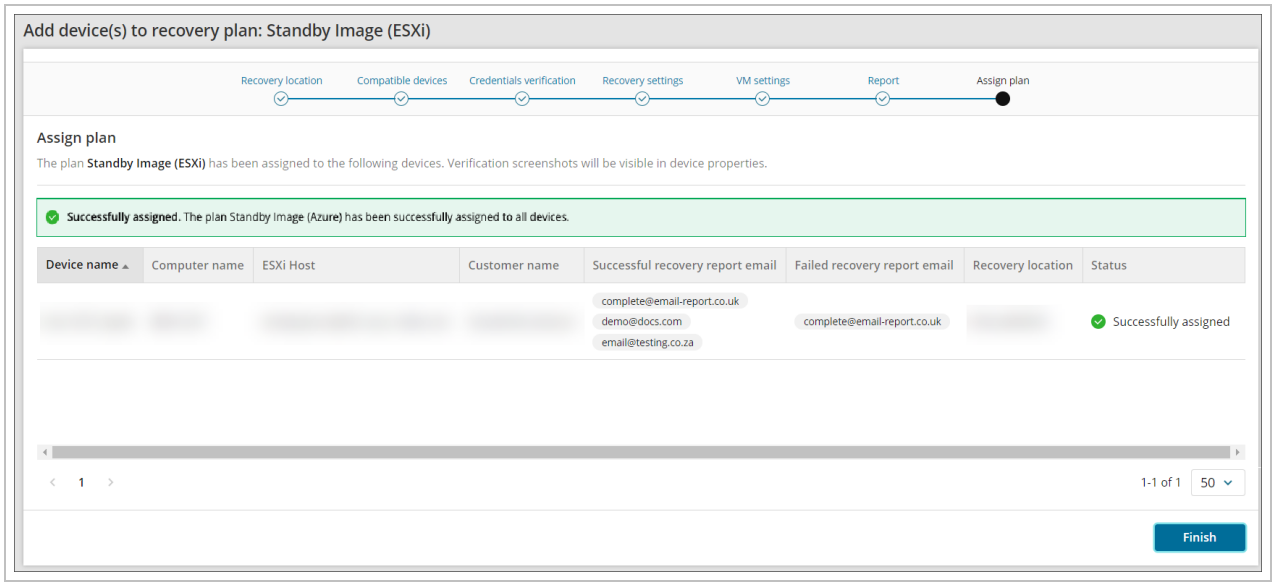
> If you do not want to add an email address to receive reports, click **Skip this step**

17. To remove all branding from the reports, use the **Remove Cove branding** toggle per device, or above the device list to apply the changes to all devices in this window



18. Confirm assigning the plan to the device(s)

19. Wait for the plan to be assigned until you see a confirmation banner on the page

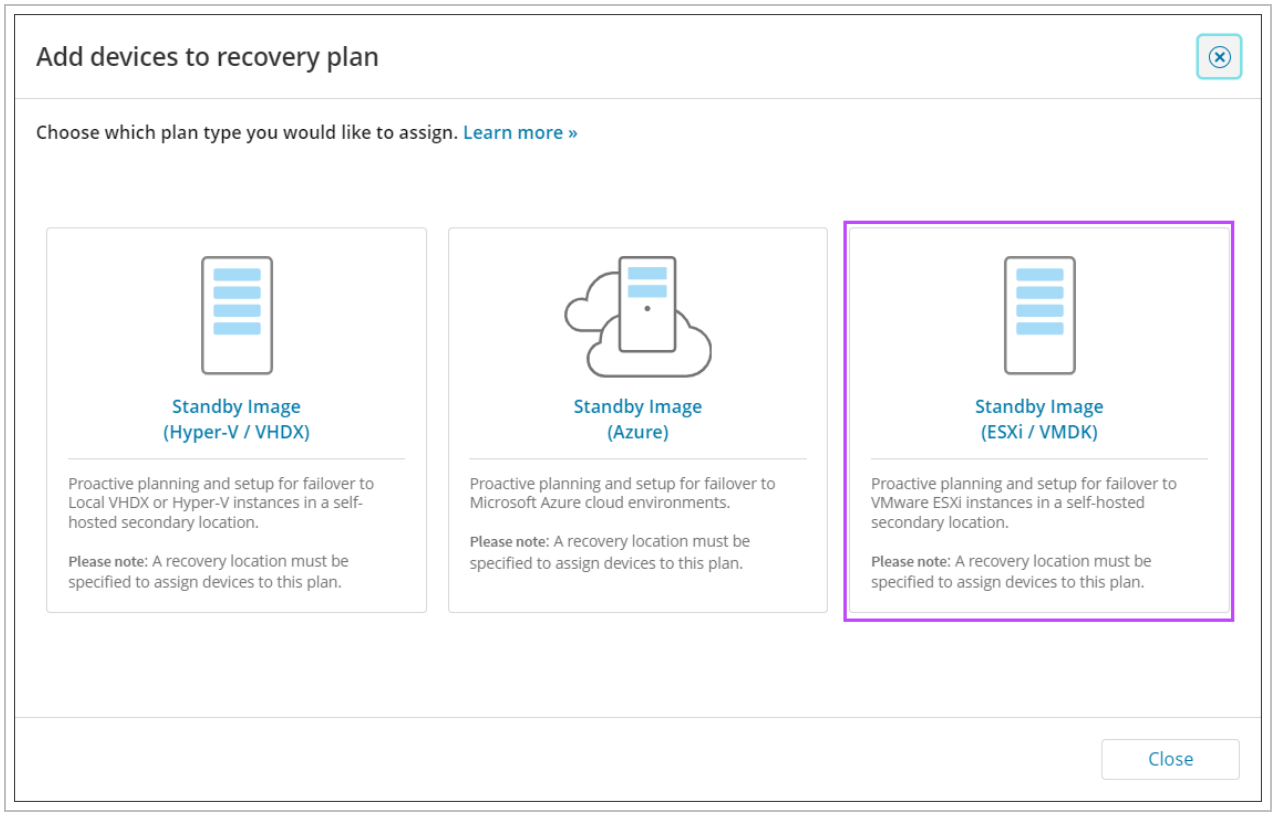


20. Click **Finish**

From Standby Image Overview

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Click **Add to Plan**

4. Select **Standby Image (ESXi)**



5. You will now be taken to the **add devices to recovery plan** wizard. Follow the steps from select the customer from the dropdown onwards

From Recovery Locations dashboard

Devices can be added to a Recovery Location from the **Continuity** > **Recovery Locations** page, thereby enabling the Standby Image Plan, using one of three methods:

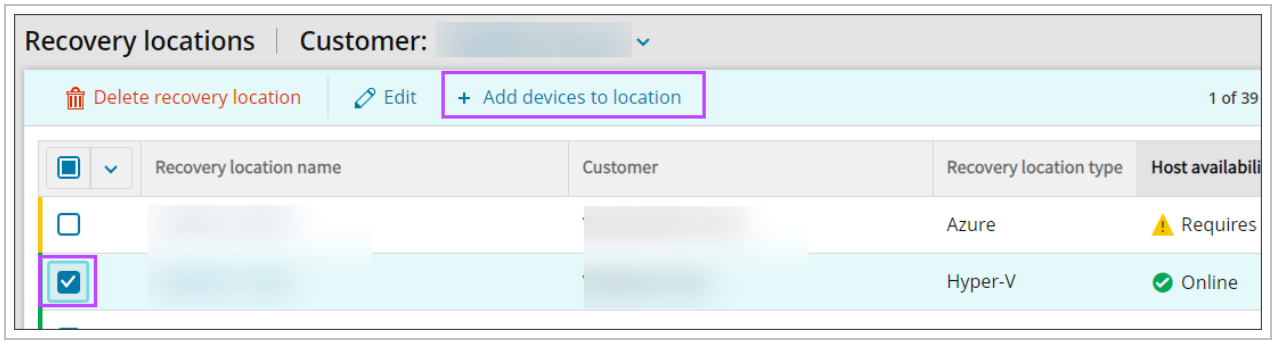
- Top bar menu
- Location context menu
- Right-hand menu

> These will only be available if the Recovery Location is **Online**.

Top bar menu

Available for Hyper-V and ESXi Locations **only**.

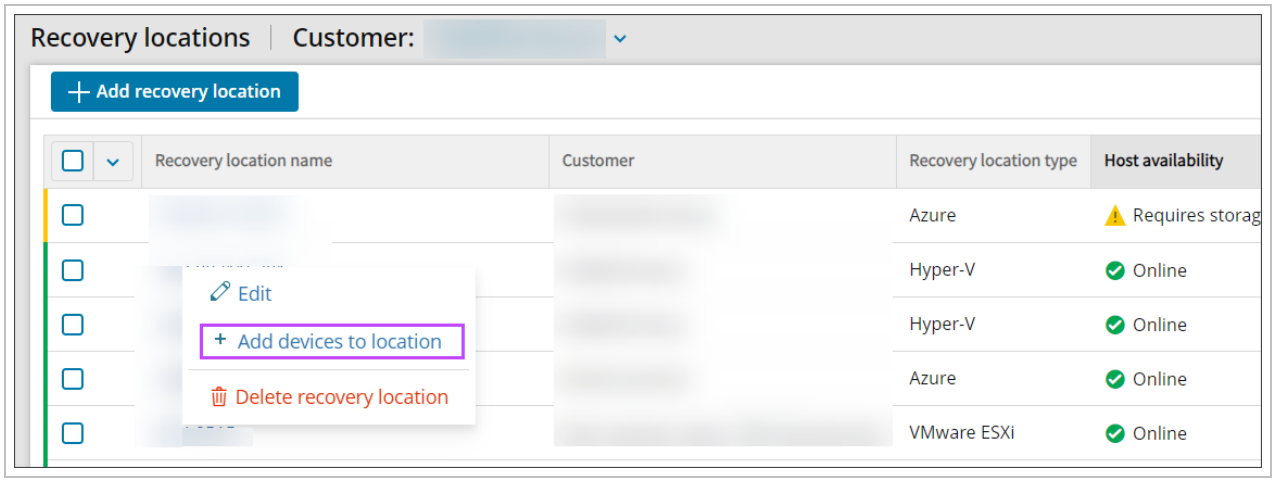
1. Select the checkbox for the Recovery Location to add the device to
2. At the top of the Recovery Locations page, select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
   a. Top bar menu
   b. Top bar menu

Location context menu

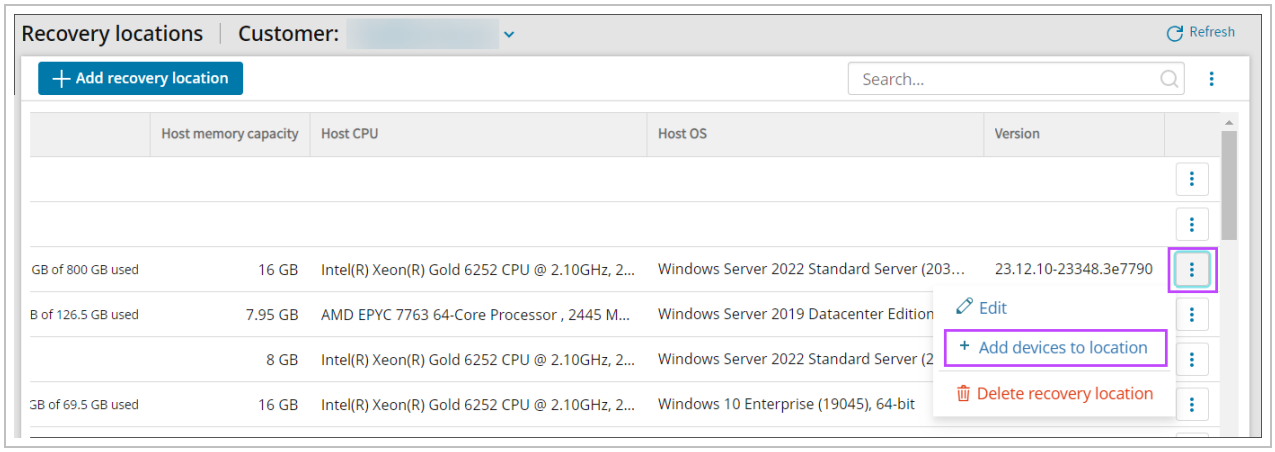
1. Right-click on the Recovery Location to add the device to
2. Select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
    a. Enable Standby Image to AzureDevices cannot be added to a Standby Image plan if already assigned to a Recovery Testing plan.Devices can be assigned to multiple Standby Image plans at once, i.e. Standby Image to Hyper-V and Standby Image to Azure. From Main DashboardTo enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:Log in to the Management Console under a SuperUser or Manager account In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan toClick Add to recovery plan from the Toolbar Select Standby Image (Azure)Select the customer the device(s) you wish to apply the Standby Image plan belong toChoose the recovery location as was configured in Add Recovery LocationsIf the selected customer does not have any locations, you must add one before continuing by selecting Add recovery location. See Add Recovery Locations for full details of adding a location.It is not possible to assign a location for which the Host availability is "Offline"Click NextConfirm the device selected from the Dashboard is compatible and click Next Enter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereClick Next to continueChoose the boot check frequency:OffEvery recovery sessionDailyWeeklyBiweeklyMonthlyIf you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Once connected, click NextClick Azure VM settings towards the right-hand side of the screen to open the settings configuration window:Configure the Azure VM Settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk typeData disk(s) typeVirtual NetworkSubnetAssign NSG and public IPDuring the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend blocking internet access for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.Click Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowConfirm assigning the plan to the device(s)Wait for the plan to be assigned until you see a confirmation banner on the pageClick FinishFrom Standby Image OverviewLog in to the Management Console under a SuperUser or Manager accountNavigate to Continuity > Standby ImageClick Add to PlanSelect Standby Image (Azure)You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the planRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding:
    b. Top bar menu
    c. Top bar menu

Right-hand menu

1. Click the action menu button for the Recovery Location, seen as three dots in a vertical line to the right of the location's version
2. Select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
    a. Enable Standby Image to AzureDevices cannot be added to a Standby Image plan if already assigned to a Recovery Testing plan.Devices can be assigned to multiple Standby Image plans at once, i.e. Standby Image to Hyper-V and Standby Image to Azure. From Main DashboardTo enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:Log in to the Management Console under a SuperUser or Manager account In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan toClick Add to recovery plan from the Toolbar Select Standby Image (Azure)Select the customer the device(s) you wish to apply the Standby Image plan belong toChoose the recovery location as was configured in Add Recovery LocationsIf the selected customer does not have any locations, you must add one before continuing by selecting Add recovery location. See Add Recovery Locations for full details of adding a location.It is not possible to assign a location for which the Host availability is "Offline"Click NextConfirm the device selected from the Dashboard is compatible and click Next Enter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereClick Next to continueChoose the boot check frequency:OffEvery recovery sessionDailyWeeklyBiweeklyMonthlyIf you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Once connected, click NextClick Azure VM settings towards the right-hand side of the screen to open the settings configuration window:Configure the Azure VM Settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk typeData disk(s) typeVirtual NetworkSubnetAssign NSG and public IPDuring the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend blocking internet access for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.Click Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowConfirm assigning the plan to the device(s)Wait for the plan to be assigned until you see a confirmation banner on the pageClick FinishFrom Standby Image OverviewLog in to the Management Console under a SuperUser or Manager accountNavigate to Continuity > Standby ImageClick Add to PlanSelect Standby Image (Azure)You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the planRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding:
    b. Top bar menu
    c. Top bar menu

Recovery Reports

When the device(s) assigned to the plan have **Successful recovery report email** or **Failed recovery report email** recipient

address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox.

Here is an example report with Cove branding:

Cove Data Protection

Recovery completed

Recovery plan: **Standby Image (ESXi)**

Last recovery session completed successfully: April 16 2024 3:45:39 AM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Workstation
Operating system	Windows 10 Enterprise (19045), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 16 2024 3:45:39 AM
Recovery status	Completed
Recovery duration	1 hour, 50 minutes and 18 seconds
Recovery location	ESXi.
Restore frequency	Each backup session
Recovery plan	Standby Image (ESXi)

BACKUP DETAILS USED FOR THE RESTORE

Backup session time	April 16 2024 3:35:44 AM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

BOOT TEST OVERVIEW

Screenshot verification	Not applicable
Boot check frequency	Off

Screenshot verification is not applicable

Here is an example **without** Cove branding:

Recovery completed

Recovery plan: **Standby Image (ESXi)**

Last recovery session completed successfully: April 16 2024 3:45:39 AM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	
Device name	
Machine name	
Device type	Workstation
Operating system	Windows 10 Enterprise (19045), 64-bit

RECOVERY OVERVIEW

Recovery session time	April 16 2024 3:45:39 AM
Recovery status	Completed
Recovery duration	1 hour, 50 minutes and 18 seconds
Recovery location	ESXi.
Restore frequency	Each backup session
Recovery plan	Standby Image (ESXi)

BACKUP DETAILS USED FOR THE RESTORE

Backup session time	April 16 2024 3:35:44 AM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

BOOT TEST OVERVIEW

Screenshot verification	Not applicable
Boot check frequency	Off

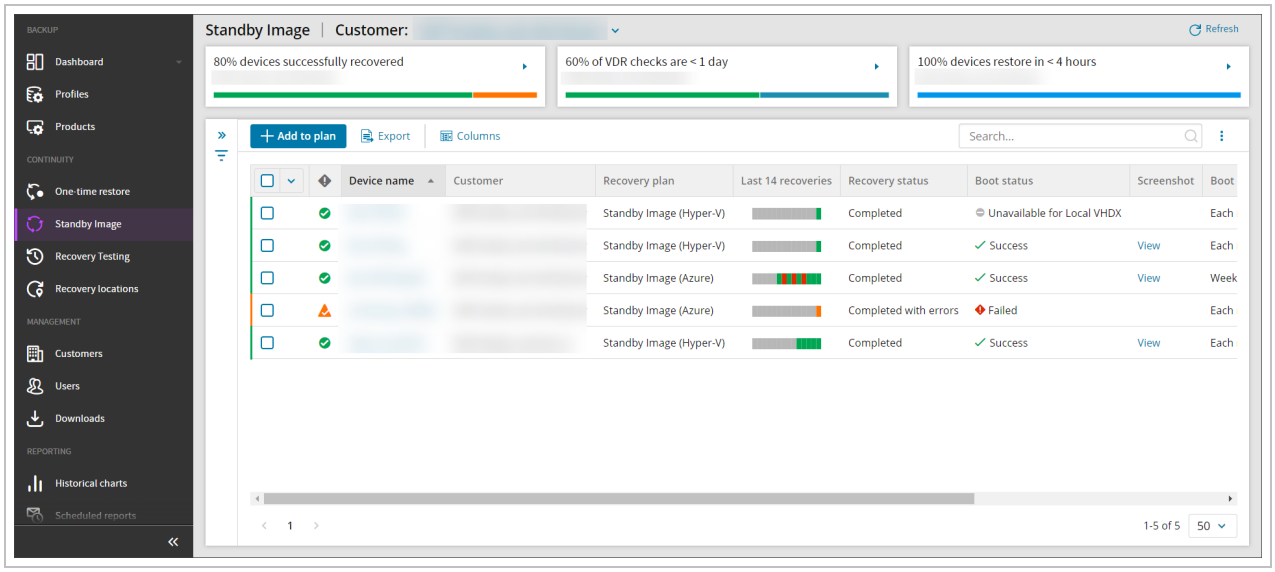
Screenshot verification is not applicable

Monitor Standby Image Devices

From the Management Console, you can view the dedicated Standby Image Overview by selecting **Continuity** > **Standby Image** from the vertical menu on the left hand side.

This page will list devices assigned to the Standby Image plans:

- Standby Image to Hyper-V
- Standby Image to Azure
- Standby Image to ESXi



From this dashboard, you will see a specified set of columns detailing information relevant to devices using the Standby Image plan, including the continuity history of the last 14 recoveries, the recovery status, boot status, and plan assigned, along with some other information.

If no devices are assigned to either Standby Image plan, the dashboard will display a message to advise, along with a button to add devices to a plan.

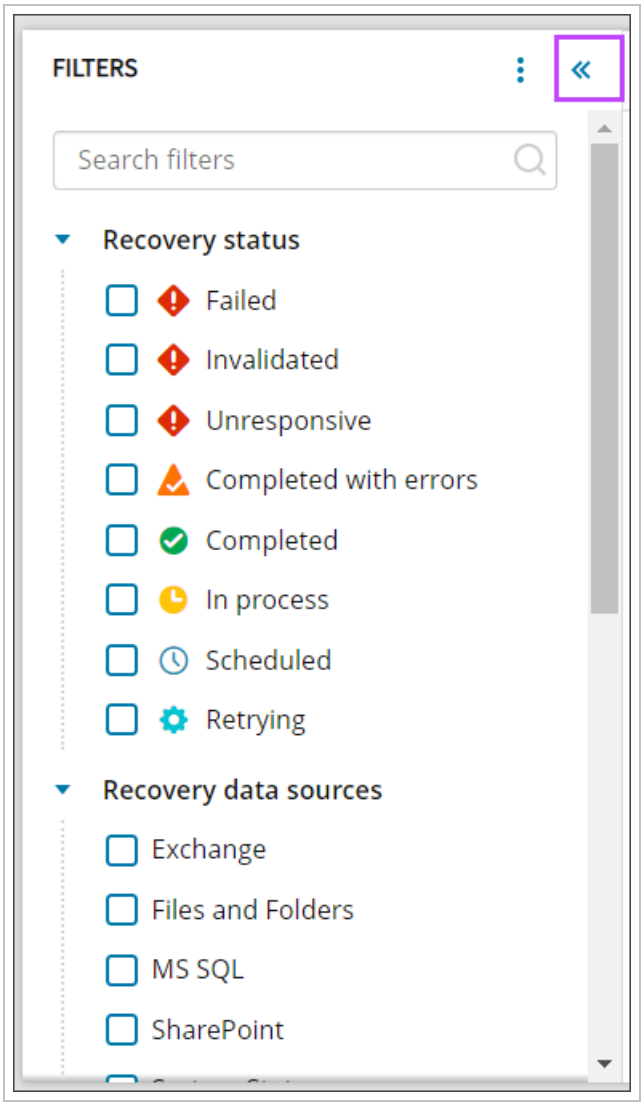
> If a device is assigned to **multiple** plans (i.e. **Standby Image to Hyper-V**, **Standby Image to Azure** and **Standby Image to ESXi**), the device will be listed for each instance of a plan and can be told apart by the **Recovery Plan** column.

Searching

Searching within the Standby Image overview can be done by using the search box over to the right hand side of the page, just above the devices list. The search can be performed by any text field.

Filtering

The Standby Image overview also includes functionality to filter devices using the filter menu to the left of the device list and can be displayed or hidden by clicking the double arrows.



From this menu, you can filter by:

Recovery status

- **Failed** - The recovery session has failed
- **Invalidated** - Device was moved to an inappropriate partner and so the session has failed
- **Unresponsive** - The recovery session was initiated but did not receive updates for at least 30 minutes because the recovery location restarted or was offline.
- **Completed with errors** - The recovery session completed, but encountered errors
- **Completed** - The recovery session completed with no errors
- **In process** - The recovery is currently in progress
- **Scheduled** - Devices just added to a recovery plan and are waiting for their first recovery session or devices where restores were paused and have since been resumed will display as scheduled
- **Retrying** - A restore session was not finished so the system is trying the restore again

Recovery data sources

- Exchange
- Files and Folders
- MS SQL
- SharePoint
- System State

Recovery session statistics

- Boot check frequency
  - Off
  - Every recovery session
  - Daily
  - Weekly
  - Biweekly
  - Monthly
- Boot Check Status
  - Success
  - Failed
  - Off
  - Unavailable for Local VHDX
- Continuous restores
  - Running
  - Paused
- Duration of the last completed recovery session
  - Sliding scale from 0 to unlimited

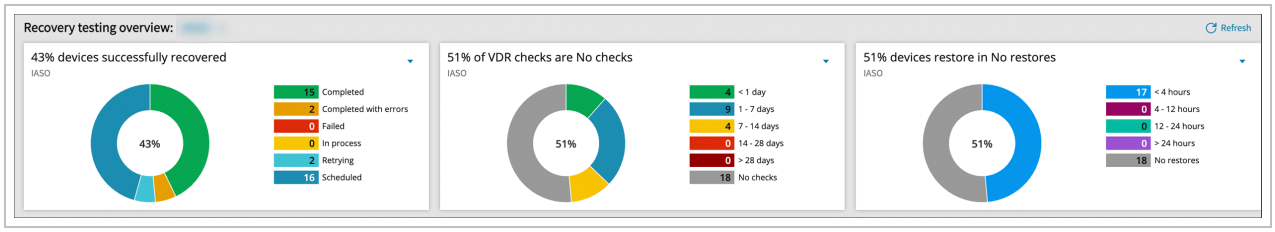
  in minutes
- Number of errors of the last completed recovery session
  - Sliding scale from 0 to unlimited
- Number of restored files
  - Sliding scale from 0 to unlimited
- Number of selected files
  - Sliding scale from 0 to unlimited
- Recovery Location name
  - Select the recovery location from a dropdown
- Recovery Plan
  - Standby Image (Hyper-V)
  - Standby Image (ESXi)
  - Standby Image (Azure)
- Restored size
  - Sliding scale from 0 to unlimited

  in KB and GB

- Recovery testing status of the last completed recovery session
  - Failed
  - Completed with errors
  - Completed
- Screenshot
  - Available
  - Not Available
- Selected size
  - Sliding scale from 0 to unlimited
  in KB and GB
- Timestamp of the last completed recovery session
  - Quick Picks of:
    - Last day
    - 1 - 7 days
    - 7 - 14 days
    - 14 - 28 days
    - > 28 days
  - Custom range, select a stat date and time and an end date and time

Widgets

Three widgets can be maximized at the top of the page, which allow for further filtering:



Device recovery status

This widget allows you to filter the devices by recovery status:

- Completed
- Completed with errors
- Failed
- In process
- Retrying
- Scheduled

VDR checks time frame

This widget allows you to see the percentage of devices whose recovery check completed within the following day ranges:

- < 1 day
- 1 - 7 days
- 7 - 14 days
- 14 - 28 days
- > 28 days
- No checks

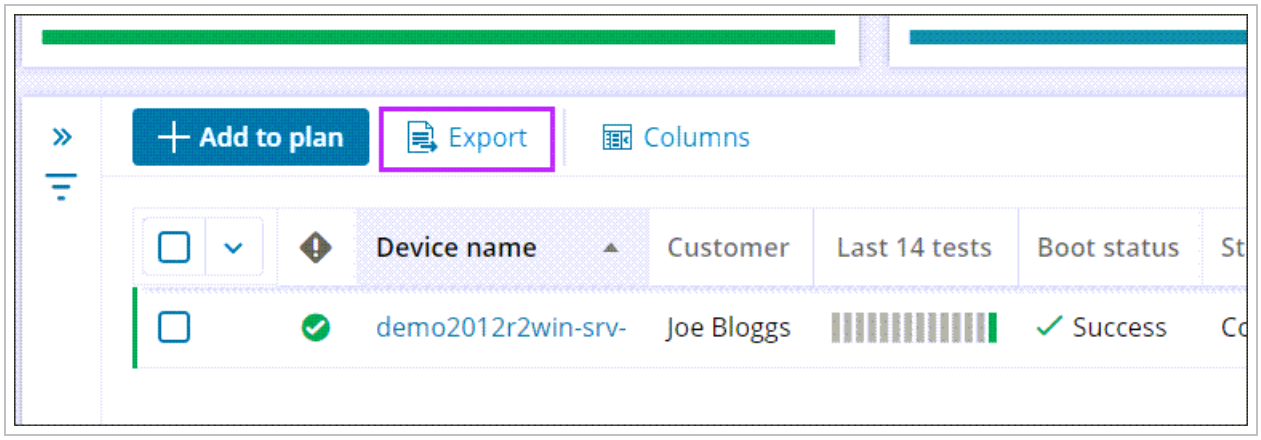
Device restore time frame

From this widget, you can filter devices by the how recent restores are done by the following time frames:

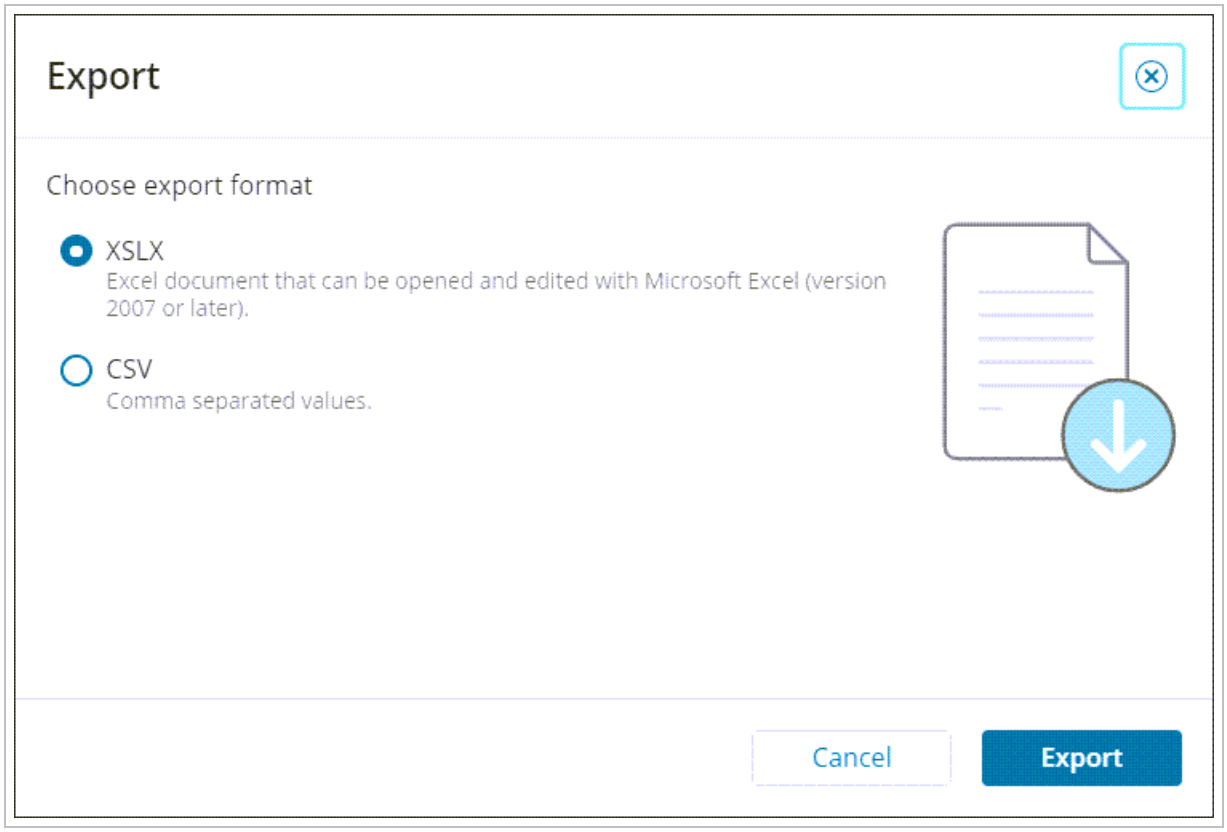
- < 4 hours
- 4 - 12 hours
- 12 - 24 hours
- > 24 hours
- No restores

Exporting

You may export a list of devices currently assigned a plan by clicking **Export**

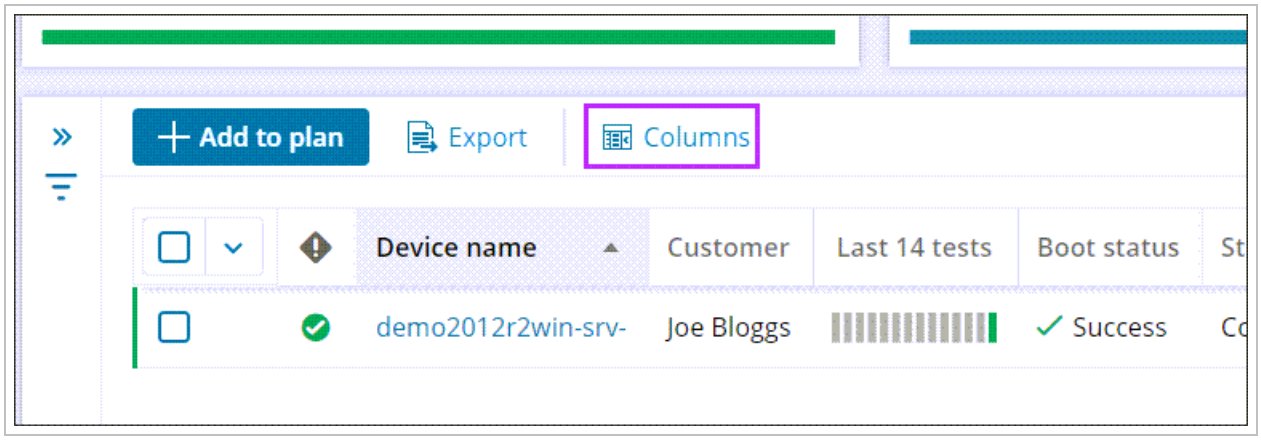


This will then provide a separate dialog where you can choose to export in either XSLX or CSV.

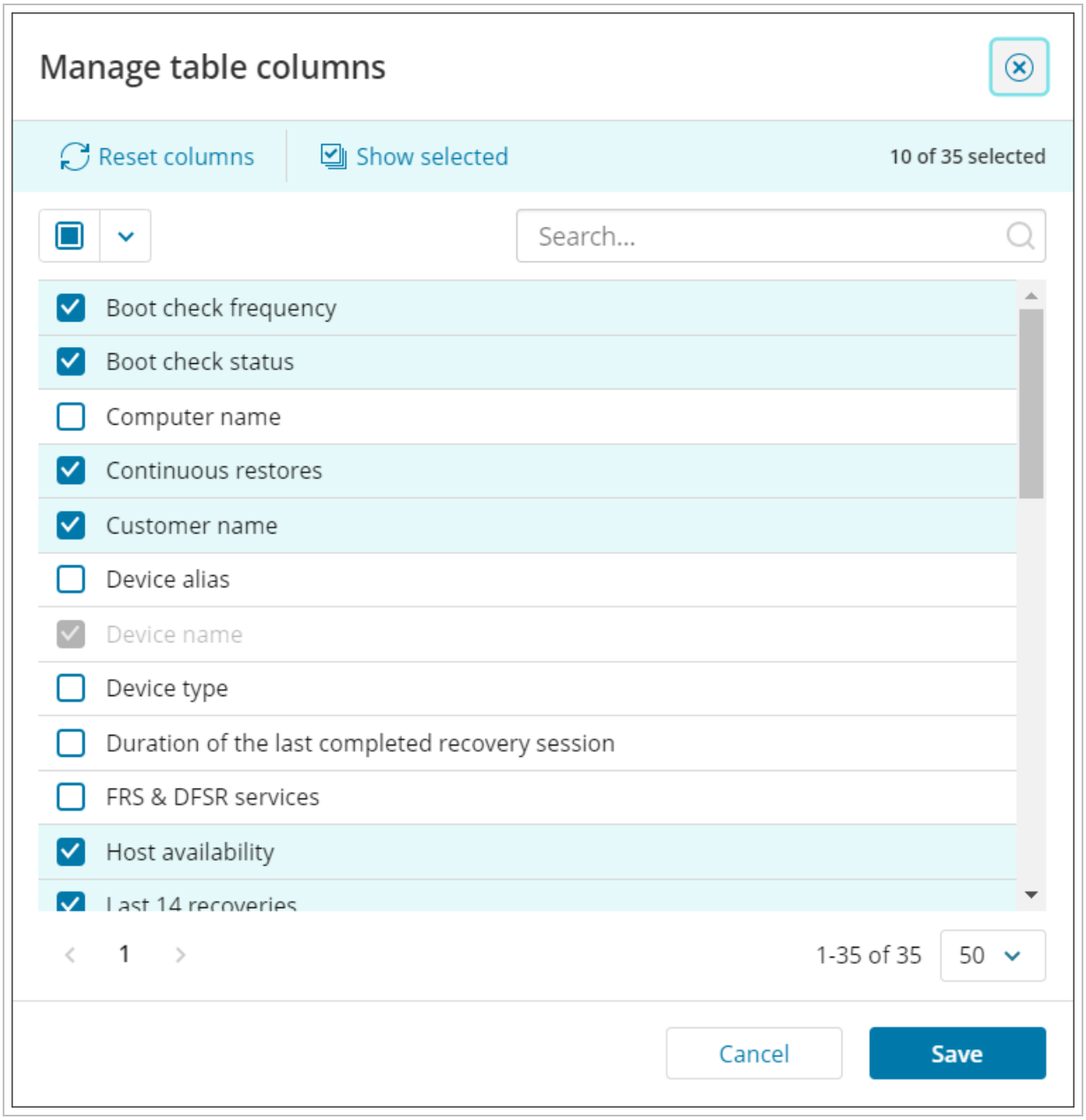


Manage Table Columns

Management Console allows you to manage the tables columns that can be seen within the Standby Image overview.



In the Manage table columns dialog, you can select and deselect columns based on the information you wish to view from the overview.

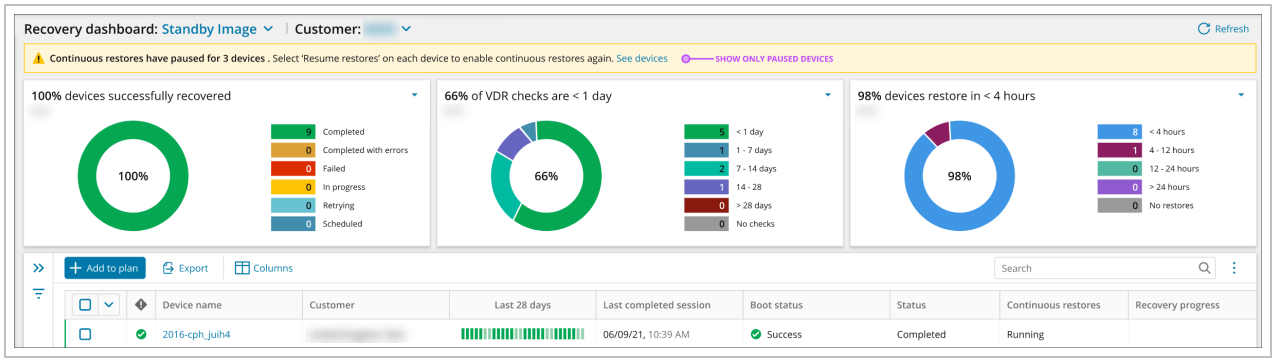


Pause Standby Image recovery

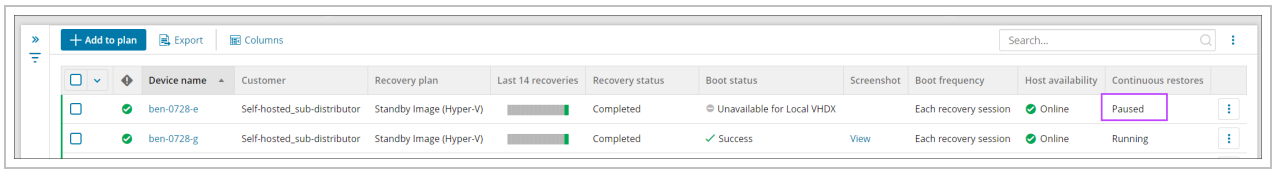
Once a Standby plan has been assigned to a device, the continuous restores can be paused and restarted. Pause or resume restores functionality there to provide a possibility to use the restored machine for failover in case of disaster.

> If a restored Virtual Machine is turned on manually, the Standby Image restore will automatically pause.

Pausing and restarting continuous restores can done be for single or multiple devices at a time. Once devices have been paused, a banner will be displayed at the top of the page to advise.

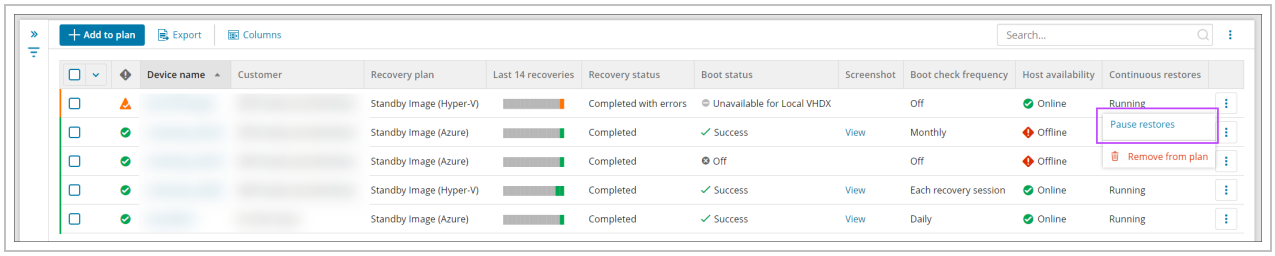


Click **See devices** to filter the devices list by **Continuous Restore: Paused** to only devices which are currently paused.



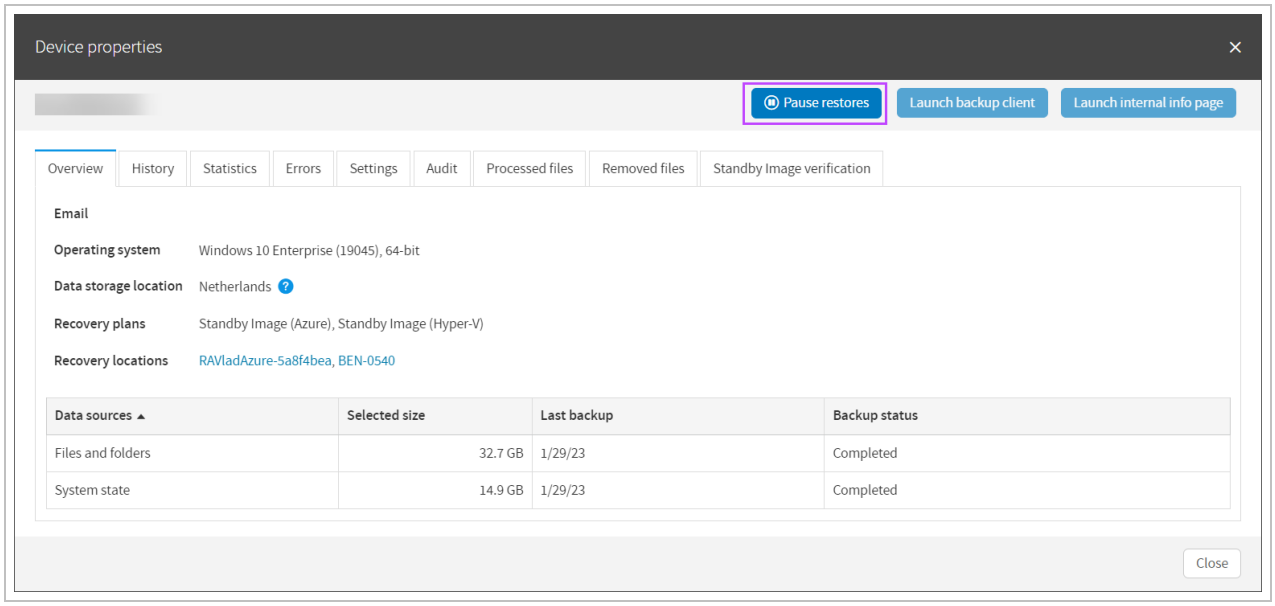
For single devices

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Click the menu action button to the right of the device (Three vertical dots)
4. Select **Pause Restores** or **Resume Restores**



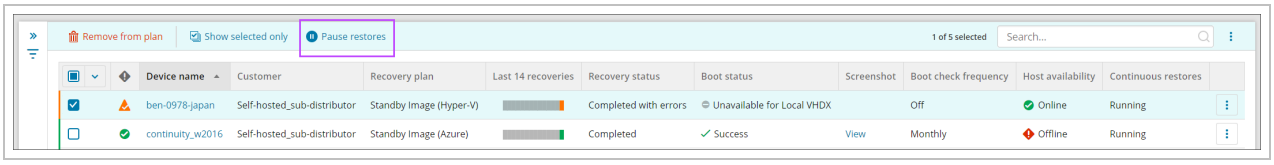
> This will differ depending on whether the plan is currently active, or has been paused already

It is also possible to pause restores from the Device Properties window:



For single or multiple devices

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Tick the checkbox for any devices that need paused from the list
4. In the top panel, select **Pause Restores** or **Resume Restores**



> This will differ depending on whether the plan is currently active, or has been paused already

Accessing device properties

The Device Properties window displays several tabs detailing information on the Backup device. Full details of the contents of each tab can be found on the Device management in Management Console page.

The two that are the most commonly used with Standby Image are the **Settings** tab and the **Standby Image Verification** tab.

Settings Tab

Broken into several sections, this tab contains:

General

This section provides the main device details:

- **customer** - Who device belongs to, can be changed to move the device to a different customer
- **Device name** - Cannot be changed

- **Installation key** - Cannot be changed
- **Creation date** - Cannot be changed
- **Expires on** - Can be amended to a date in the future, or set to **'no expiration'** if required

> You may also see the Request Passphrase button here if the device is set up to use this instead of its own security code/encryption key

Backup

This section contains:

- **Backup product** - Use the dropdown to change the Product used by the device
- **Profile** - Use the dropdown to change the Profile applied to the device

Recovery

On a device assigned to the Standby Image plan, this section will allow you to see plan in use and amend some details of this:

- **Recovery Plan** - Standby Image (Each backup session)
- **Recovery Location** - Cannot be changed from this panel. To change this, see Add Device to Recovery Location
- **Successful recovery report email** - Specify the email address(es) that will receive reports when the most recent Recovery as per the assigned plan has been successful
- **Failed recovery report email** - Specify the email address(es) that will receive reports when the most recent Recovery as per the assigned plan has failed
- **Remove Cove branding** - toggle branding of the email reports on or off
- **Restore format** - This option will not be available for Standby Image to Azure.
  - For **Standby Image to Hyper-V**, this is a choice between **Hyper-V** or **Local VHDX**
  - For **Standby Image to ESXi**, this is a choice between **ESXi** and Local **VHDX**

    > Further settings displayed are dependent on the Restore Format selected for the device. These settings can be changed as required.

> All Recovery Plans associate to the device will be included here, and can be minimized or expanded by clicking the arrow to the left of the plan name.

Device properties

Launch backup client | Launch internal info page

Overview | History | Statistics | Errors | Settings | Audit | Processed files | Removed files | Standby Image verification

General

Customer

Device name

Installation key

Creation date 2/21/23

Expires on 04/18/24 No expiration

Backup

Product _test

Profile -servers

Recovery

Standby Image (ESXi)

Recovery plan Standby Image (ESXi)

Recovery location ESXiRA

Successful recovery report email e.g email@email.com

Failed recovery report email e.g email@email.com

Remove Cove branding OFF

Restore format ESXi VMDK

Boot check frequency Daily

FRS and DFSR services OFF

Local Speed Vault OFF

CPU cores 4

RAM (GB) 4

VM Subnet mask Enter a custom subnet mask to the new virtual mac

VM gateway Enter a custom gateway to the new virtual machine

VM DNS server Enter a DNS server to be used on the restored mach

Separate multiple DNS servers with a comma or semicolon

VM IP address Enter a custom IP address to the new virtual machir

Standby Image (Hyper-V)

Recovery plan Standby Image (Hyper-V)

Recovery location BEN-6478

Successful recovery report email e.g email@email.com

Failed recovery report email e.g email@email.com

Remove Cove branding OFF

Restore format Hyper-V Local VHDX

Boot check frequency Daily

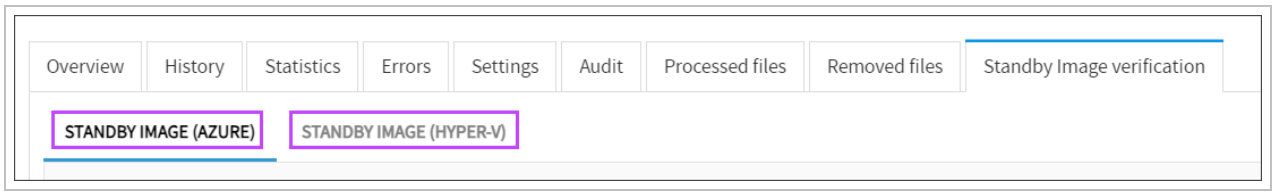
FRS and DFSR services OFF

Local Speed Vault OFF

Standby Image Verification Tab

To view statistics of the Standby Image and check the screenshots to ensure this has been successful, you can view this by following one of the below methods.

All plans associated to the device will have their own sub-tabs that can be selected to view the appropriate screenshot:



From Device Properties

1. Log in to the Management Console
2. Click the device name on either the Backup Dashboard or the Standby Image overview to open the Device Properties
3. Navigate to the **Standby Image Verification** tab

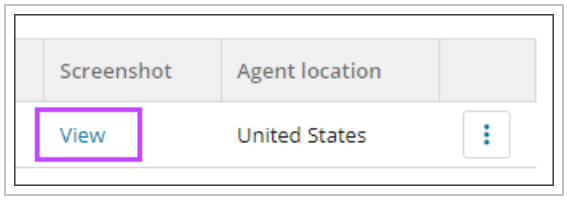
From Standby Image Overview

The Standby Image Verification tab can be viewed from the Standby Image overview in one of two ways:

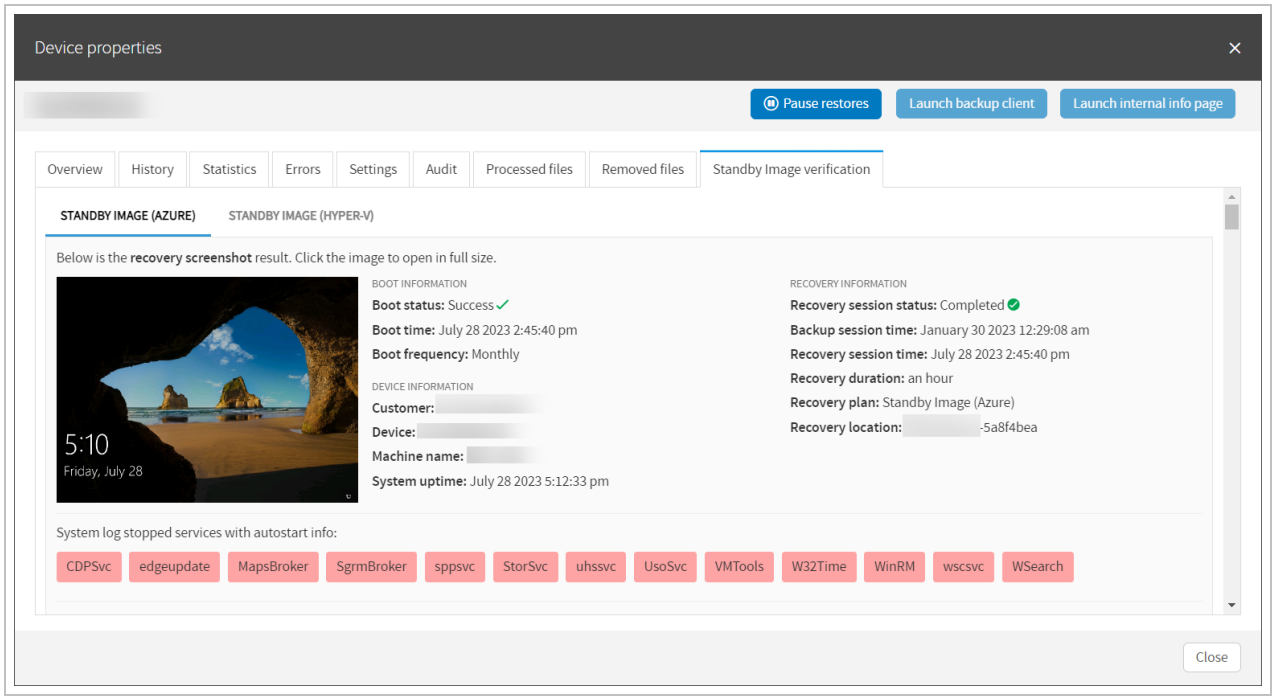
- Via theScreenshot column
- Via the Last 14 recoveries column

Screenshot column

1. Log in to the Management Console
2. Navigate to **Continuity** > **Standby Image**
3. Click **View** under the Screenshot column

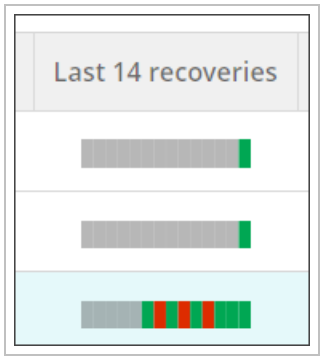


4. This will take you in to the Device Properties dialogue, where you will now see the **Standby Image Verification** tab:

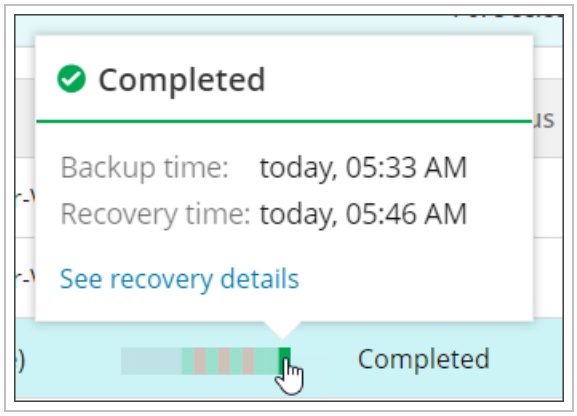


Last 14 recoveries column

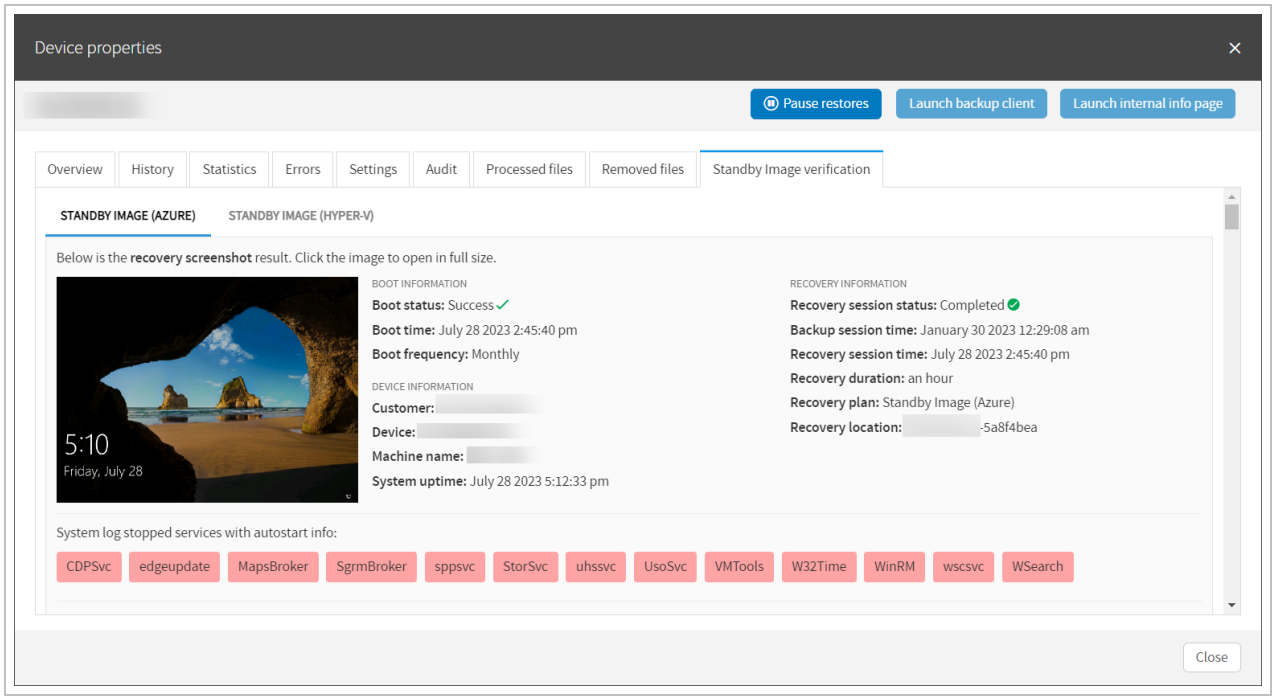
1. Log in to the Management Console
2. Navigate to **Continuity** > **Standby Image**
3. Hover your mouse over the most recent colored bar in the Last 14 recoveries column



4. Click **See recovery details** in the popup box that appears



5. This will take you in to the Device Properties dialogue, where you will now see the **Standby Image Verification** tab:



Standby Image Use in Case of Disaster

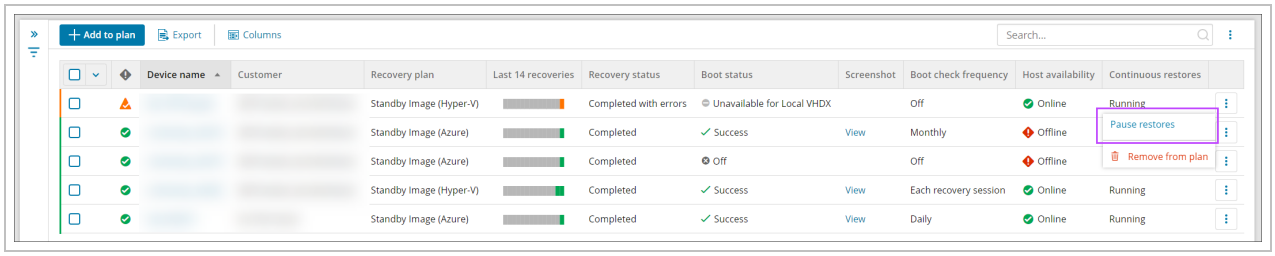
Using Standby Image, you can continuously restore the most recent backup to a secure location, either Hyper-V or to the Azure Cloud. In case of disaster, the restored machine can be used for failover by following the relevant procedures below.

For Hyper-V

To use a Standby Image to Hyper-V:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Find the affected device and click the menu action button to the right of the device (Three vertical dots)

4. Select **Pause Restores**



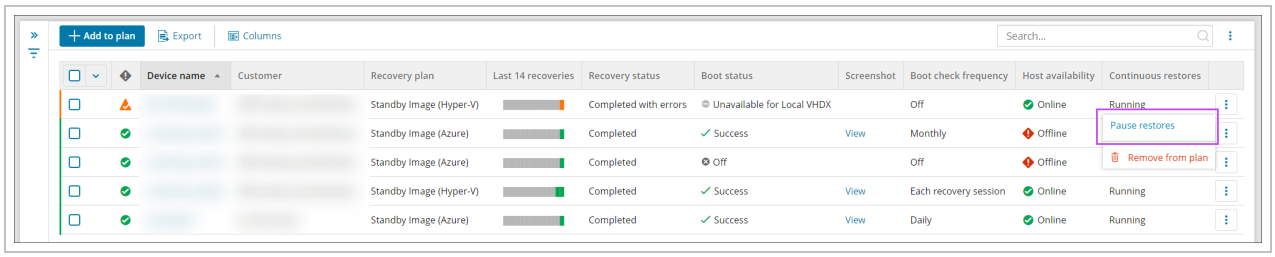
> By doing so, this halts further restoration for the device and prevents accidental damage to the Standby Image

5. Once paused, connect to the device hosting the Recovery Location
6. Navigate to the Hyper-V manager
7. Find the virtual machine created for the standby image device and select **Start**

For ESXi

To use Standby Image to ESXi:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Find the affected device and click the menu action button to the right of the device (Three vertical dots)
4. Select **Pause Restores**



> By doing so, this halts further restoration for the device and prevents accidental damage to the Standby Image

5. Connect to the device (virtual machine or dedicated server/host) by either:
   a. Sign in to the **vCenter Server** by using the **vSphere Client**
   b. Navigate to **Inventory** in the menu and find the virtual machine created
   c. Power it on and click **Launch remote console**

   Or

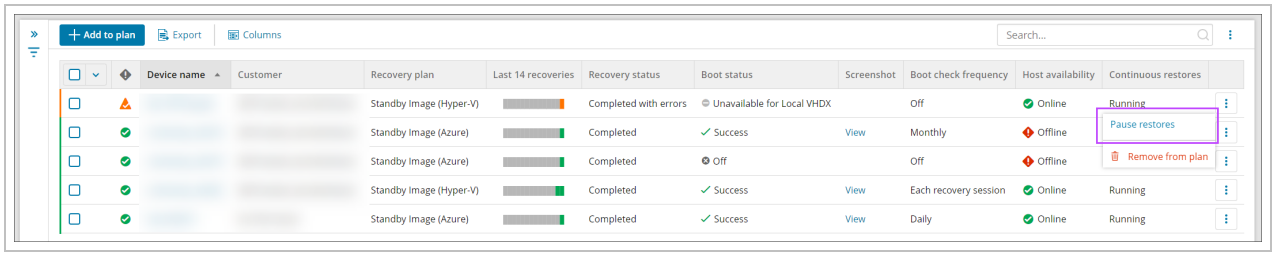
   a. If restoring to the ESXi server/host directly, login to the dedicated server/host machine

For Azure

To use a Standby Image to Azure:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Standby Image**
3. Find the affected device and click the menu action button to the right of the device (Three vertical dots)

4. Select **Pause Restores**



> By doing so, this halts further restoration for the device and prevents accidental damage to the Standby Image

5. Sign into Microsoft Azure
6. Locate the machine associated to the device in Cove Data Protection. Navigate to the "Locks" section of this virtual machine and remove any existing locks.
7. Power on the machine hosted in Azure

Recovery Testing

Cove Data Protection (Cove)'s Recovery Testing service is a scheduled, automated service to test the recoverability of critical devices. There is no need for manual setup or local resources.

Choose to run Recovery Testing restore every 14 or 30 days and with each restore, a virtual machine is automatically created. Once the Virtual Machine has been created, we will boot it and create a screenshot to check that the Virtual Machine is bootable, then send this screenshot to the Management Console so that users can check it.

> The virtual machines that are created as part of Recovery Testing are **purged** once the restore is completed and the screenshot taken. This means these restored virtual machines are **not accessible** by the user.

Limitations

- Only devices with Backup Manager version 17.4 and above are supported for Recovery Testing
- Software-only devices are not compatible with Recovery Testing
- Recovery Testing cannot be used on the RMM integrated version of Backup (Managed Online Backup)
- There is a size restriction of <= 2 TB selected size per device. You can opt to use "Restore OS-disk only" (available only in standalone version) feature to bypass this limitation
- Recovery Testing restores only System State, Files and Folders, and MS SQL
- Recovery Testing is not available for devices with disabled ‘Virtual disaster recovery’ feature in the assigned product
- Recovery Testing does **not** support 32-bit architecture
- Maximum supported capacity for virtual hard disks is **64 TB** per disk
- Devices cannot be added to a Recovery Testing plan if already assigned to a Standby Image plan

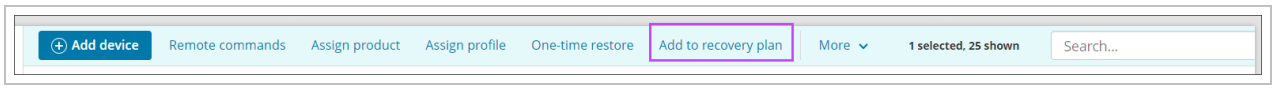
Enable Recovery Testing

> Devices cannot be added to a **Recovery Testing plan** if already assigned to a **Standby Image plan to Hyper-V** or **Standby Image to Azure plan**.

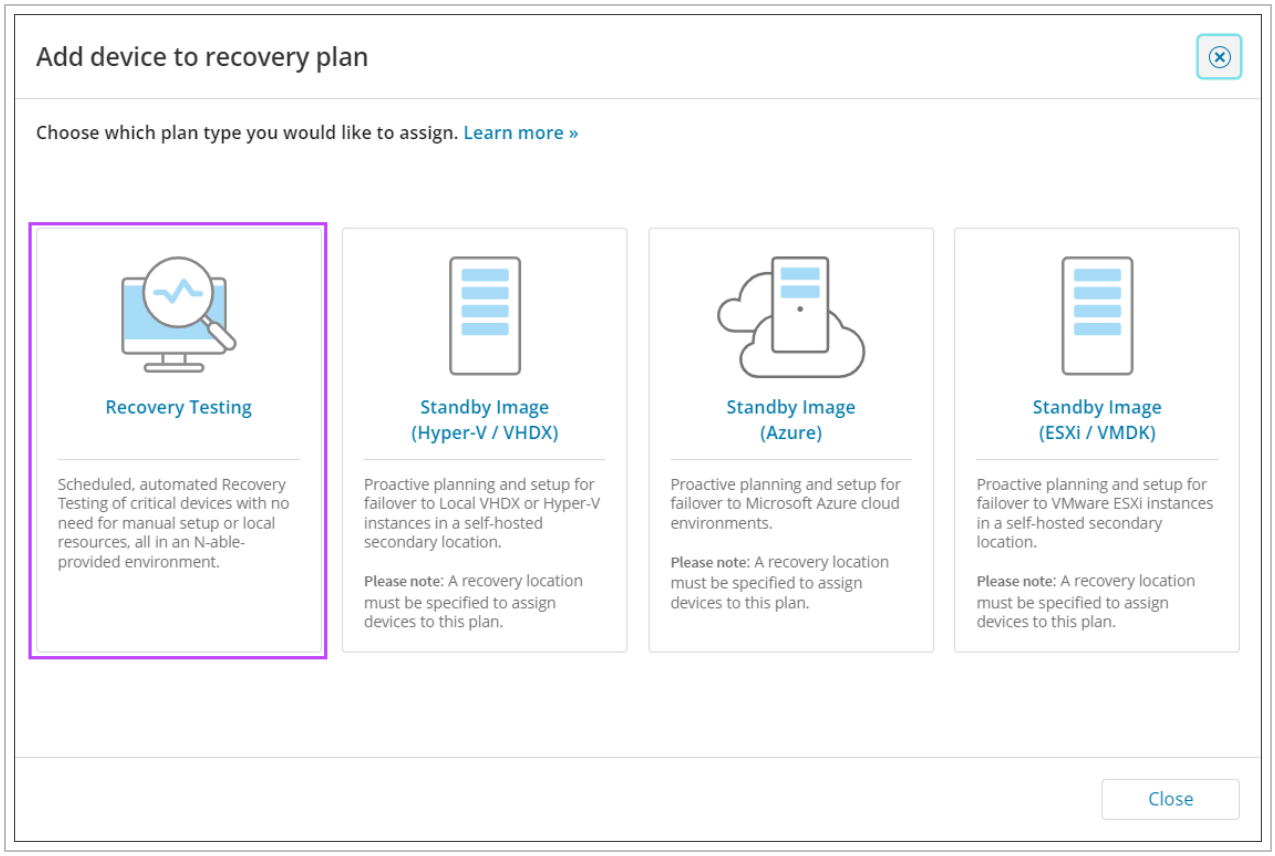
From Main Dashboard

To enable Recovery Testing on a device from the Management Console's main Dashboard, follow the steps below:

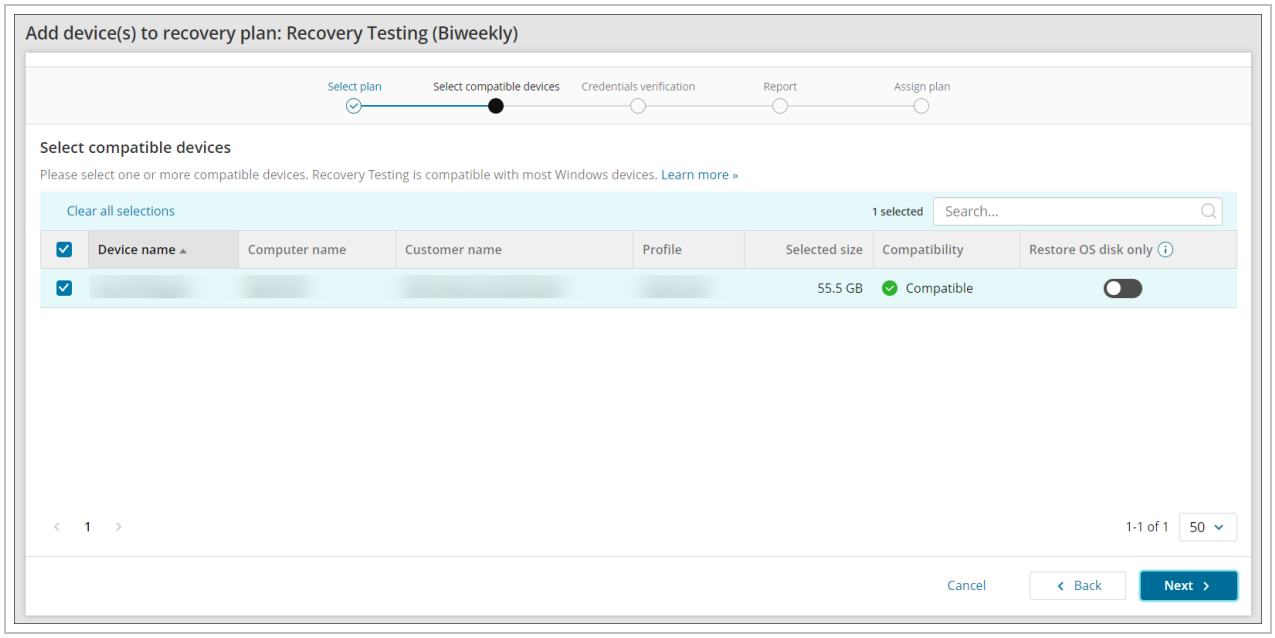
1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan to
3. Click **Add to recovery plan** from the Toolbar



4. Select **Recovery Testing**



5. Select the **customer** from the dropdown
6. Choose the frequency of the plan to assign:
   - **Biweekly** - This will automate the recovery with fortnightly boot testing and screenshot creation (every 14 days)
   - **Monthly** - This will automate the recovery with monthly boot testing and screenshot creation (every 30 days)
7. Click **Next**
8. Confirm the compatibility of devices and the selected size of the device's data and click **Next**



9. If you wish to skip all data drives, enable **Restore OS disk only**

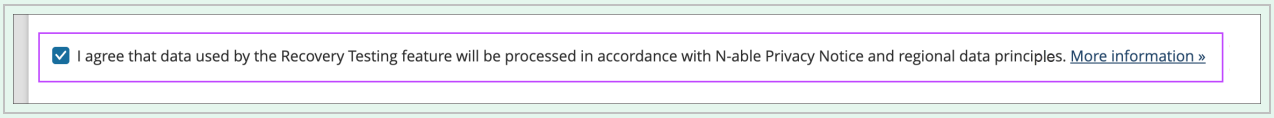
> This will restore the system drive and check the machine's bootability, but it will not restore the data drives.

> This function will be automatically enabled if the device is incompatible due to exceeding the 2TB selected size limitation

10. Enter the security code/encryption key or passphrase for the device(s). This can be either:
    - **Private encryption key** - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryption
    - **Passphrase encryption** - These are generated on demand for automatically installed devices. You can find information on this here

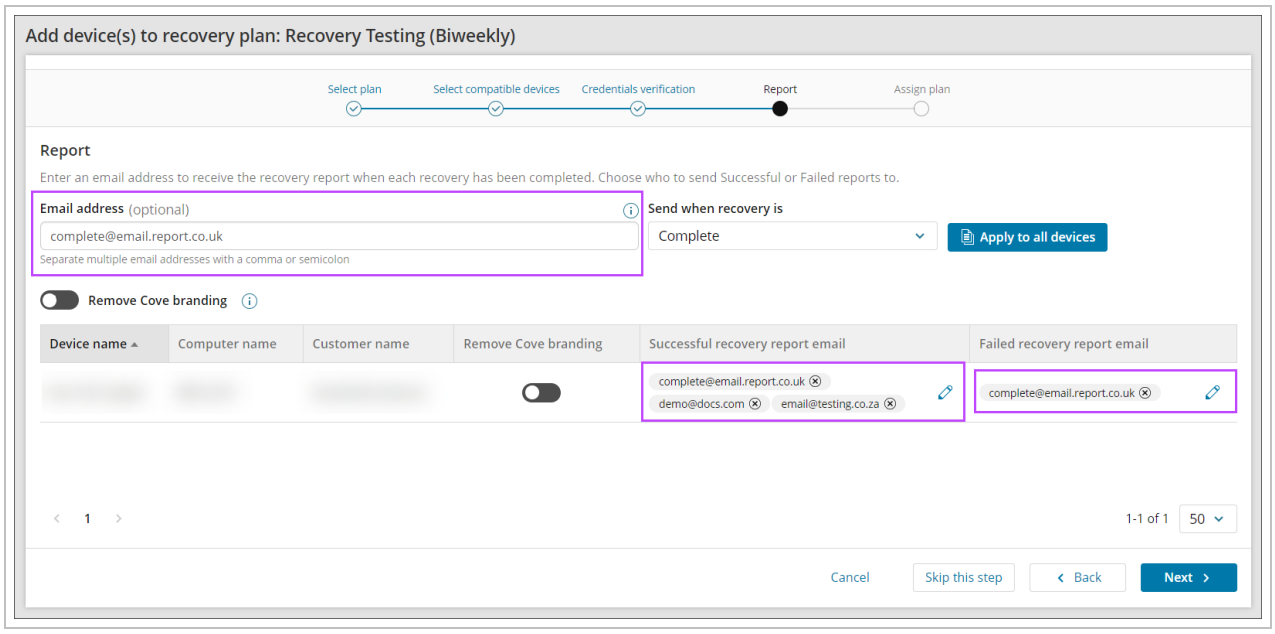
> If you are logged in as a security officer, this will be detected automatically.

> Any customer based in the EU (except Germany) will be required to agree to the policies linked.



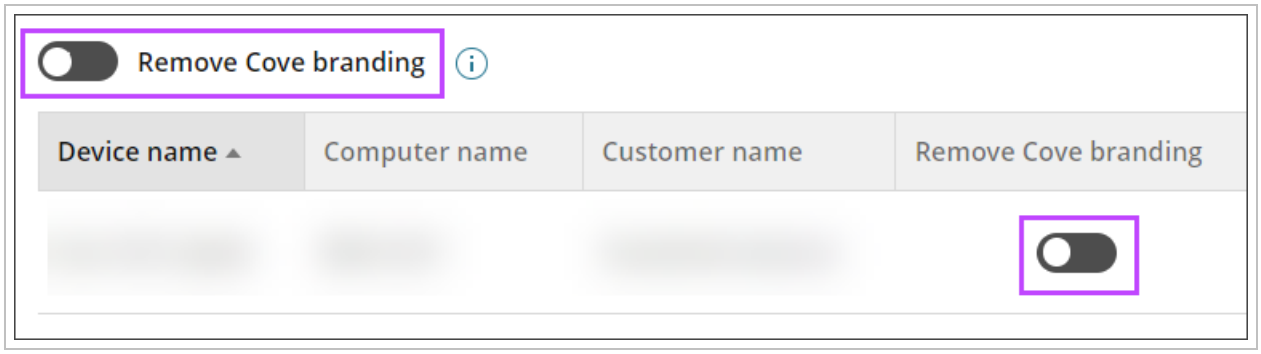
11. Click **Next** to progress to the **Report** window to enter one or more email addresses to receive a report when:
    a. The recovery is complete (Successful or Failed)
    b. The recovery was successful
    c. The recovery failed

> Multiple addresses should be separated using a comma or semi-colon

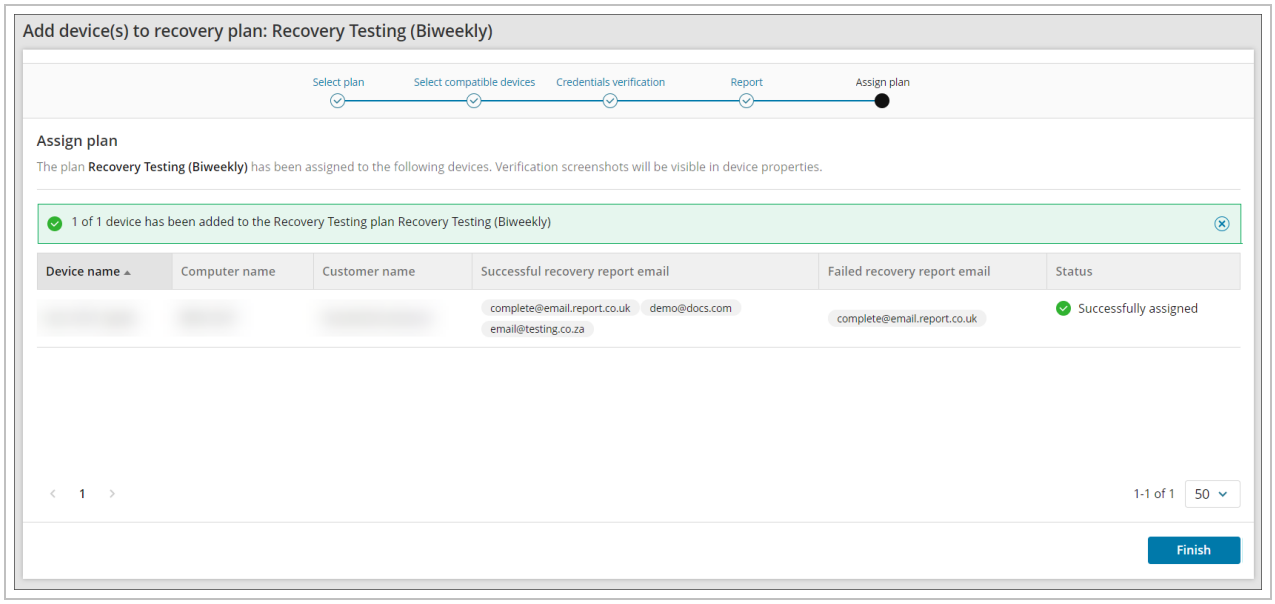


> If you do not want to add an email address to receive reports, click **Skip this step**

12. To remove all branding from the reports, use the **Remove Cove branding** toggle per device, or above the device list to apply the changes to all devices in this window



13. Select **Next** to enable the plan on the selected devices
14. You will now see the status of the plan has changed to **Completed** and the banner shows the number of devices added to the plan.



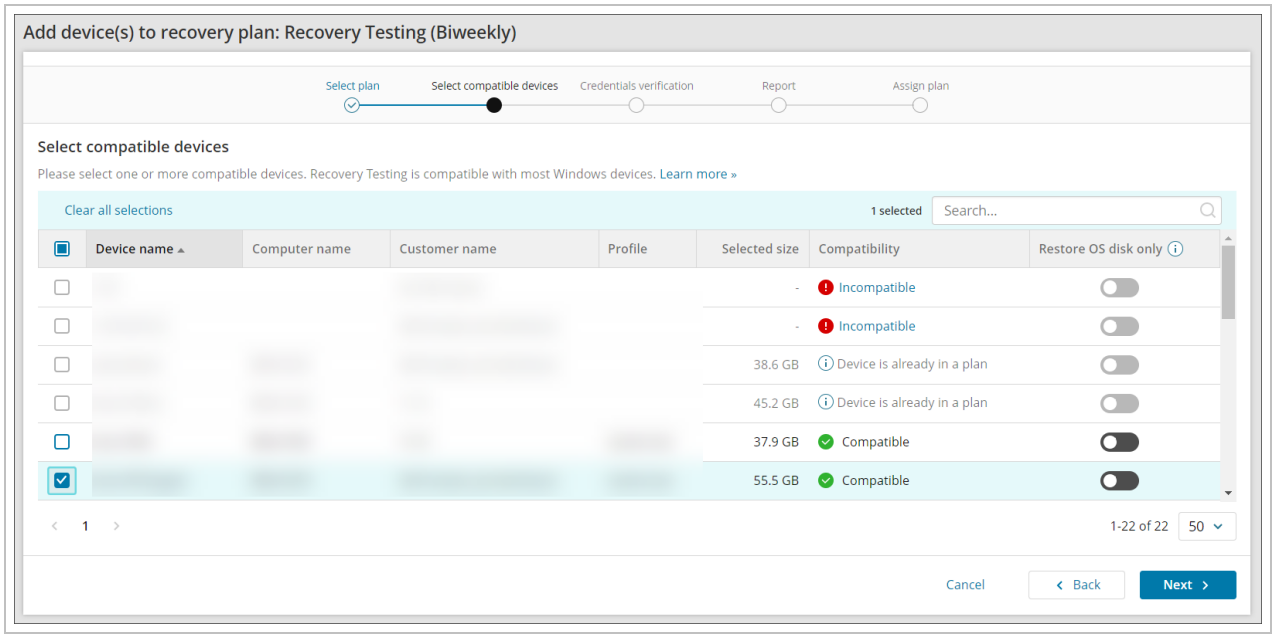
15. Click **Finish** to complete the process

From Recovery Testing Overview

To add Recovery Testing to devices from the dedicated Recovery Testing Overview:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Recovery Testing**
3. Click **Add to Plan**
4. Select the customer the device(s) you wish to apply the Recovery Testing plan belong to
5. Choose the restore frequency
    - Biweekly (every 14 days)
    - Monthly (every 30 days)
6. Click **Next**

7. Select all devices to apply the recovery testing plan



> In this window, it is possible to search compatible devices by Device Name, Customer Name and Profile

8. If you wish to skip all data drives, enable **Restore OS disk only**

> Use this function if the device is otherwise incompatible due to exceeding the 2TB selected size limitation

9. You will now be taken to the Add device to plan wizard. Follow the steps to enter the devices Security Code/Encryption Key starting at step #10 where you can now follow the above instructions to add the device to the plan

Recovery reports

When the device(s) assigned to the plan have **Successful recovery report email** or **Failed recovery report email** recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox.

Here is an example report **with** Cove branding:

Cove Data Protection

Recovery completed

Recovery plan: **Recovery Testing (Biweekly)**

Last recovery session completed successfully: March 20 2024 3:01:33 PM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	[redacted]
Device name	
Machine name	
Device type	Server
Operating system	Windows Server 2016 Standard Server (14393), 64-bit

RECOVERY OVERVIEW

Recovery session time	March 20 2024 3:01:33 PM
Recovery status	Completed
Recovery duration	21 minutes and 58 seconds
Recovery location	Germany
Recovery plan	Recovery Testing (Biweekly)
Screenshot verification	Completed

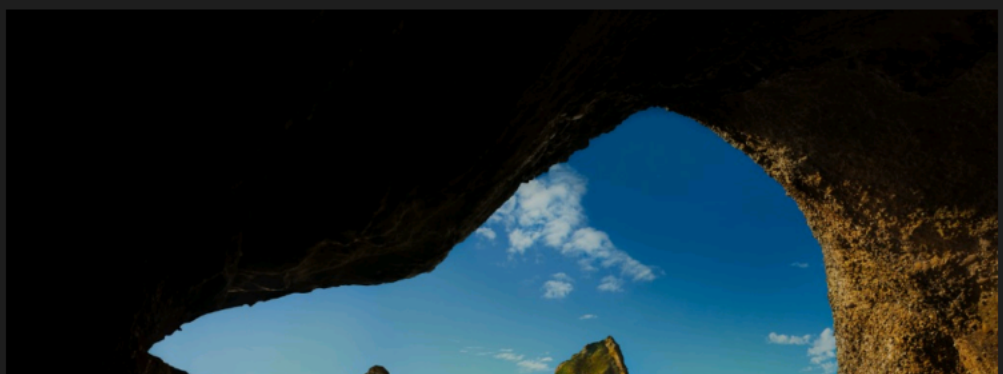
BACKUP DETAILS USED FOR THE RESTORE

Backup session time	March 20 2024 0:05:34 PM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

Below is a screenshot of the virtual machine created during the boot phase of recovery.



Here is an example **without** Cove branding:

Recovery completed

Recovery plan: **Recovery Testing (Biweekly)**

Last recovery session completed successfully: March 20 2024 3:01:33 PM

Hello,

This is your automated recovery report.
Additional details can be found in the **Management Console** Device Properties.

DEVICE OVERVIEW

Customer	[redacted]
Device name	
Machine name	
Device type	Server
Operating system	Windows Server 2016 Standard Server (14393), 64-bit

RECOVERY OVERVIEW

Recovery session time	March 20 2024 3:01:33 PM
Recovery status	Completed
Recovery duration	21 minutes and 58 seconds
Recovery location	Germany
Recovery plan	Recovery Testing (Biweekly)
Screenshot verification	Completed

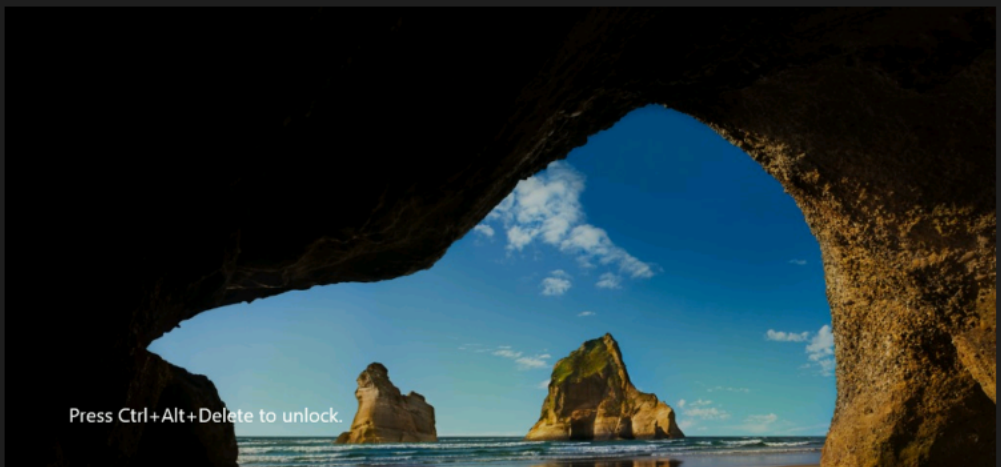
BACKUP DETAILS USED FOR THE RESTORE

Backup session time	March 20 2024 0:05:34 PM
Backup status	Completed

DATA SOURCE BACKUP STATUS

Files and Folders	Completed
System State	Completed

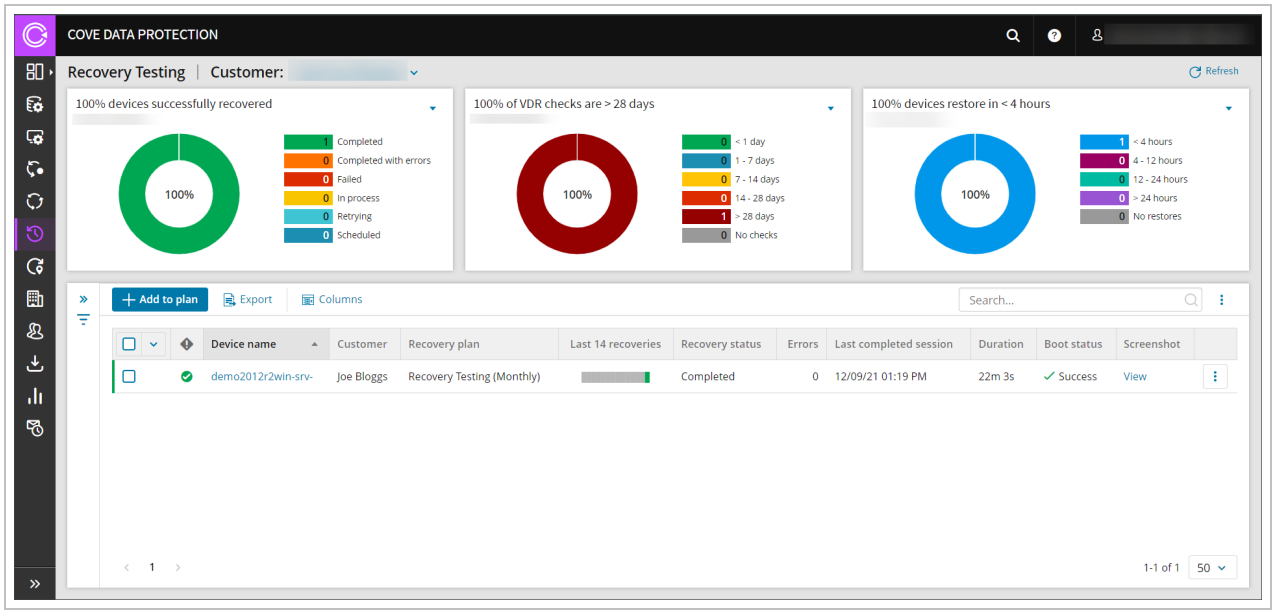
Below is a screenshot of the virtual machine created during the boot phase of recovery.



Monitor Recovery Testing Devices

From Recovery Testing Overview

From the Management Console, you can view the dedicated Recovery Testing overview by selecting **Continuity** > **Recovery Testing** from the vertical menu on the left hand side.

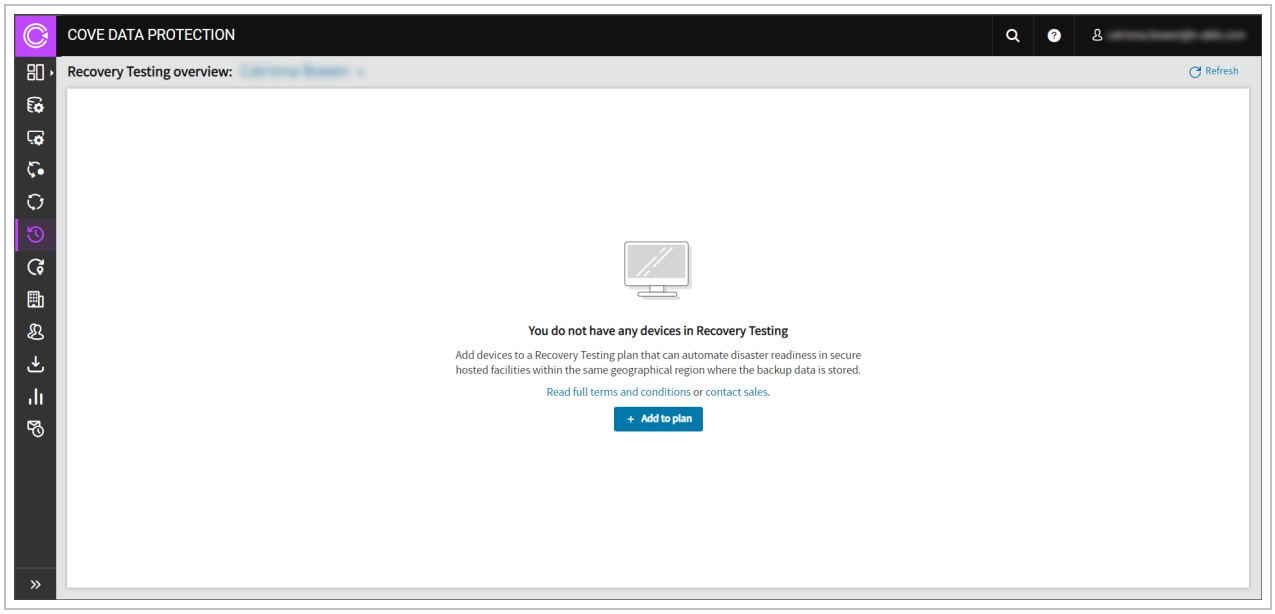


From this overview, you will see a specified set of columns detailing information relevant to Recovery Testing, including the continuity history of the last 14 recoveries, the status, and plan, along with some other information.

You can distinguish between Recovery Testing plans by the **Recovery Testing Plan** column. You will see one of two plan names:

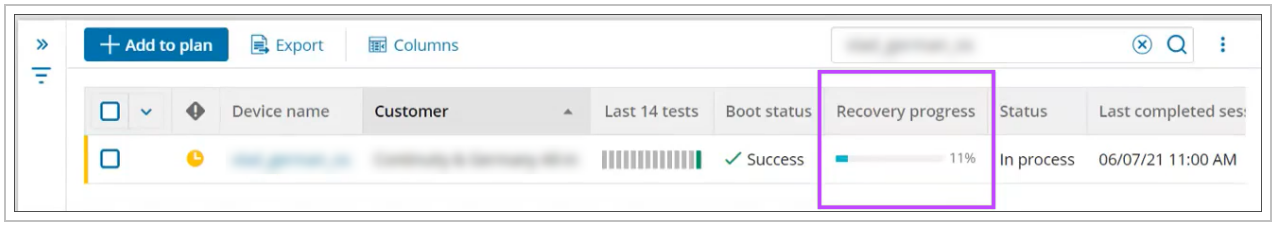
- Recovery Testing (Bi-Weekly)
- Recovery Testing (Monthly)

If no devices are assigned to the Recovery Testing, the overview will display a message to advise, along with a button to add devices to the plan.



Recovery Progress

From the Recovery Testing overview, the **Recovery Progress** column can be added, which will allow you to see the progress of the recovery as a percentage.



This column can be added by:

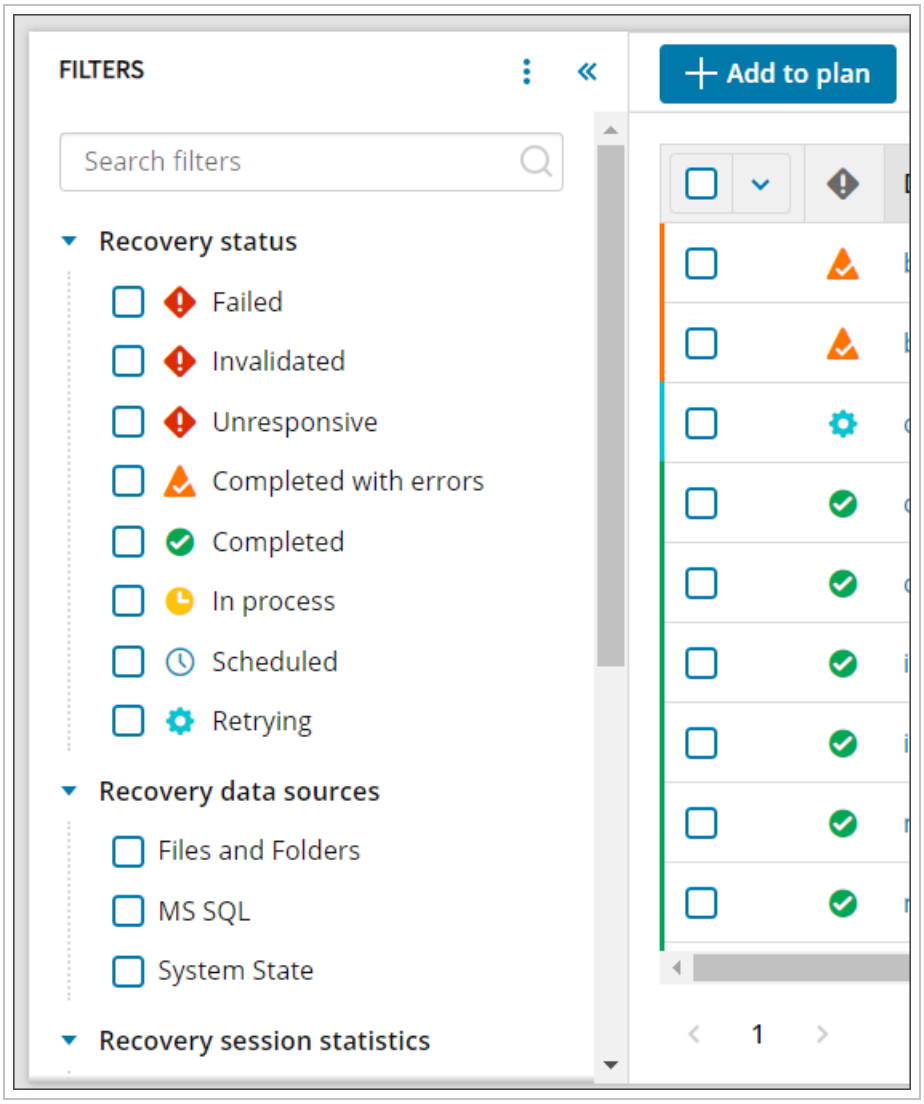
1. Selecting **Columns**
2. Search for and select **Recovery Progress**
3. Click **Save**

Searching

Searching within the Recovery Testing overview can be done by using the search box over to the right hand side of the page, just above the devices list. The search can be performed by any text field.

Filtering

The Recovery Testing overview also includes functionality to filter devices using the filter menu to the left of the device list and can be displayed or hidden by clicking the double arrows.



From this menu, you can filter by:

- Recovery status
  - Failed - The recovery session has failed
  - Invalidated - Device was moved to an inappropriate partner and so the session has failed
  - Unresponsive - The recovery session was initiated but did not get updates for at least 30 minutes and so the session has failed The recovery session was initiated but did not receive updates for at least 30 minutes because the recovery location was restarted or offline
  - Completed with errors - The recovery session completed, but encountered errors
  - Completed - The recovery session completed with no errors
  - In process - The recovery is currently in progress
  - Retrying - A restore session was not finished so the system is trying the restore again
  - Scheduled - Devices just added to a recovery plan and are waiting for their first recovery session or devices where restores were paused and have since been resumed will display as scheduled

- Recovery data sources
  - Files and Folders
  - MS SQL
  - System State
- Recovery testing session statistics
  - Boot Check Status
    - Success
    - Failed
    - Off
    - Unavailable for Local VHDX
  - Duration of the last completed recovery session
    - Sliding scale from 0 to unlimited
    in minutes
  - Number of errors of the last completed recovery session
    - Sliding scale from 0 to unlimited
  - Number of restored files
    - Sliding scale from 0 to unlimited
  - Number of selected files
    - Sliding scale from 0 to unlimited
  - Restored size
    - Sliding scale from 0 to unlimited
    in KB and GB
  - Screenshot
    - Available
    - Not Available
  - Selected size
    - Sliding scale from 0 to unlimited
    in KB and GB
  - Recovery testing status of the last completed recovery session
    - Failed
    - Completed with errors
    - Completed
  - Timestamp of the last completed recovery session
    - Quick Picks of:
      - Last day
      - 1 - 7 days
      - 7 - 14 days
      - 14 - 28 days
      - > 28 days
    - Custom range, select a stat date and time and an end date and time

Recovery status

- Failed - The recovery session has failed
- Invalidated - Device was moved to an inappropriate partner and so the session has failed
- Unresponsive - The recovery session was initiated but did not get updates for at least 30 minutes and so the session has failed
- Completed with errors - The recovery session completed, but encountered errors
- Completed - The recovery session completed with no errors
- In process - The recovery is currently in progress
- Retrying - A restore session was not finished so the system is trying the restore again
- Scheduled - Devices just added to a recovery plan and are waiting for their first recovery session or devices where restores were paused and have since been resumed will display as scheduled

Recovery data sources

- Exchange
- Files and Folders
- MS SQL
- SharePoint
- System State

Recovery testing session statistics

- Boot Status
  - Success
  - Failed
  - Off
  - Unavailable for Local VHDX
- Duration of the last completed recovery session
  - Sliding scale from 0 to unlimited

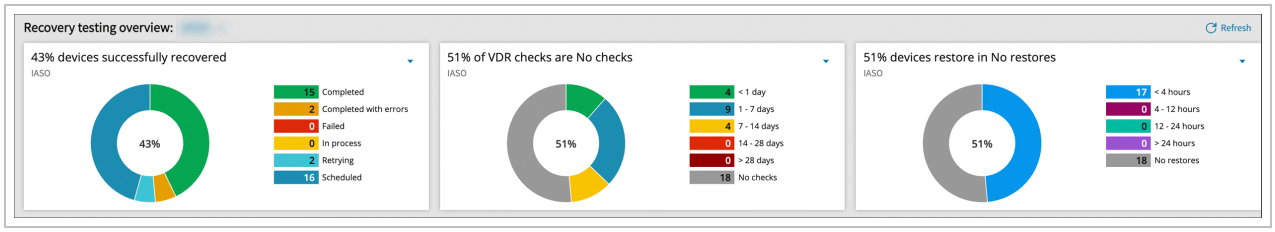
  in minutes
- Number of errors of the last completed recovery session
  - Sliding scale from 0 to unlimited
- Number of restored files
  - Sliding scale from 0 to unlimited
- Number of selected files
  - Sliding scale from 0 to unlimited
- Continuous restores
  - Paused
  - Running
- Recovery Location name
  - Select the Recovery Location name from the dropdown
- Restored size
  - Sliding scale from 0 to unlimited

  in KB and GB

- Screenshot
  - Available
  - Not Available
- Selected size
  - Sliding scale from 0 to unlimited
  in KB and GB
- Recovery testing status of the last completed recovery session
  - Failed
  - Completed with errors
  - Completed
- Timestamp of the last completed recovery session
  - Quick Picks of:
    - Last day
    - 1 - 7 days
    - 7 - 14 days
    - 14 - 28 days
    - > 28 days
  - Custom range, select a stat date and time and an end date and time

Widgets

Three widgets can be maximized at the top of the page, which allow for further filtering:



Device recovery status

This widget allows you to filter the devices by recovery status:

- Completed
- Completed with errors
- Failed
- In process
- Retrying
- Scheduled

VDR checks time frame

This widget allows you to see the percentage of devices whose recovery check completed within the following day ranges:

- < 1 day
- 1 - 7 days
- 7 - 14 days
- 14 - 28 days
- > 28 days
- No checks

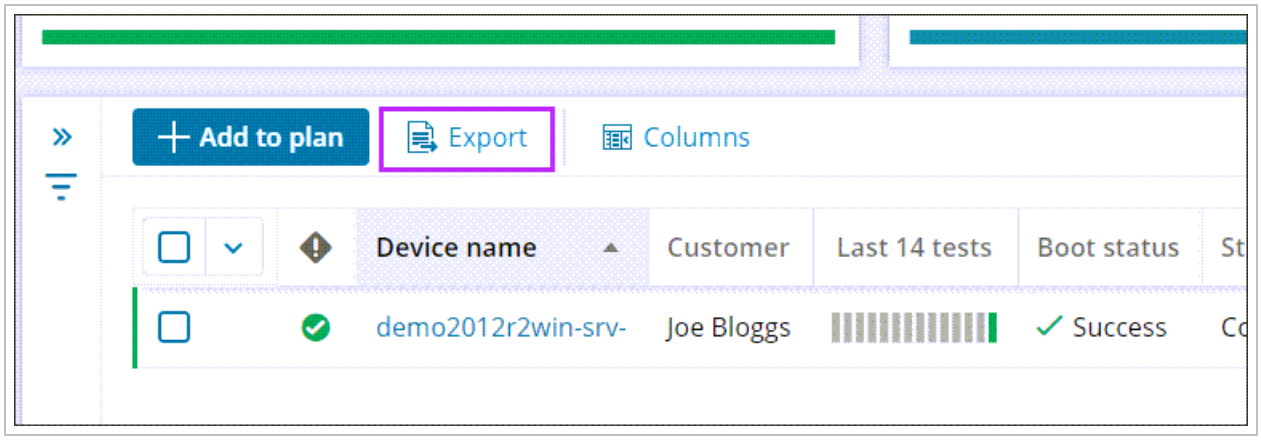
Device restore time frame

From this widget, you can filter devices by the how recent restores are done by the following time frames:

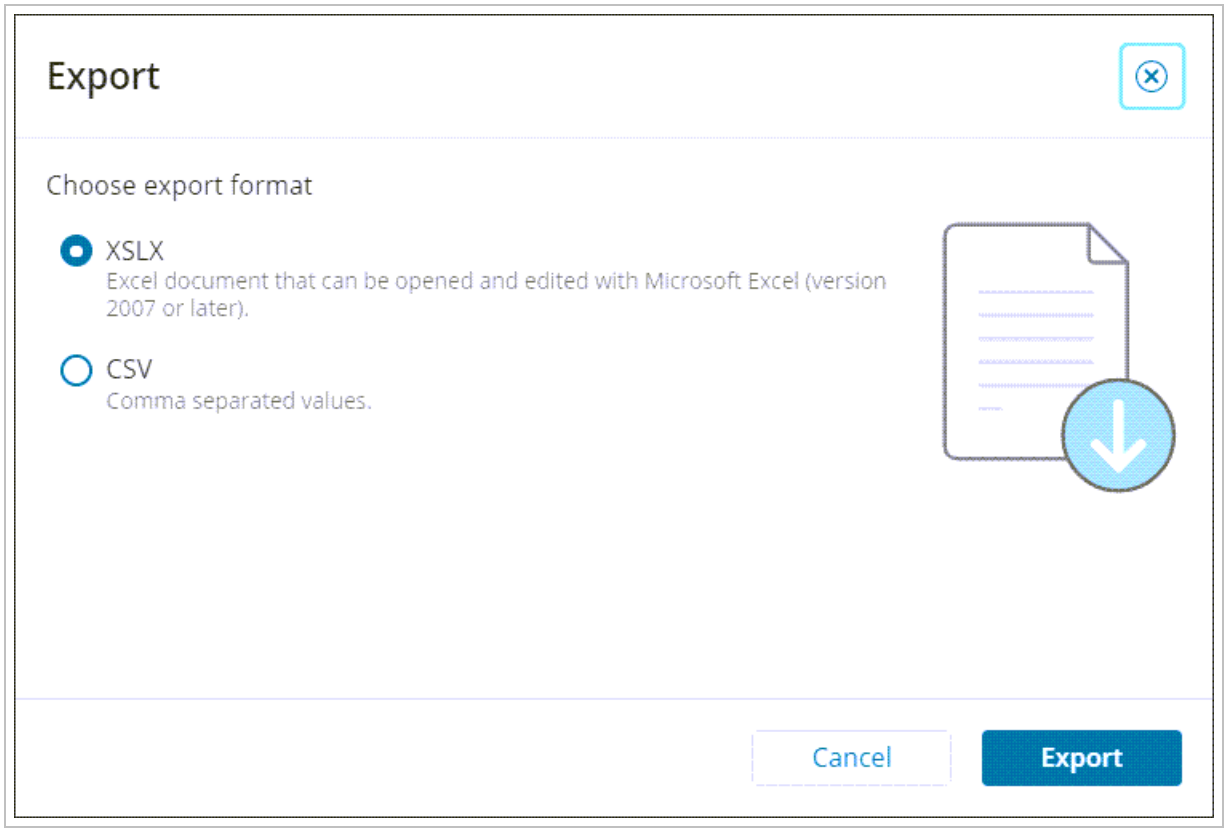
- < 4 hours
- 4 - 12 hours
- 12 - 24 hours
- > 24 hours
- No restores

Exporting

You may export a list of devices currently assigned a plan by clicking **Export**

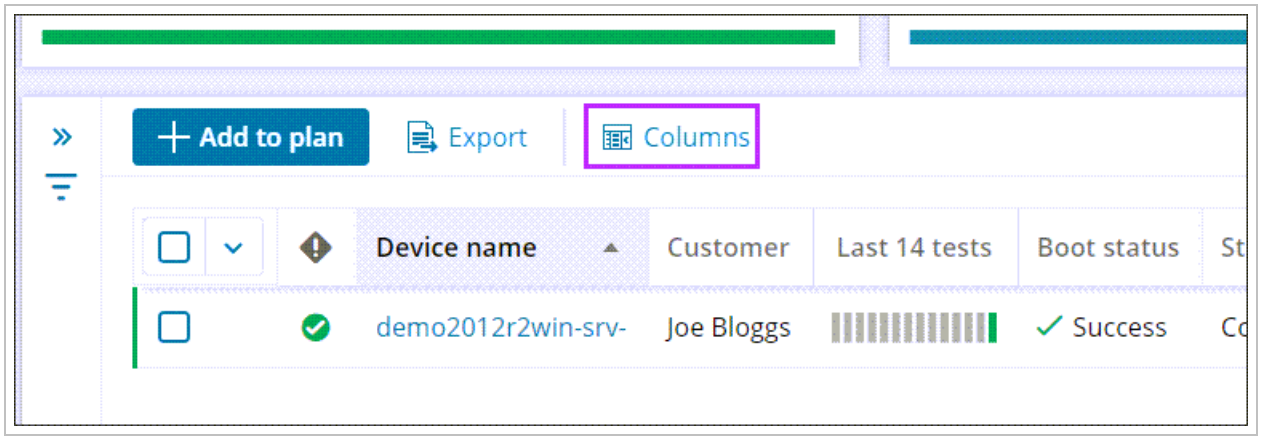


This will then provide a separate dialog where you can choose to export in either XSLX or CSV.

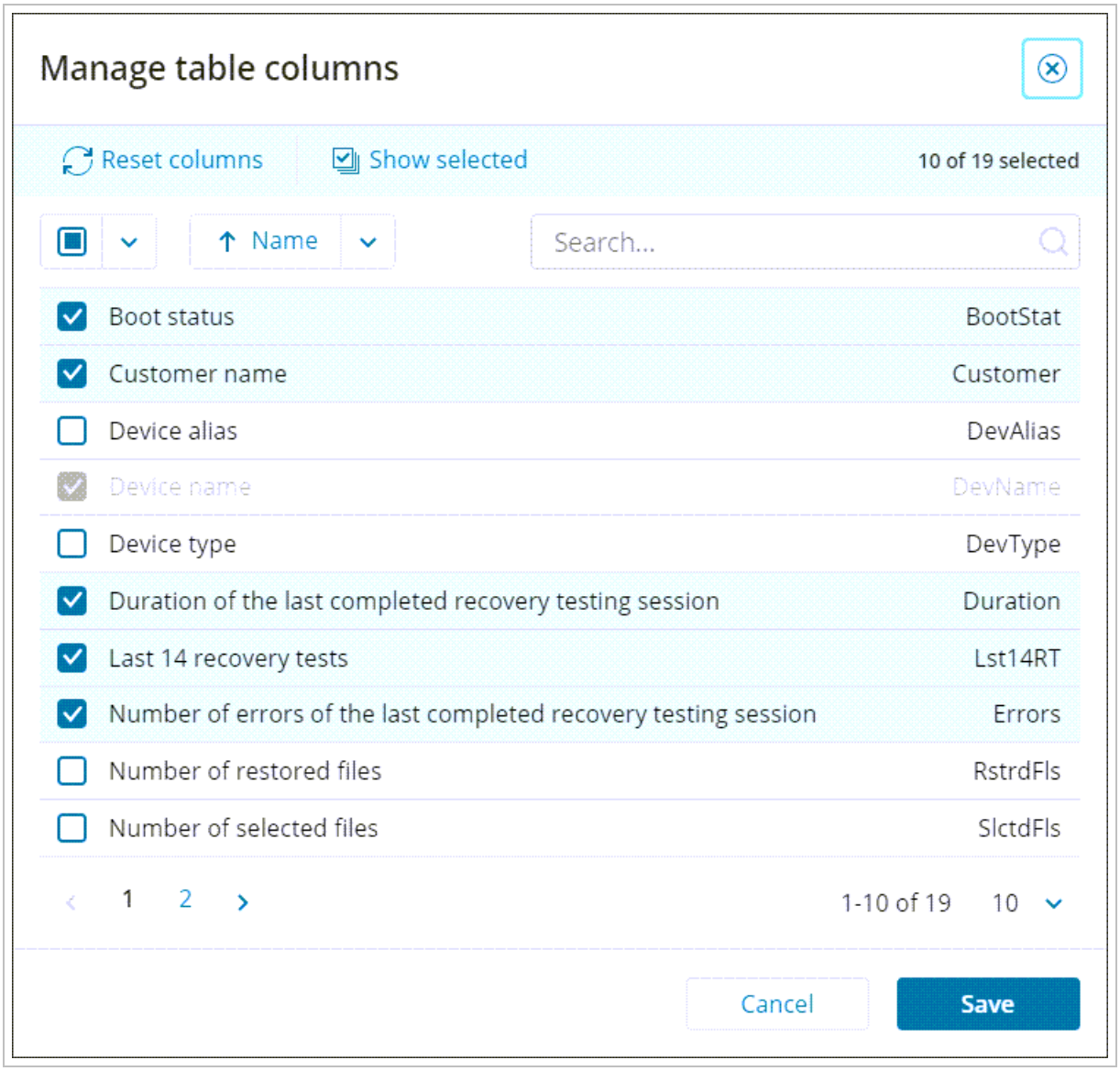


Manage Table Columns

Management Console allows you to manage the tables columns that can be seen within the Recovery Testing overview.



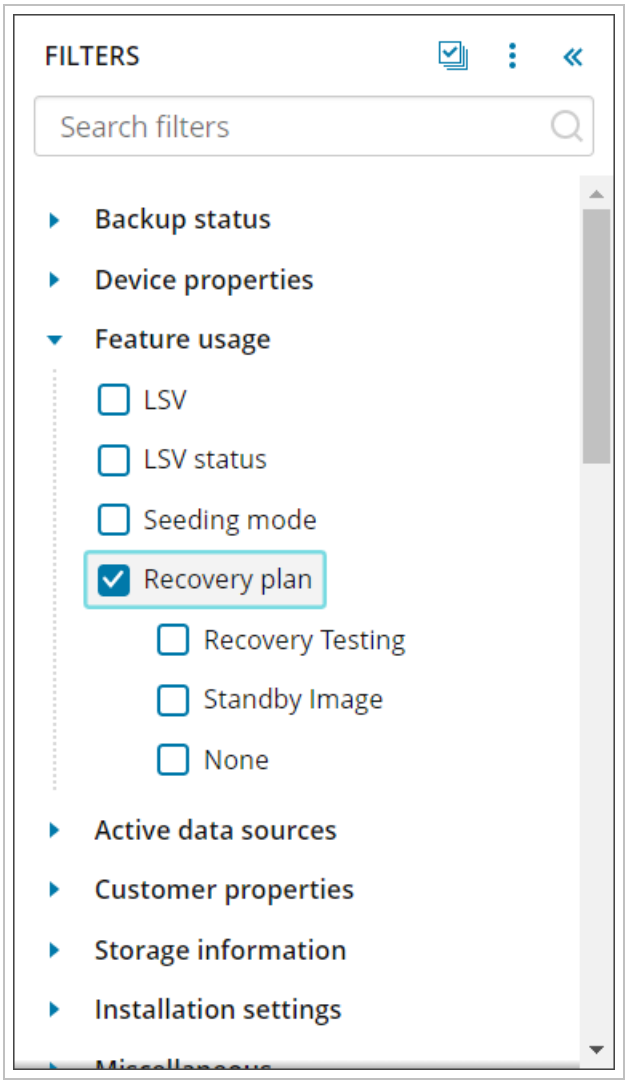
In the Manage table columns dialog, you can select and deselect columns based on the information you wish to view from the dashboard.



From Main Dashboard

Users of all roles can view devices in the Console with Recovery Testing enabled. They appear as regular Backup Manager devices in **Backup > Dashboard** and can be found by filtering in the Beta Dashboard:

1. Expand the **Filters** pane on the left of the Toolbar
2. Search for **Recovery Plan** in the **Feature Usage** section



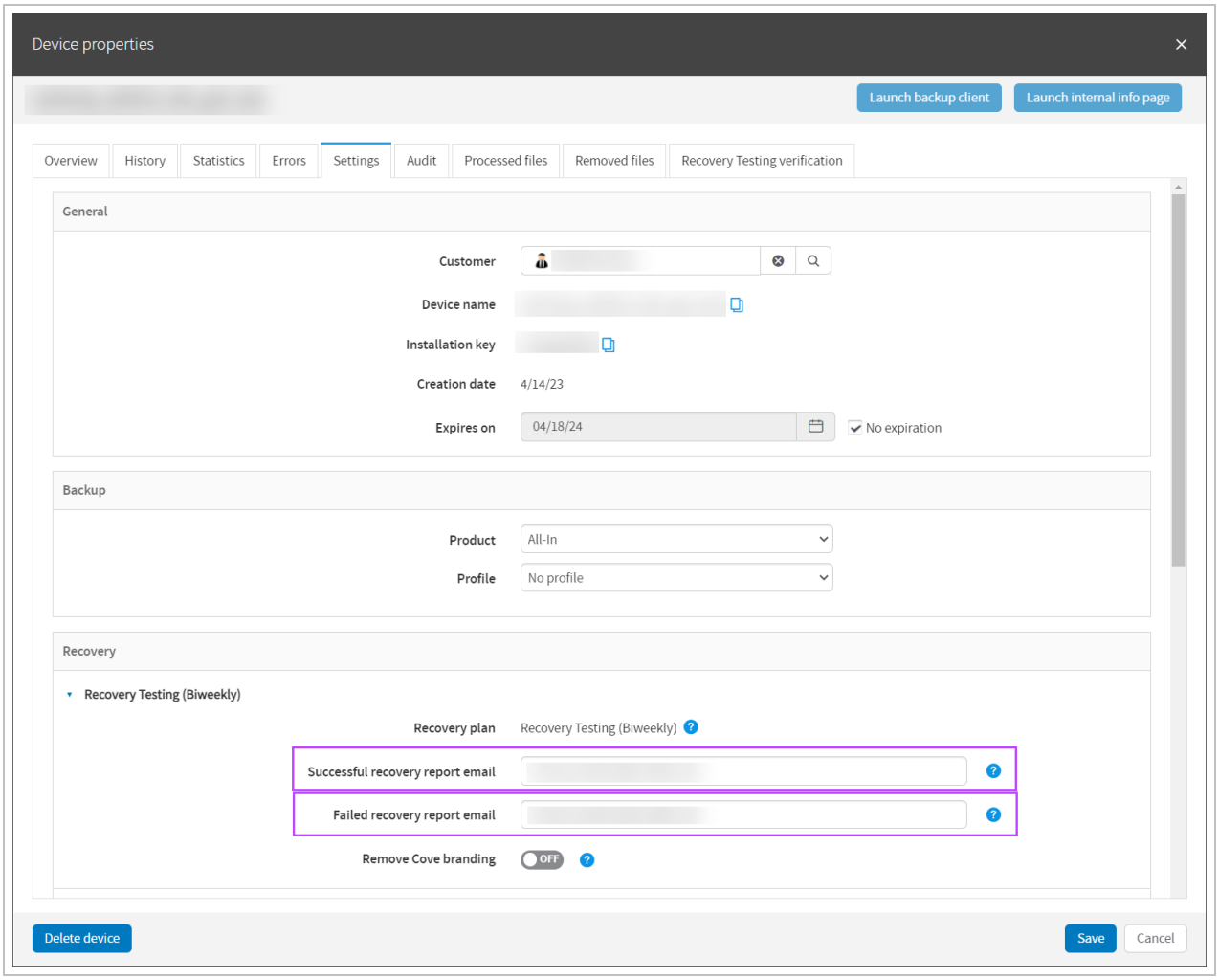
3. Tick the **Recovery Testing** plan

> Your devices list will automatically update to show only devices where the Recovery Testing plan is enabled.

Accessing device properties

As with any normal device, when you click on the device name, you will see the Device Properties dialogue. If the device is assigned to a plan, details of this will be visible in a Recovery section.

You can also add, remove, or amend the **Successful recovery report email** and **Failed recovery report email** recipient email addresses from here as well as toggle **Cove branding** on the reports on or off.



View results and check screenshots

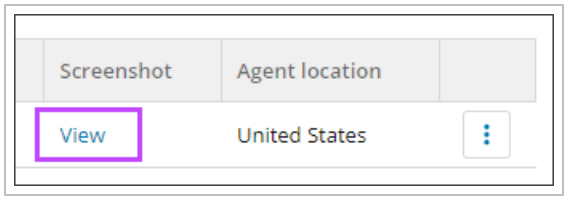
To view statistics of the Recovery Testing and check the screenshots to ensure this has been successful, you can view this by following one of the below methods:

From Device Properties

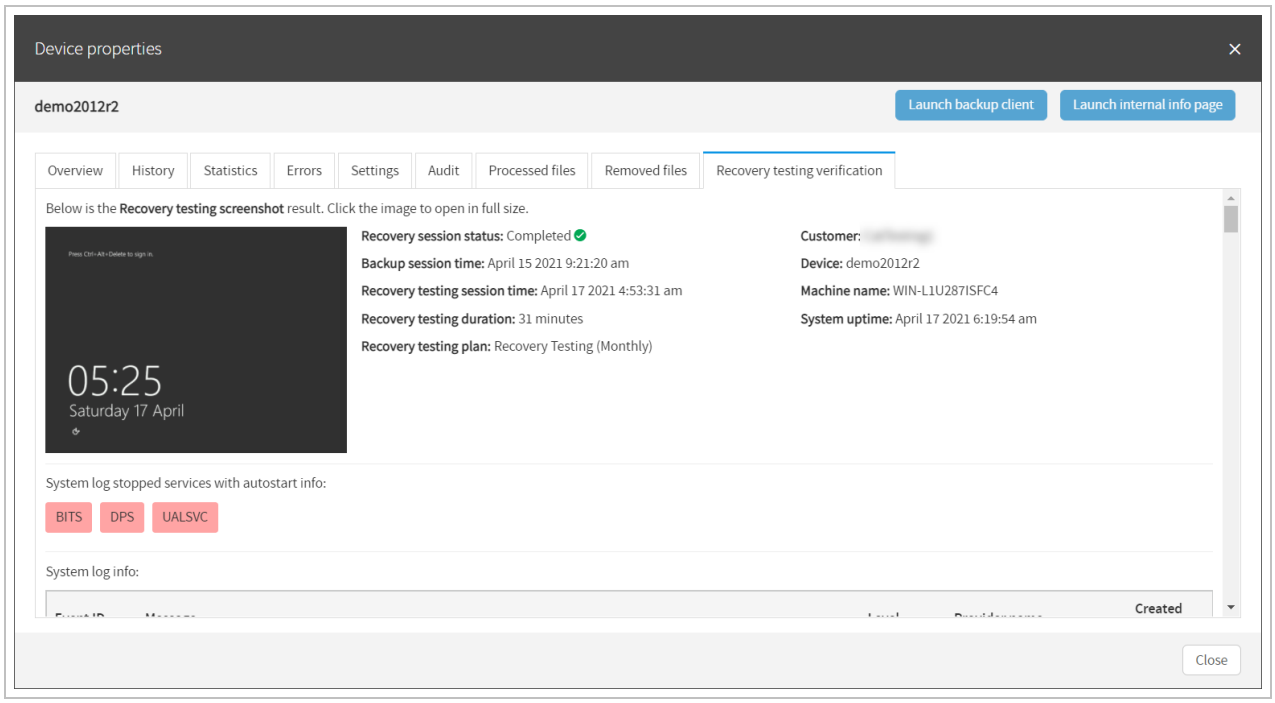
1. Log in to the Management Console under a **SuperUser** account
2. Click the device name to open Device Properties
3. Navigate to the **Recovery Testing Verification** tab

From Recovery Testing Overview

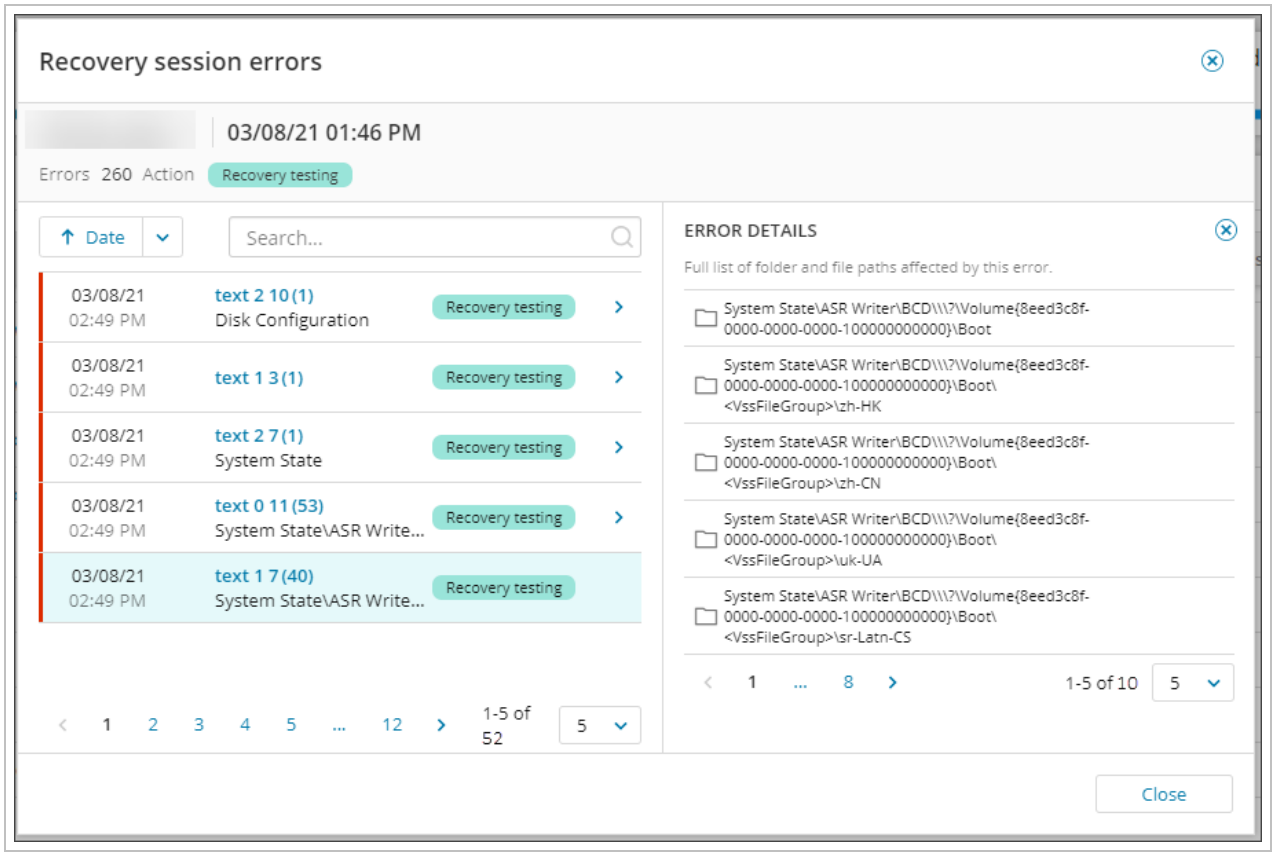
1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Testing**
3. Click **View** under the Screenshot column



4. This will take you in to the Device Properties dialogue, where you will now see the **Recovery testing verification** tab:



If an error was found during the recovery, you can view a wider look at the error details from the Recovery session errors dialog box.



This can be accessed by hovering over the recovery session with the error and selecting to show the Recovery session errors.

Recovery Testing Verification

In the **Recovery Testing Verification** tab you will see the screenshot taken from the virtual machine during the boot phase of Recovery Testing.

In this tab, you will also see information on the device, such as system uptime, when the session was last recovered, services that were stopped in order to perform the recovery and system log information.

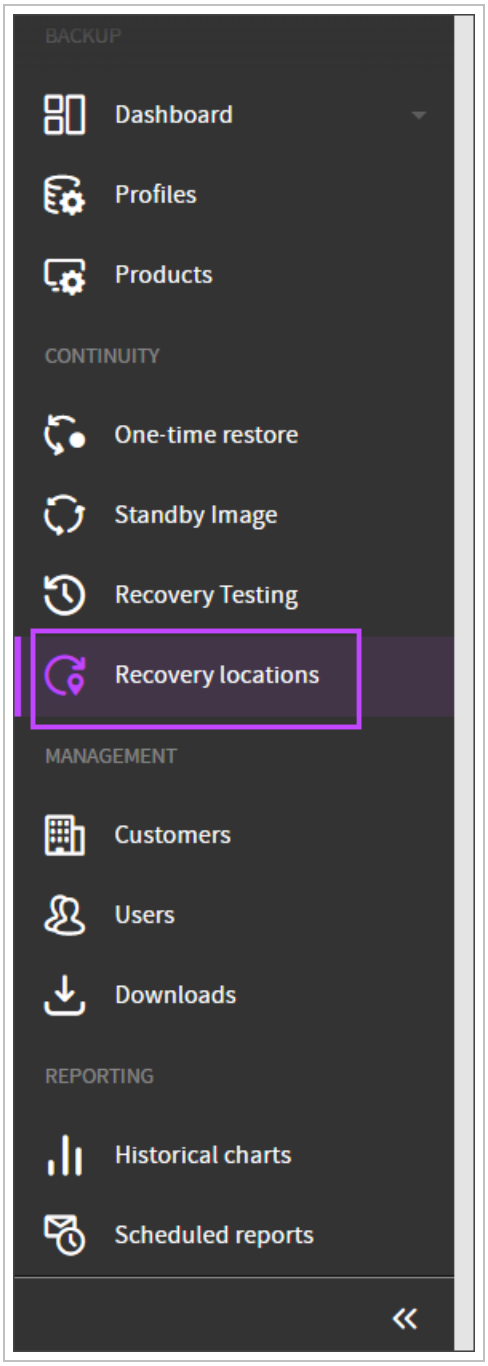
You can find full details on device statistics and what each tab is used for here.

> In the case of a failed test recovery, the captured screenshot may not display the error or state that caused the failure. To understand the cause of the failed restore, we recommend using the virtual recovery option in the Backup Manager or Recovery Console to recreate and diagnose the issue.

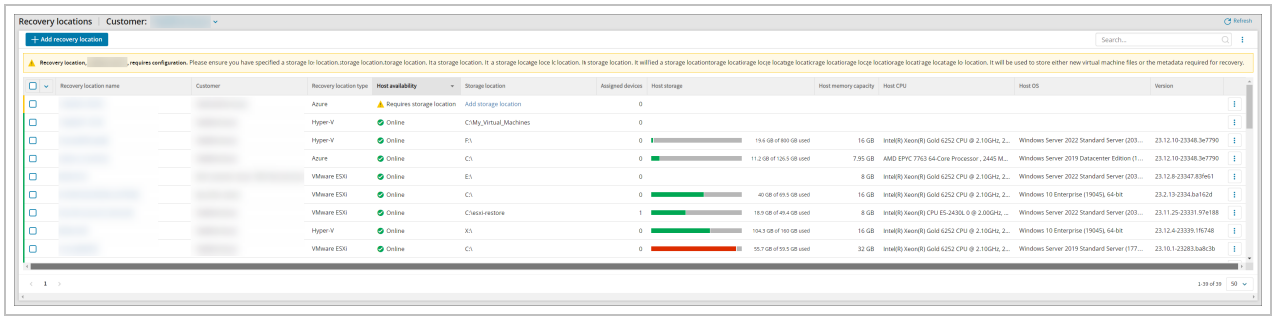
Recovery Locations

Recovery Locations, the host running the recovery service and processing data restores, can be added, edited, and deleted in the **Recovery Locations** page of the Management Console. They can be added prior to adding devices to the Standby Image plan, or on the first step of the Top bar menu, Enable Standby Image to AzureDevices cannot be added to a Standby Image plan if already assigned to a Recovery Testing plan.Devices can be assigned to multiple Standby Image plans at once, i.e. Standby Image to Hyper-V and Standby Image to Azure. From Main DashboardTo enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:Log in to the Management Console under a SuperUser or Manager account In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan toClick Add to recovery plan from the Toolbar Select Standby Image (Azure)Select the customer the device(s) you wish to apply the Standby Image plan belong toChoose the recovery location as was configured in Add Recovery LocationsIf the selected customer does not have any locations, you must add one before continuing by selecting Add recovery location. See Add Recovery Locations for full details of adding a location.It is not possible to assign a location for which the Host availability is "Offline"Click NextConfirm the device selected from the Dashboard is compatible and click Next Enter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereClick Next to continueChoose the boot check frequency:OffEvery recovery sessionDailyWeeklyBiweeklyMonthlyIf you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Once connected, click NextClick Azure VM settings towards the right-hand side of the screen to open the settings configuration window:Configure the Azure VM Settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk typeData disk(s) typeVirtual NetworkSubnetAssign NSG and public IPDuring the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend blocking internet access for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.Click Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowConfirm assigning the plan to the device(s)Wait for the plan to be assigned until you see a confirmation banner on the pageClick FinishFrom Standby Image OverviewLog in to the Management Console under a SuperUser or Manager accountNavigate to Continuity > Standby ImageClick Add to PlanSelect Standby Image (Azure)You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the planRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding: and Top bar menu wizards.

The Recovery Locations page can be found on the Management Console under the **Continuity** section:



The page displays several pieces of information relating to previously created recovery locations.



The columns displayed are:

- Recovery location name
- Customer
- Recovery location type
  - Azure
  - Hyper-V
  - VMware ESXi
- Host availability
  - Offline
  - Online
  - Requires a storage drive

    > Drive is required for Standby Image and Recovery Testing locations as this is the location in the file system where the new Virtual Machine files will be created. This is not required for Azure and ESXi locations
- Storage location

  > For Hyper-V, this can be added by clicking **Add storage location**, entering the drive letter or local path in the box and clicking **Save**
- Assigned devices
- Host storage
- Host memory capacity
- Host CPU
- Host OS
- Version

Minimum Requirements

For Standby Image and Recovery Testing, Windows Admin Center must be installed on the management machine, available here.

> This is not required for One-Time Restore.

Default Hardware Configuration

By default, each Recovery Location is configured to run 5 restores in parallel with a target VM size of 4 CPU cores and 4 GB of RAM. The following minimal configuration is recommended depending on the restore target:

- Hyper-V and ESXi
  - **CPU** - 22 Cores or more
  - **RAM** - 32 GB or more
  - **Restore Target Drive Capacity** - more than two times the size of the selected size of all devices combined
- Local VHD and Azure
  - **CPU** - 12 Cores or more
  - **RAM** - 16 GB or more
  - **Restore Target Drive Capacity** - more than two times the size of the selected size of all devices combined

Single device restore

To start Recovery Service on a Windows Server and run a single device restore we recommend the following hardware configuration, depending on the restore format:

- Hyper-V and ESXi
  - **CPU** - 6 Cores or more
  - **RAM** - 6 GB or more
  - **Restore Target Drive Capacity** - more than two times the size of the backed up data
- Local VHD and Azure
  - **CPU** - 4 Cores or more
  - **RAM** - 5 GB or more
  - **Restore Target Drive Capacity** - more than two times the size of the backed up data

> Also, make sure that Recovery Location operating system conforms to the requirements stated here: Virtual Disaster Recovery Requirements

Azure Requirements

To install the Recovery Location's recovery service on an Azure VM, the following requirements are necessary:

- A user created for you in your Azure tenant. The user must:
  - Have access to a subscription
  - Have access to a resource group you want to use to keep the Recovery Location VM and restored (target) Azure VMs
  - Be able to assign permissions on virtual machines within the resource group

Additional resources for more devices

The default number of parallel restores can be adjusted depending on the hardware you use for the Standby Image Recovery Location. When configuring each recovery location, it is important to do this in a way it is neither too big (as it might slow down the restore because the host will be overloaded) nor too low (as in this case you might not use the full capacity of your computing resources and hence receive a slower than ideal performance).

While network bandwidth and disk IOPS don't have any strict requirements to run the Standby Image Recovery Service it does directly affect the restore speed and low resources can cause poor performance.

CPU and RAM might be a blocker to adding more restores in parallel. If you do not have enough CPU and/or RAM it is possible to see performance degradation, failing restores, or Virtual Machine boot issues due to “out of memory“ errors.

We recommend reserving the following additional resources for **each extra device** when configuring a number of parallel restores:

- Hyper-V and ESXi
  - **CPU** - 4 cores
  - **RAM** - 4 GB
- Local VHD and Azure
  - **CPU** - 2 cores
  - **RAM** - 2 GB

> The requirements mentioned above are recommendations. You may set the number of cores and memory at your discretion, however, taking into account the recommendations above.
>
> If you have already had experience using Recovery Console and have a suitable configuration, it is possible to use the same configuration for Standby Image when taking into account the recovery of the same number of devices of a similar configuration.

Recommendations for Maximum Performance

Hardware

When running multiple restores in parallel, we recommend the following to increase the performance of each machine:

- Use SSD disks with higher IOPs
- A fast network connection with good bandwidth

Both the **target disk** and **system disk** should have enough performance as the system disk may be used by system services and Hyper-V.

Hypervisor Configuration

While required to effectively mitigate certain classes of vulnerabilities, the **core scheduler** (enabled by default for Windows Server 2019 and newer) may also potentially reduce performance. We recommend changing the scheduler to **Classic** to increase performance.

> This action should be done along with applying appropriate security controls to mitigate risks raised by this change.

> The free Hyper-V Server 2019 ISO can be found here.

Anti-Virus Recommended Exclusions

The following are recommended to add to the anti-virus exclusions list to allow for successful backups:

Recovery Service Exclusions

- `AuthTool.exe [file] SYSTEM_DRIVE:\Program Files\Recovery Service\*\AuthTool.exe`
- `unified_entry.exe [file]. SYSTEM_DRIVE:\Program Files\Recovery Service\*\unified_entry.exe`
- `RecoveryFP.exe [file] SYSTEM_DRIVE:\Program Files\Recovery Service\*\BM\RecoveryFP.exe`
- `VdrAgent.exe [file] SYSTEM_DRIVE:\Program Files\Recovery Service\*\BM\VdrAgent.exe`
- `ProcessController.exe [file] SYSTEM_DRIVE:\Program Files\Recovery Service\*\BM\ProcessController.exe`
- `ClientTool.exe [file] SYSTEM_DRIVE:\Program Files\Recovery Service\*\BM\ClientTool.exe`

Virtual Machines Exclusions

- `*.vhd RESTORE_TARGET_DRIVE\StandbyImage\*\vm\*.vhd`
- `*.vhdx RESTORE_TARGET_DRIVE\StandbyImage\*\vm\*.vhdx`

Hyper-V Processes Exclusions

- `%ProgramData%\Microsoft\Windows\Hyper-V [folder]`
- `Vmms [process]. %systemroot%\System32\Vmms.exe`
- `Vmwp [process]. %systemroot%\System32\Vmwp.exe`
- `Vmsp [process]. %systemroot%\System32\Vmsp.exe`
- `Vmcompute [process]. %systemroot%\System32\Vmcompute.exe`

System Network Configuration

When running a large number of parallel restores on the same recovery location, (around 50) a lot of network connections may be utilized. In order to improve the performance and stability of such heavily loaded systems it is recommend to adjust network configuration in the following way:

1. Increase ephemeral ports count, set up new values:
   a. `start = 20000`
   b. `number of ports = 45000`
2. Reduce `TcpTimedWaitDelay` to **5 seconds**

> See details here: Settings that can be Modified to Improve Network Performance - BizTalk Server

Add Recovery Locations

Instructions for how to Configure N-able Recovery Service on Azure Recovery Locations must be followed specifically, due to several differences in the Azure configuration.

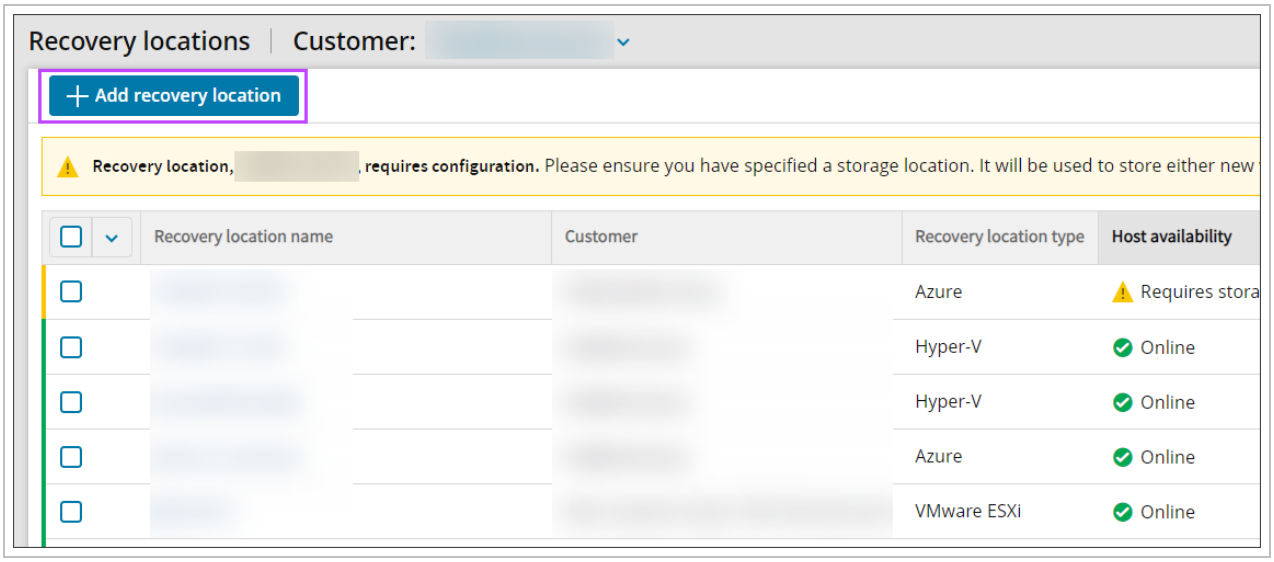
Instructions for how to Configure N-able Recovery Service on ESXi Host Server must followed specifically, due to several differences in the ESXi server configuration.

Instructions for how to Configure N-able Recovery Service on Hyper-V Server 2019 must be followed specifically, due to several differences in the Hyper-V 2019 server configuration.

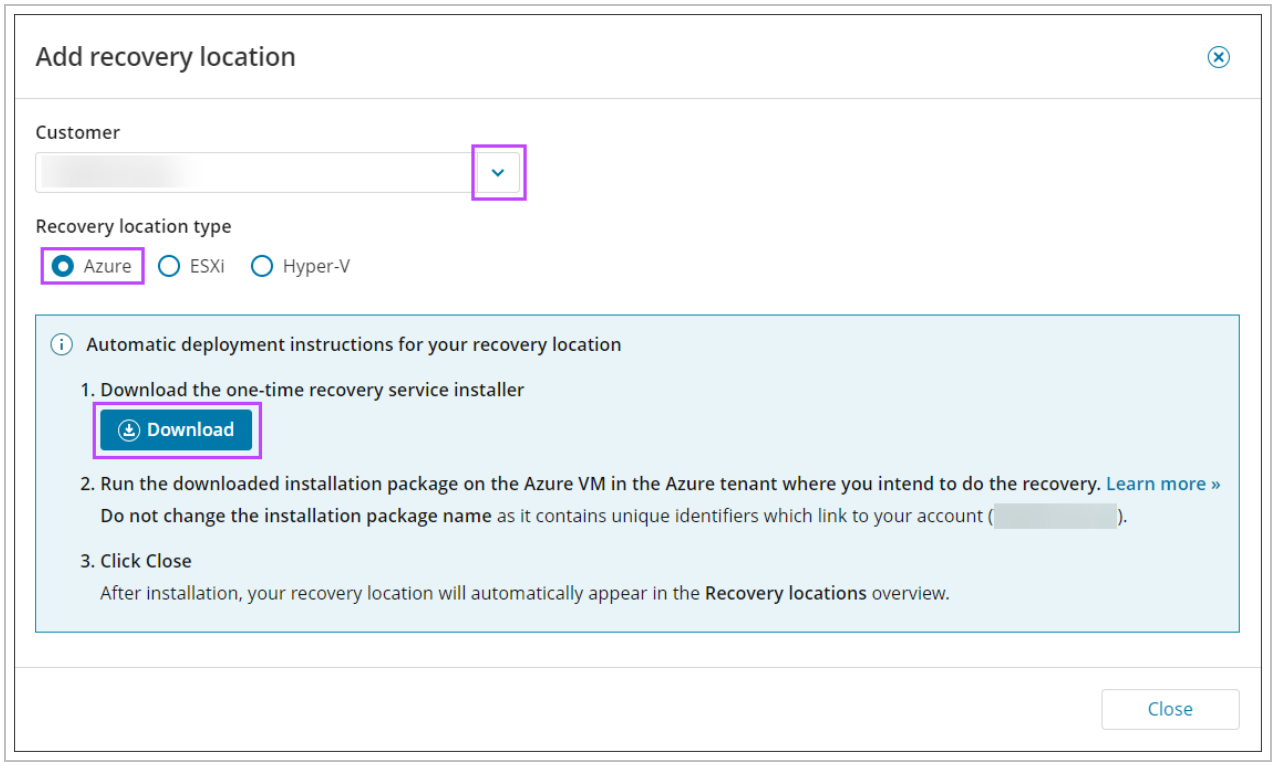
Create Recovery Locations

Azure

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Click **Add recovery location** at the top of the page



4. In the **Add Recovery Location wizard**, select the customer to attribute the recovery location to, from the dropdown



5. Select **Azure** as the Recovery Location Type
6. Download the recovery service installer and save it to an easily found place on your device

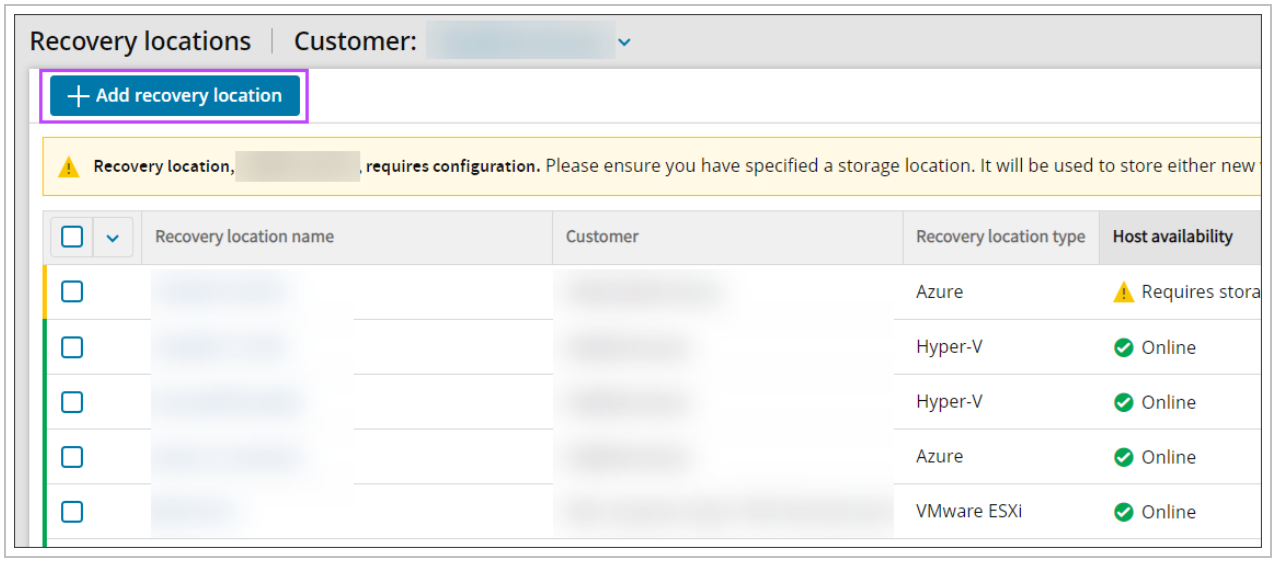
> Do **not** change the installation package name. The installation package name contains unique identifiers to your account.
>
> This is a one-time installer and can only be used to install a single instance of the recover service. The installer will fail if you attempt to use the same package for another installation.

7. Continue following the instructions on how to Create the Recovery Location VM
8. Then Installing and Configuring the Recovery Location on the Azure VM
9. Followed by Assigning Permissions to the Recovery Location VM

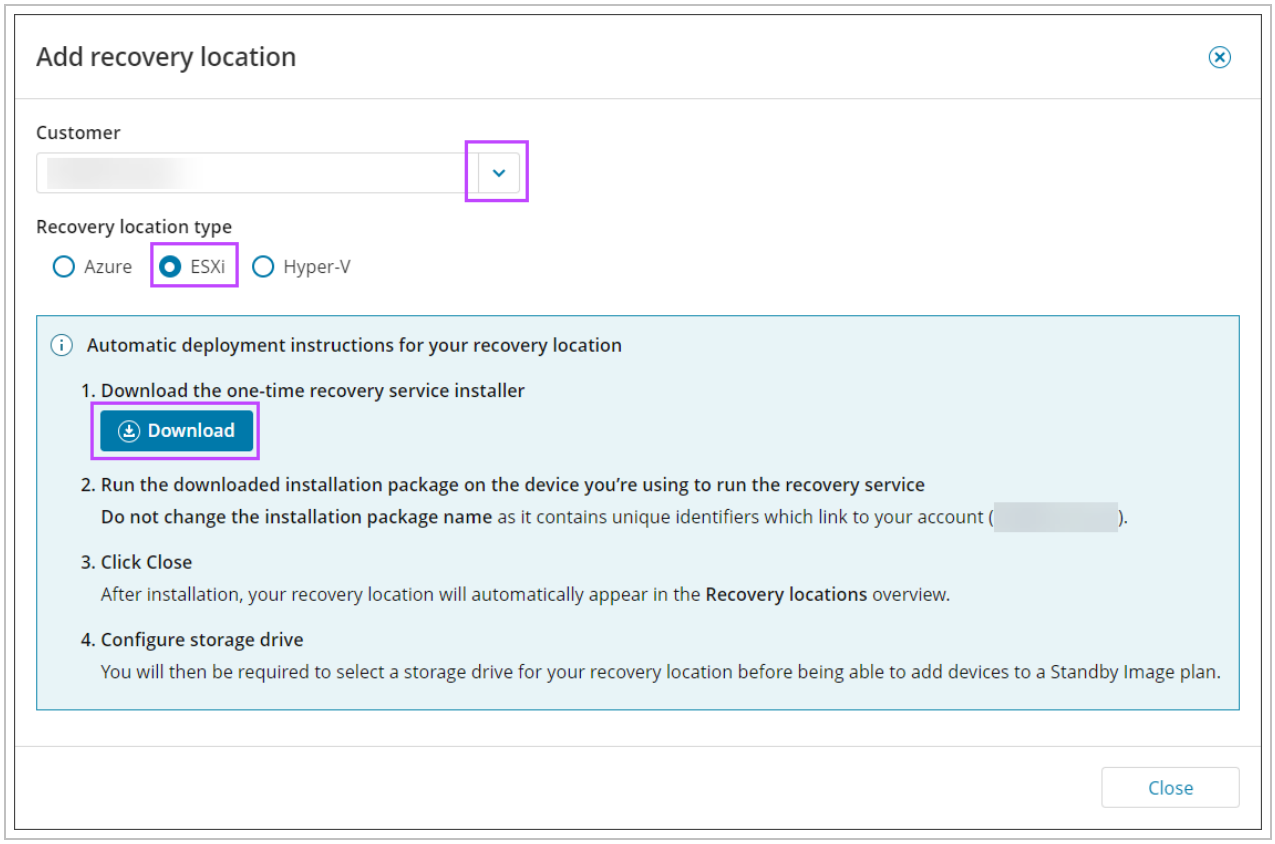
Only once location VMs are created, installed, configured and all permissions given, can you begin the One-Time Restore or Standby Image to Azure.

ESXi

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Click **Add recovery location** at the top of the page



4. In the **Add Recovery Location wizard**, select the customer to attribute the recovery location to from the dropdown



5. Select **ESXi** as the recovery location type
6. Download the recovery service installer

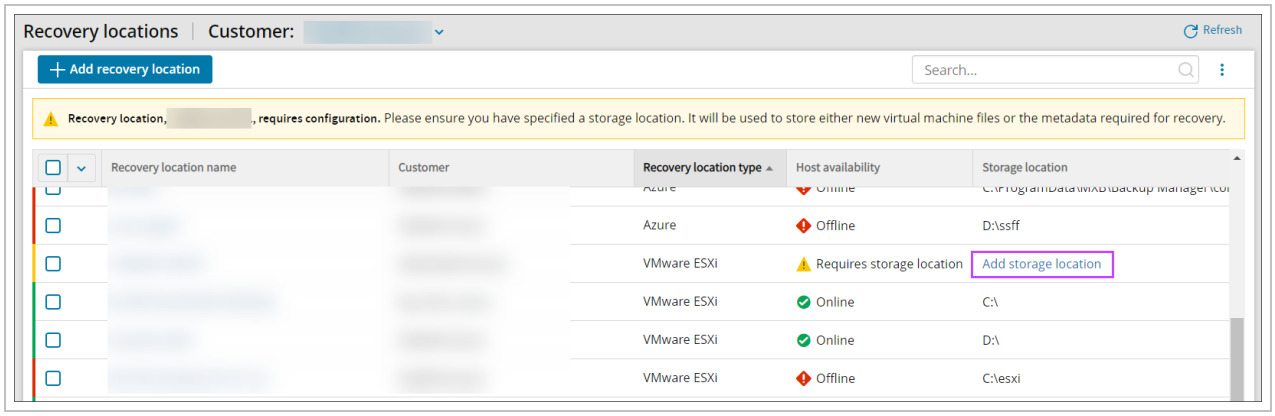
> Do **not** change the installation package name. The installation package name contains unique identifiers to your account.
>
> This is a one-time installer and can only be used to install a single instance of the recovery service. The installer will fail if you attempt to use the same package for another installation.

7. Run the downloaded installation package on the Virtual Machine as created in Step 3: Create Recovery Location Virtual Machine

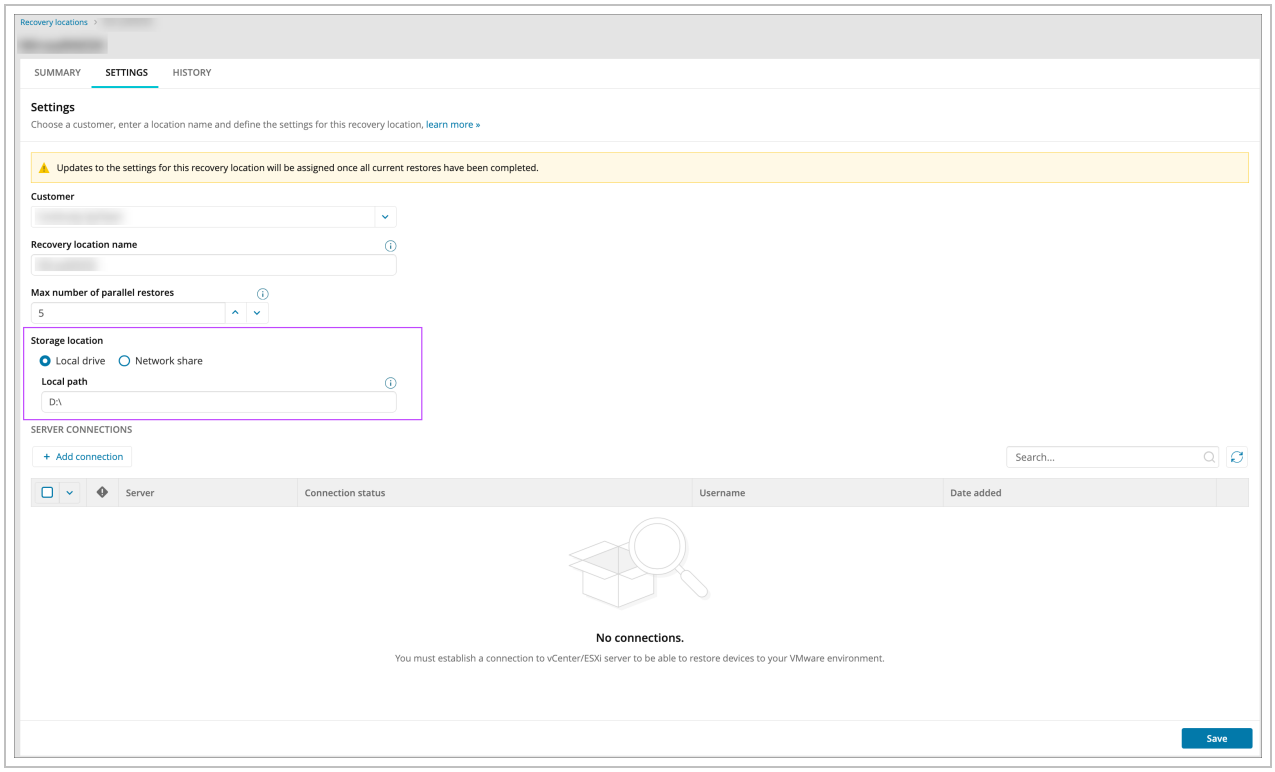
> The recovery location will appear in the list after installation is complete

Add Storage Location and Server Connections

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Find the new recovery location in the list and click **Add storage location**

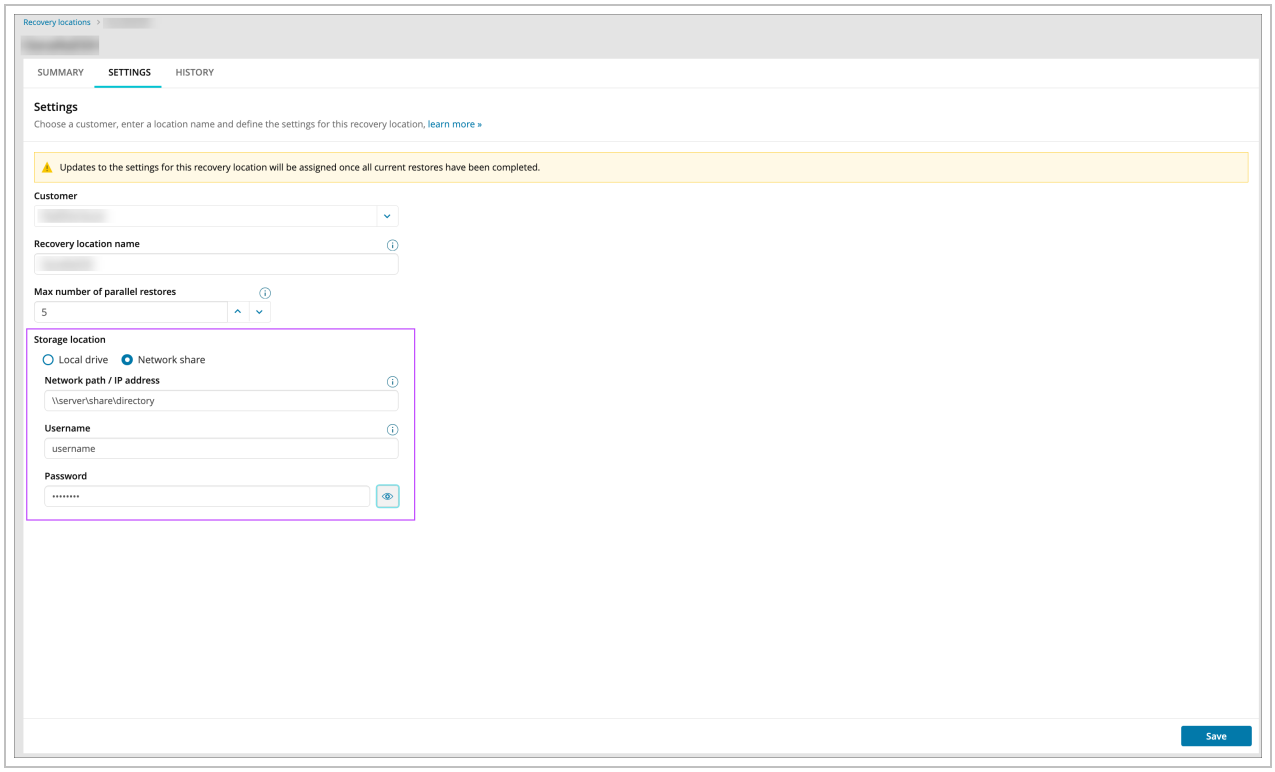


4. Provide local file path for the storage location
   - Local Drive:



> Without a storage location, connections **cannot** be made to any of the added servers. If you want to restore to Local VMDK is not obligatory to configure server connections. The VMDK file will be restored directly to the storage path, and not on the ESXi server.

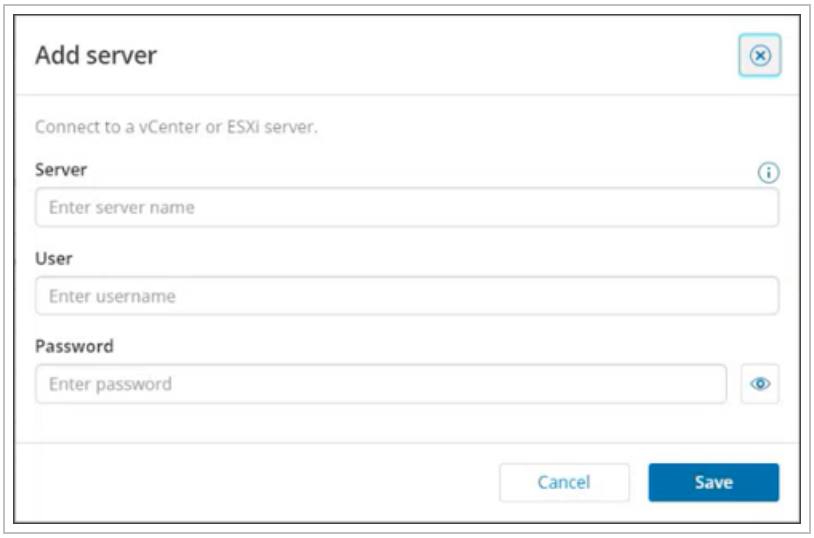
- Network Share:



> Recovery Locations using **Network Shares** will **not** see the option to configure any server connections as the restore will not be done on an ESXi server, and will be done on the Network Share to a Local VMDK restore format.

5. Click **Add Connection** to connect to the vCenter or ESXi server

> If using a connection to the vCenter server, you will be able to restore to any ESXi host connected to the vCenter server



6. Enter the vCenter or ESXi **server name** or **IP address**, and your username and password for this
7. Click **Save**

> Multiple server connections can be added to the recovery location, but must be done one at a time. Doing so will allow you to connect and restore to several ESXi hosts which are not connected to one vCenter Server

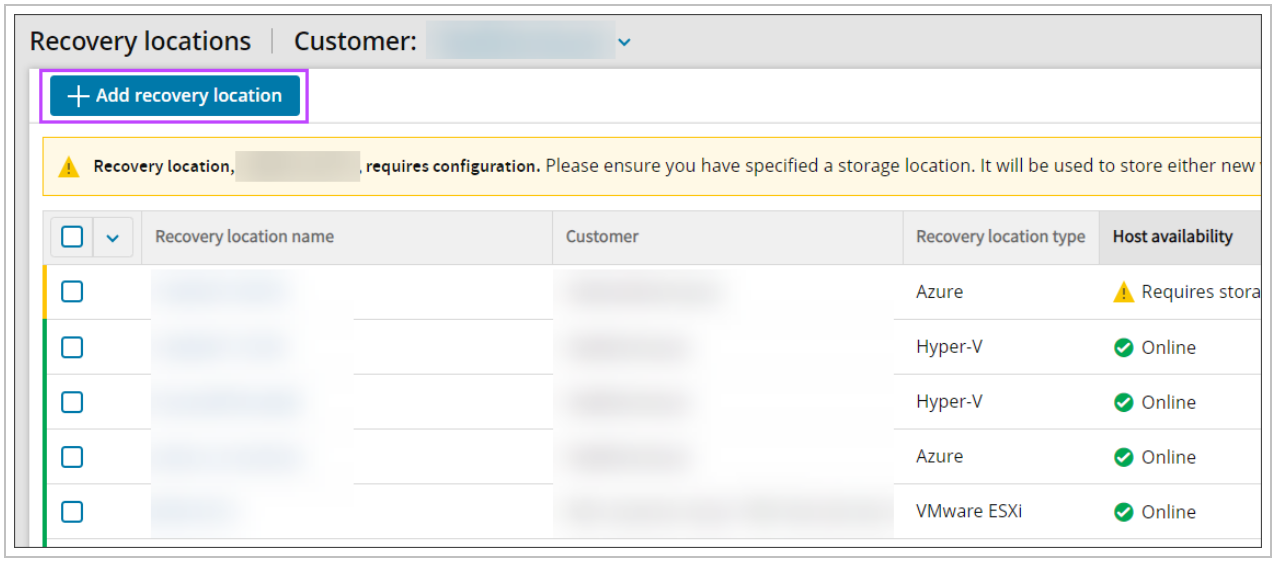
> You must click the **refresh** button to above the list of server connections to update the status from 'connecting' to 'connected'. The connection may take a few minutes.

Once locations are added, you may continue with adding devices to the Standby Image plan.

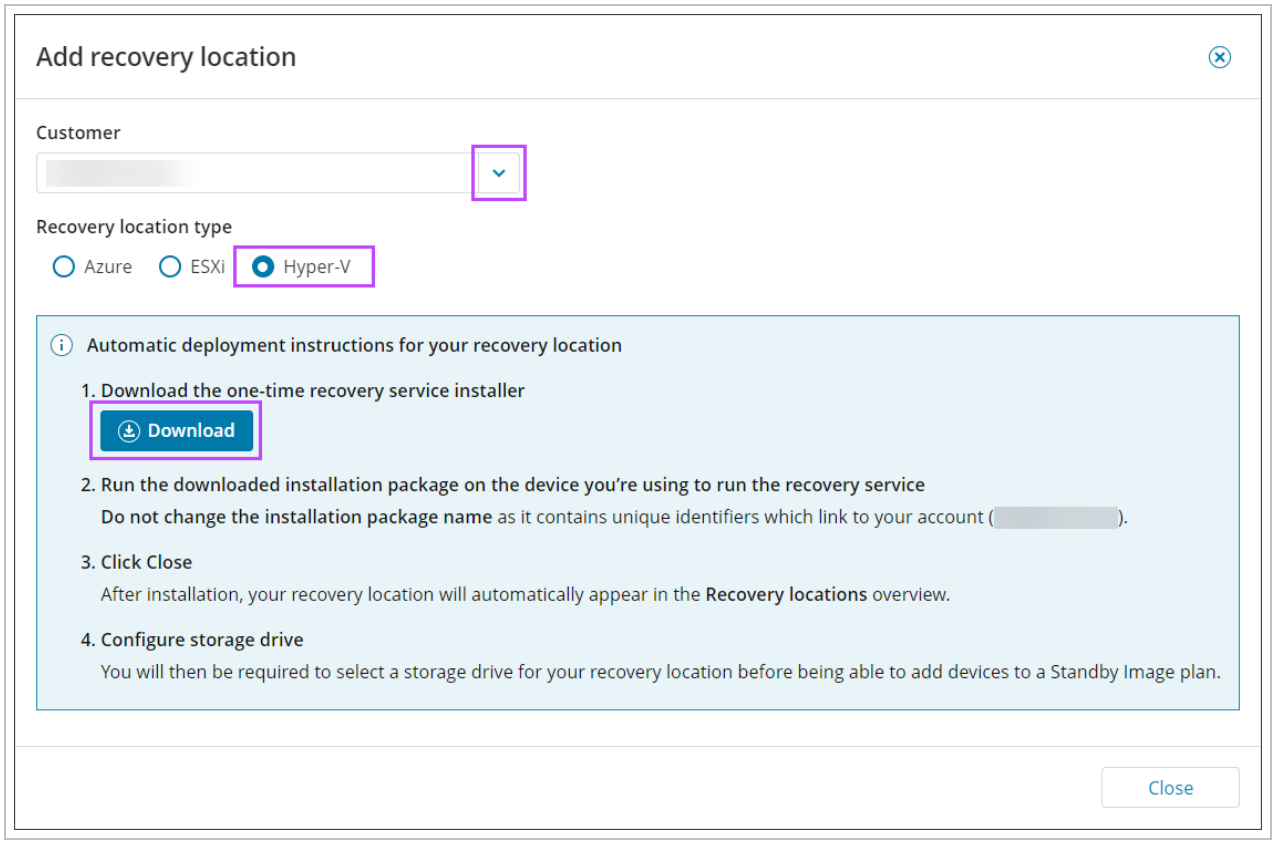
> Installing the Recovery Locations recovery service on an ESXi Host server requires additional configuration during the setup of the environment. See here for instructions on configuration of the recovery service on ESXi Host Servers.

Hyper-V

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Click **Add recovery location** at the top of the page



4. In the **Add Recovery Location wizard**, select the customer to attribute the recovery location to from the dropdown



5. Select **Hyper-V** as the recovery location type
6. Download the recovery service installer

> Do **not** change the installation package name. The installation package name contains unique identifiers to your account.
>
> This is a one-time installer and can only be used to install a single instance of the recovery service. The installer will fail if you attempt to use the same package for another installation.

7. Run the downloaded installation package on the device where the Virtual Machines should be restored to

> The recovery location will appear in the list after installation is complete

8. Give the recovery location a storage location by:
   a. Click **Add storage location**
   b. Enter the drive letter or local path to the folder where your virtual machine files will be stored in the box
   c. Click **Save**

Once locations are added, you may continue with adding devices to the Standby Image plan.

> Installing the Recovery Locations recovery service on a Hyper-V Server 2019 requires additional configuration during the setup of the Hyper-V. See here for instructions on configuration of the recovery service on Hyper-V Server 2019.

Add Device to Recovery Location

Devices can be added to a Recovery Location from the **Continuity** > **Recovery Locations** page, thereby enabling the Standby Image Plan, using one of three methods:

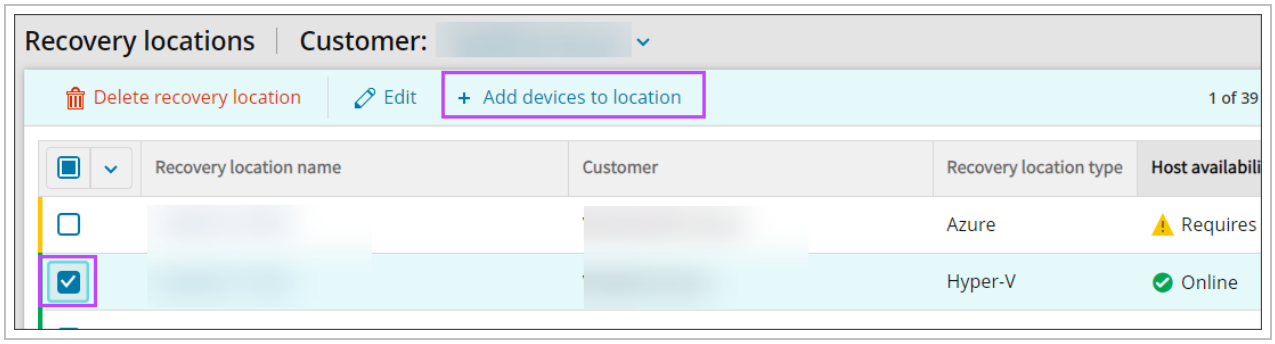
- Top bar menu
- Location context menu
- Right-hand menu

> These will only be available if the Recovery Location is **Online**.

Top bar menu

Available for Hyper-V and ESXi Locations **only**.

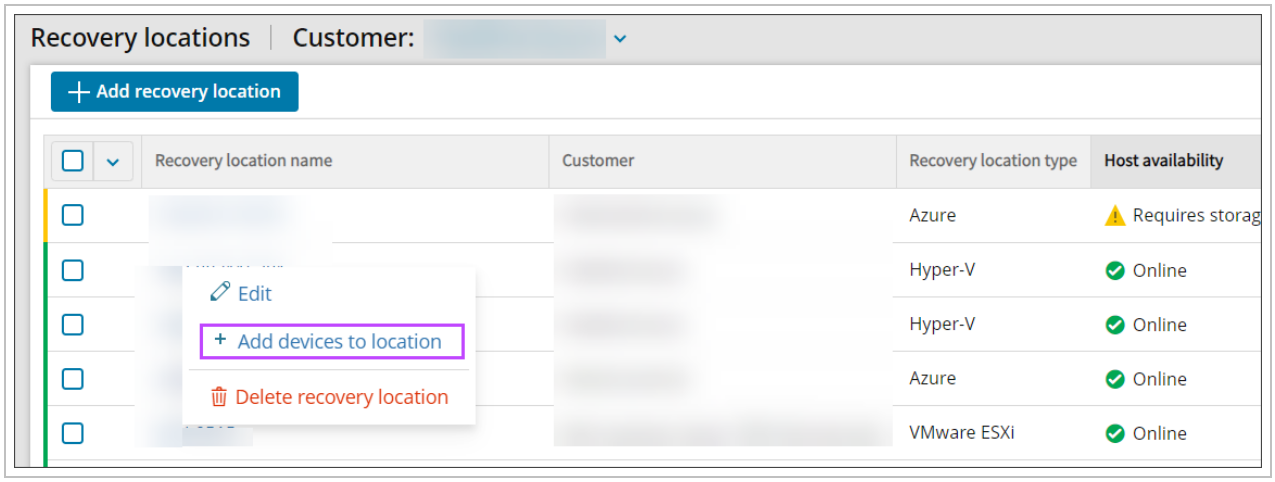
1. Select the checkbox for the Recovery Location to add the device to
2. At the top of the Recovery Locations page, select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
    a. Top bar menu
    b. Top bar menu

Location context menu

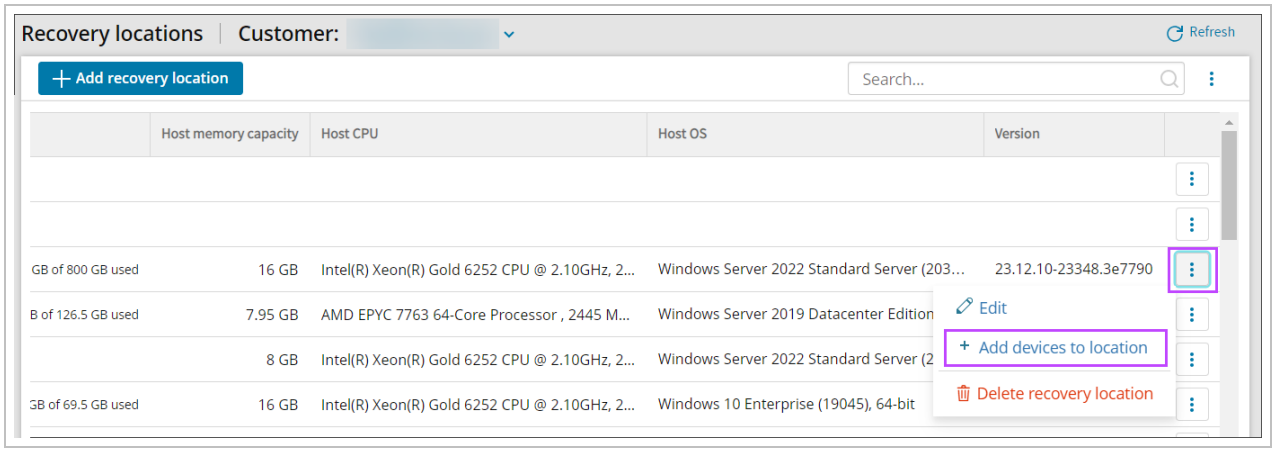
1. Right-click on the Recovery Location to add the device to
2. Select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
    a. Enable Standby Image to AzureDevices cannot be added to a Standby Image plan if already assigned to a Recovery Testing plan.Devices can be assigned to multiple Standby Image plans at once, i.e. Standby Image to Hyper-V and Standby Image to Azure. From Main DashboardTo enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:Log in to the Management Console under a SuperUser or Manager account In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan toClick Add to recovery plan from the Toolbar Select Standby Image (Azure)Select the customer the device(s) you wish to apply the Standby Image plan belong toChoose the recovery location as was configured in Add Recovery LocationsIf the selected customer does not have any locations, you must add one before continuing by selecting Add recovery location. See Add Recovery Locations for full details of adding a location.It is not possible to assign a location for which the Host availability is "Offline"Click NextConfirm the device selected from the Dashboard is compatible and click Next Enter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereClick Next to continueChoose the boot check frequency:OffEvery recovery sessionDailyWeeklyBiweeklyMonthlyIf you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Once connected, click NextClick Azure VM settings towards the right-hand side of the screen to open the settings configuration window:Configure the Azure VM Settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk typeData disk(s) typeVirtual NetworkSubnetAssign NSG and public IPDuring the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend blocking internet access for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.Click Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowConfirm assigning the plan to the device(s)Wait for the plan to be assigned until you see a confirmation banner on the pageClick FinishFrom Standby Image OverviewLog in to the Management Console under a SuperUser or Manager accountNavigate to Continuity > Standby ImageClick Add to PlanSelect Standby Image (Azure)You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the planRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding:
    b. Top bar menu
    c. Top bar menu

Right-hand menu

1. Click the action menu button for the Recovery Location, seen as three dots in a vertical line to the right of the location's version
2. Select **Add devices to location**



3. You will now be taken to the Add devices wizard for the location type:
    a. Enable Standby Image to AzureDevices cannot be added to a Standby Image plan if already assigned to a Recovery Testing plan.Devices can be assigned to multiple Standby Image plans at once, i.e. Standby Image to Hyper-V and Standby Image to Azure. From Main DashboardTo enable Standby Image to Azure on a device from the Management Console's main Dashboard, follow the steps below:Log in to the Management Console under a SuperUser or Manager account In the Backup Dashboard, tick the checkbox to the left of the device(s) you wish to assign a plan toClick Add to recovery plan from the Toolbar Select Standby Image (Azure)Select the customer the device(s) you wish to apply the Standby Image plan belong toChoose the recovery location as was configured in Add Recovery LocationsIf the selected customer does not have any locations, you must add one before continuing by selecting Add recovery location. See Add Recovery Locations for full details of adding a location.It is not possible to assign a location for which the Host availability is "Offline"Click NextConfirm the device selected from the Dashboard is compatible and click Next Enter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key - Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereClick Next to continueChoose the boot check frequency:OffEvery recovery sessionDailyWeeklyBiweeklyMonthlyIf you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Once connected, click NextClick Azure VM settings towards the right-hand side of the screen to open the settings configuration window:Configure the Azure VM Settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk typeData disk(s) typeVirtual NetworkSubnetAssign NSG and public IPDuring the boot test process, certain softwares on your virtual machine (VM) may communicate with vendor servers, initiating a check for updates or license validation. This could be interpreted as a new software license, leading to unexpected charges. To avoid these extra costs, we recommend blocking internet access for your target VMs in Azure. You must ensure the target VM still retains access to Azure storage as Cove will need this to process syslog to verify boot test results.Click Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowConfirm assigning the plan to the device(s)Wait for the plan to be assigned until you see a confirmation banner on the pageClick FinishFrom Standby Image OverviewLog in to the Management Console under a SuperUser or Manager accountNavigate to Continuity > Standby ImageClick Add to PlanSelect Standby Image (Azure)You will now be taken to the Add device to plan wizard. Follow the steps to enable the Standby Image to Azure Plan starting at step #5 by confirming the Customer selected is correct where you can now follow the above instructions to add the device to the planRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding:
    b. Top bar menu
    c. Top bar menu

Configure N-able Recovery Service on Azure Recovery Locations

Installing the Recovery Locations recovery service on Azure requires additional configuration during setup of the Azure VM:

- Check the Requirements
- Configuration
  - Step 1: Download the Recovery Service
  - Step 2: Create Recovery Location VM
  - Step 3: Assign Permissions to the Recovery Location VM
  - Step 4: Install the Recovery Service on the Recovery Location VM
  - Step 5: Add Antivirus Exclusions
  - Step 6: Configure Recovery Location in Management Console
- Check recovery location

Azure Requirements

To install the Recovery Location's recovery service on an Azure VM, the following requirements are necessary:

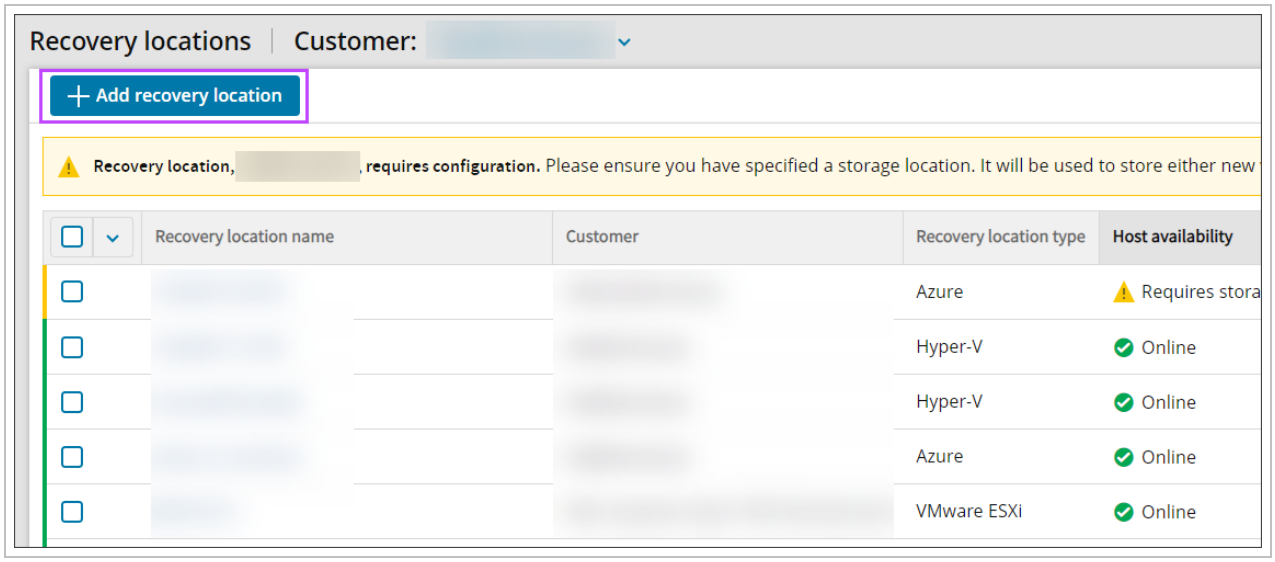
- A user created for you in your Azure tenant. The user must:
  - Have access to a subscription
  - Have access to a resource group you want to use to keep the Recovery Location VM and restored (target) Azure VMs
  - Be able to assign permissions on virtual machines within the resource group

Configuration

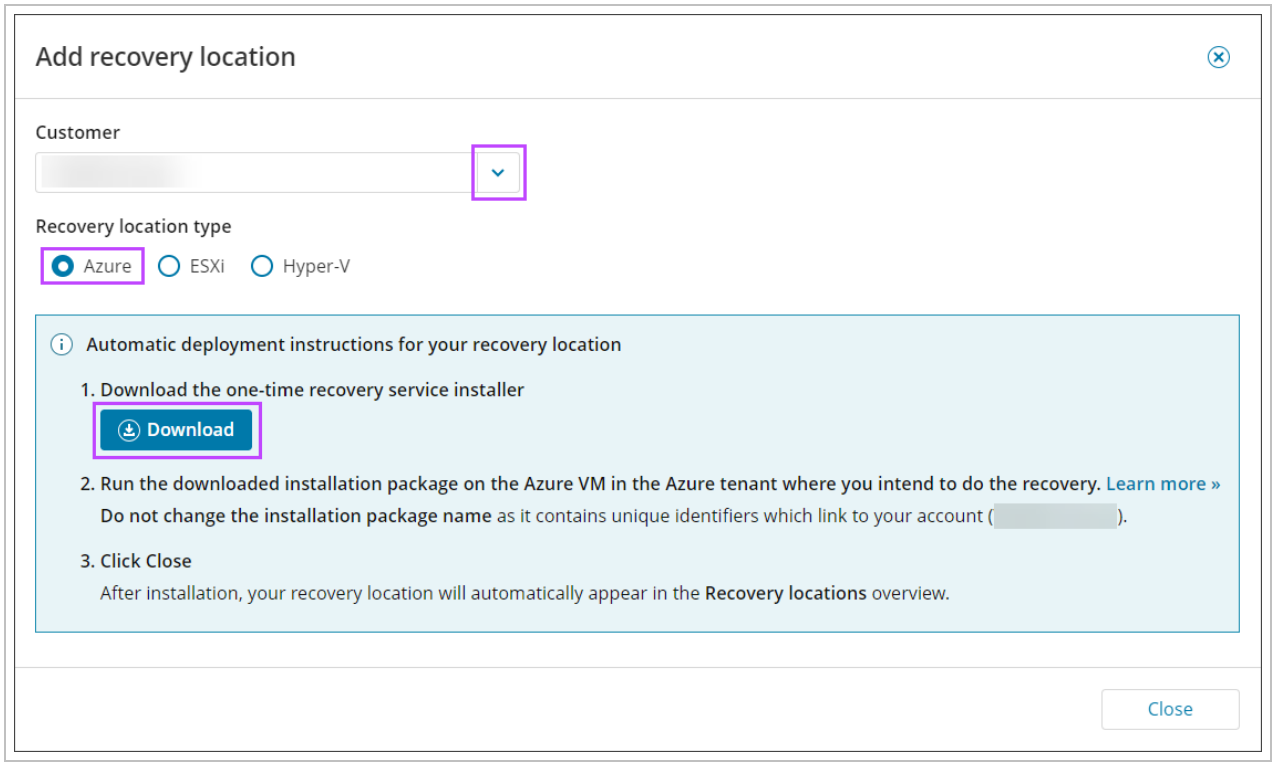
> It is important to follow the installation steps in the order below. If you grant the Recovery Location VM access to a resource group after installing the Recovery Service, you must then reboot the Recovery Location VM for these changes to take effect.

Step 1: Download the Recovery Service

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Click **Add recovery location** at the top of the page



4. In the **Add Recovery Location wizard**, select the customer to attribute the recovery location to, from the dropdown



5. Select **Azure** as the Recovery Location Type
6. Download the recovery service installer and save it to an easily found place on your device

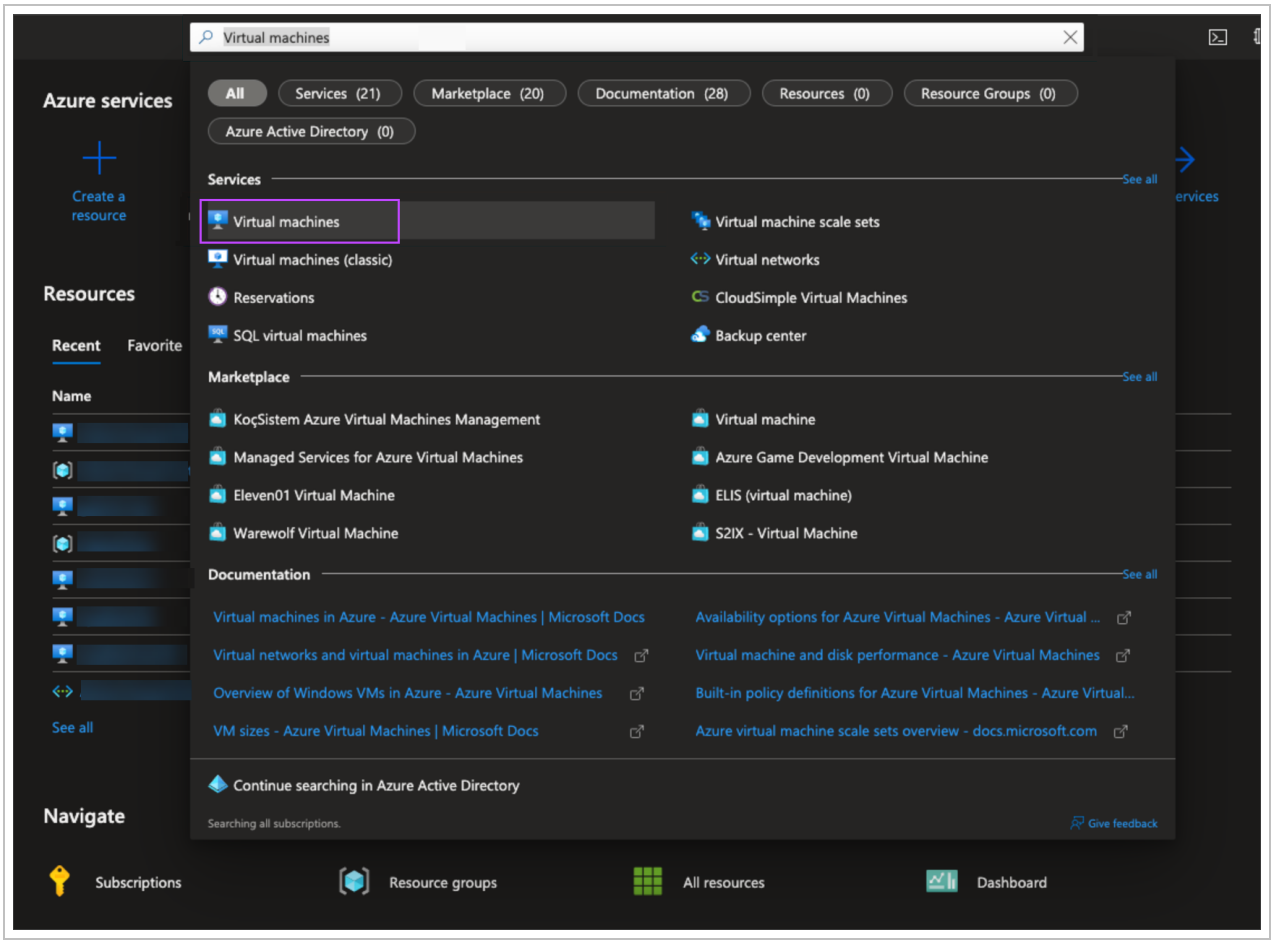
Do **not** change the installation package name. The installation package name contains unique identifiers to your account.

This is a one-time installer and can only be used to install a single instance of the recover service. The installer will fail if you attempt to use the same package for another installation.

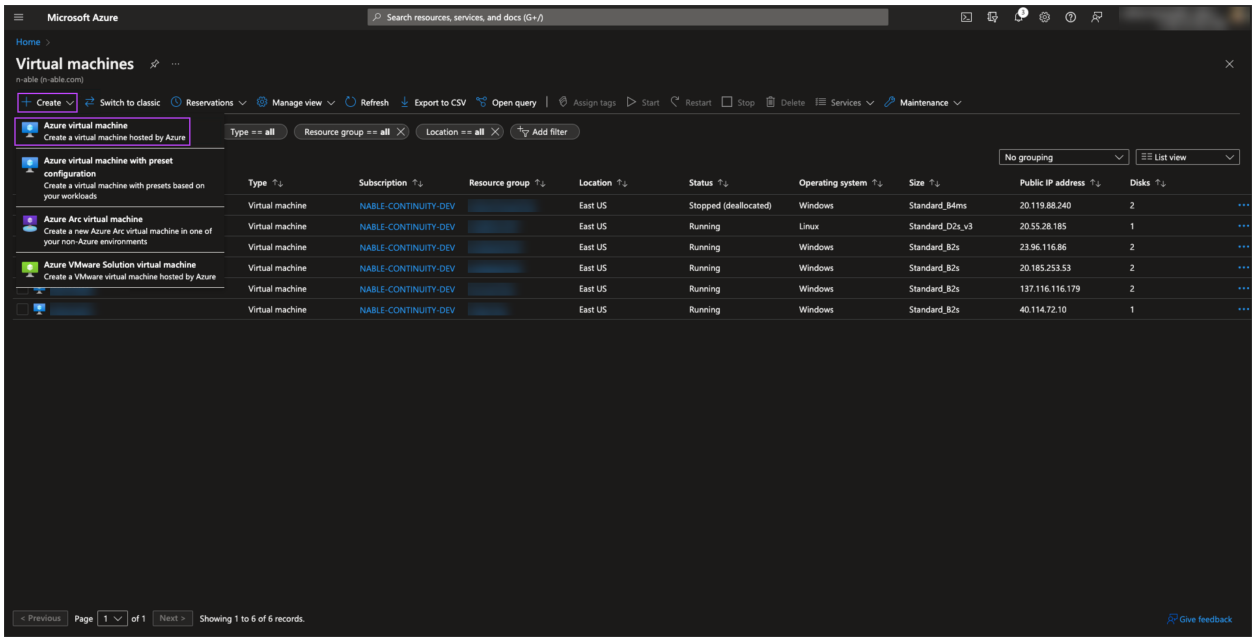
Do **not** run the installer at this point, there are additional changes that are required first.

Step 2: Create Recovery Location VM

1. Login to the Azure portal
2. Using the search bar within the Azure Portal, type **Virtual Machines**, then select the **Virtual Machines service** from the results



3. On the Virtual Machines page, select **+ Create** and select **Azure Virtual Machine** from the dropdown provided



4. On the Basics tab:

Microsoft Azure

Home > Virtual machines >

Create a virtual machine

Basics | Disks | Networking | Management | Monitoring | Advanced | Tags | Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * azure-on-demand

Create new

Instance details

Virtual machine name * -machine

Region * (US) East US

Availability options Availability zone

Availability zone * Zones 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more

Security type Standard

Image * Windows Server 2019 Datacenter - Gen2

See all images | Configure VM generation

VM architecture

- Arm64
- x64

Arm64 is not supported with the selected image.

Run with Azure Spot discount

Size * Standard_D2s_v3 - 2 vcpus, 8 GiB memory (US$137.24/month)

See all sizes

Administrator account

Username *

The value must not be empty.

The value must be between 1 and 20 characters long.

Password *

The value must not be empty.

The value must be between 12 and 123 characters long.

Confirm password *

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular

a. Select a **Subscription** from the dropdown

> The subscription selected here will be used to keep future restored devices. When a subscription is selected for the Recovery Location, this subscription will be used to keep the devices being restored to Azure. A different subscription **cannot** be selected in the One-Time Restore wizard at Azure VM settings step.

b. Select the **Resource Group** you want to use to keep the Recovery Location VM

c. Provide a valid **Virtual Machine Name** for your Recovery Location VM

d. Select the geographic region

> Select the closest geographic region from geographic standpoint to the node where you store backups of the devices you are going to restore to Azure

e. In the **Image** field, select one of:
   a. **Windows Server 2019 Datacenter - Gen2(9)**
   b. **Windows (Windows 10 Pro), version 21H2 Gen 2**

f. Under the **Size** field, click **See all sizes** and search for **b4ms**

> This VM size is the lowest priced size that meets our hardware recommendations for Local VHD restores

g. Set a **Username** and **Password** for the Administrator account

h. For the **Select Inbound Ports** field choose one of:
   a. **RDP connections**
   b. **Bastion**

5. Click **Next : Disks**
6. On the **Disks** tab, select the **OS disk Type** of **Standard HDD**
7. Click **Next: Networking**
8. On the **Networking** tab specify the **vnet** and **subnet**

> The **Recovery Location VM** should be added to the **Network Security Group**, which allows outbound communication.

9. Click **Review + Create**

10. After a few seconds, the request will be validated. Review the settings and click **Create**

Microsoft Azure

Home > azure-on-demand > Marketplace > Virtual machine >

Create a virtual machine ...

Validation passed

Basics | Disks | Networking | Management | Monitoring | Advanced | Tags | **Review + create**

Cost given below is an estimate and not the final price. Please use Pricing calculator for all your pricing needs.

PRODUCT DETAILS

1 X Standard B4ms
by Microsoft
Terms of use | Privacy policy

Subscription credits apply

0.1820 USD/hr
Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

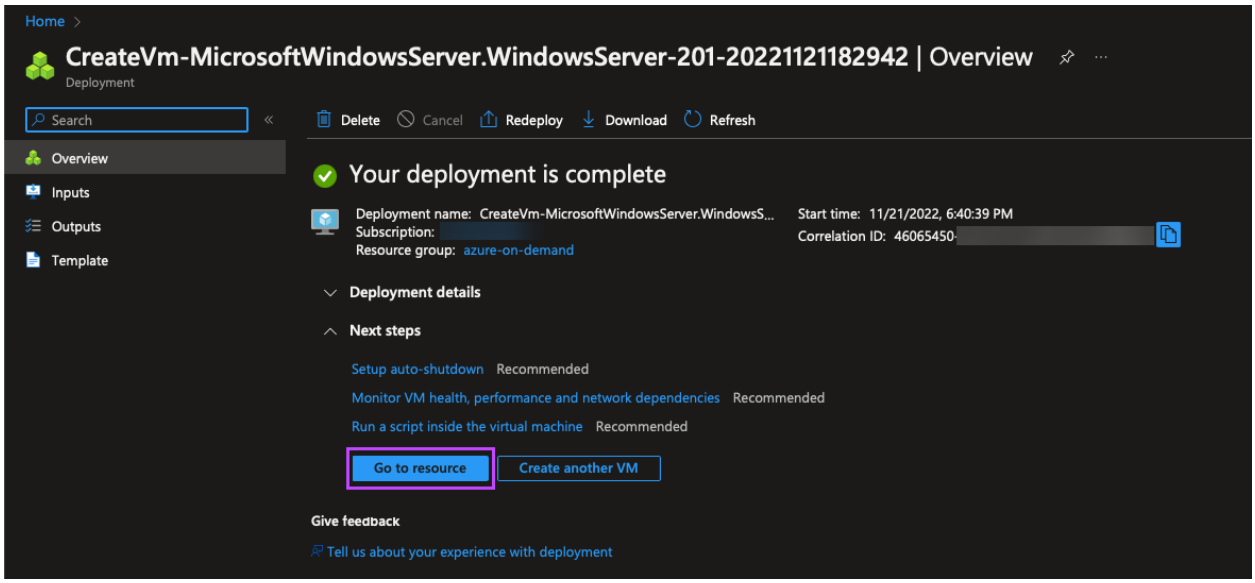
Basics

Subscription	[redacted]
Resource group	azure-on-demand
Virtual machine name	[redacted]-machine
Region	East US
Availability options	Availability zone
Availability zone	1
Security type	Standard
Image	Windows Server 2019 Datacenter - Gen2
VM architecture	x64
Size	Standard B4ms (4 vcpus, 16 GiB memory)
Username	[redacted]
Already have a Windows license?	No
Azure Spot	No

Disks

OS disk type	Standard HDD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

11. A page will display with the progress of the deployment. Once deployment is complete, you are able to go to the resource by clicking **Go to resource**

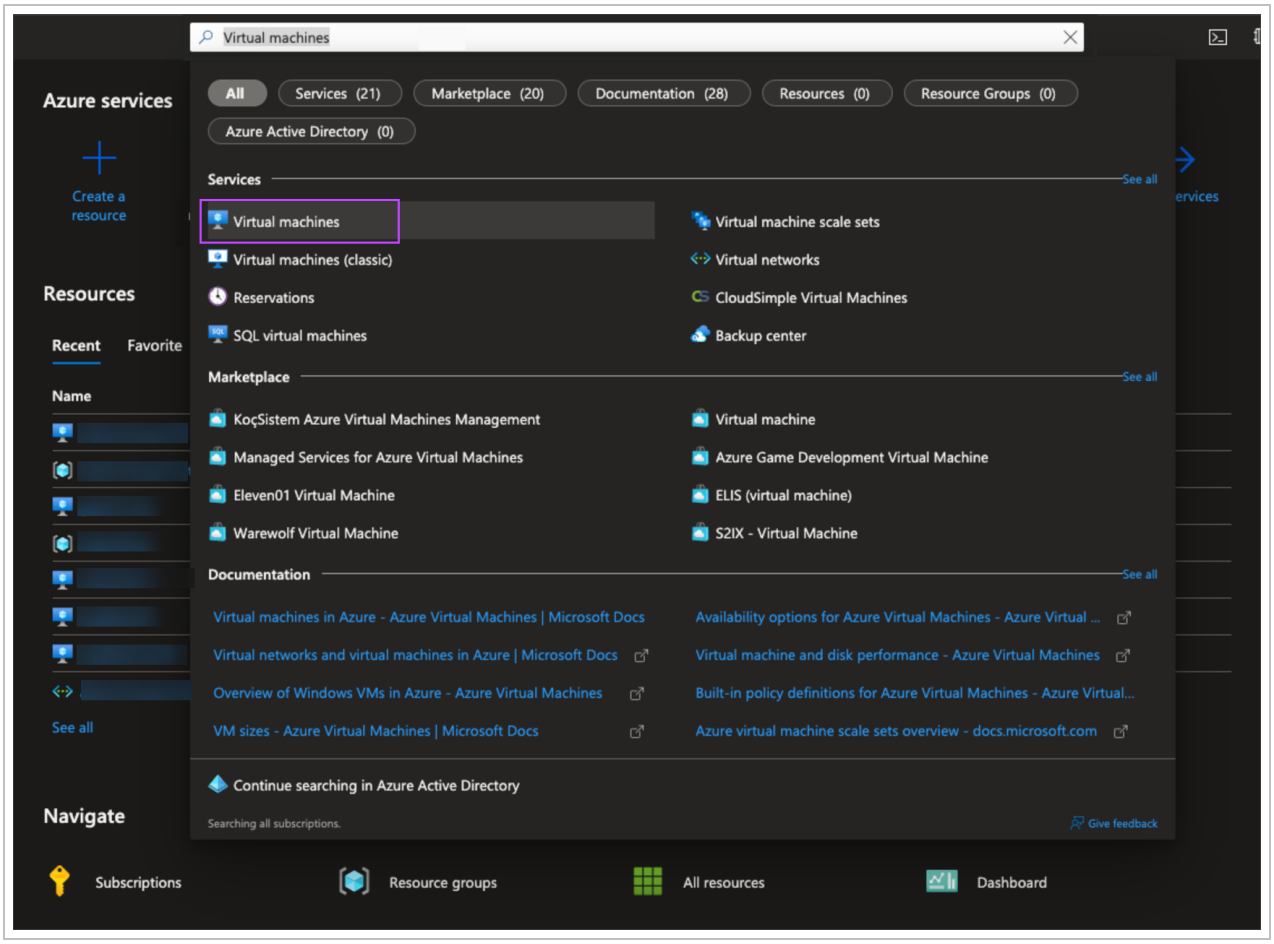


Step 3: Assign Permissions to the Recovery Location VM

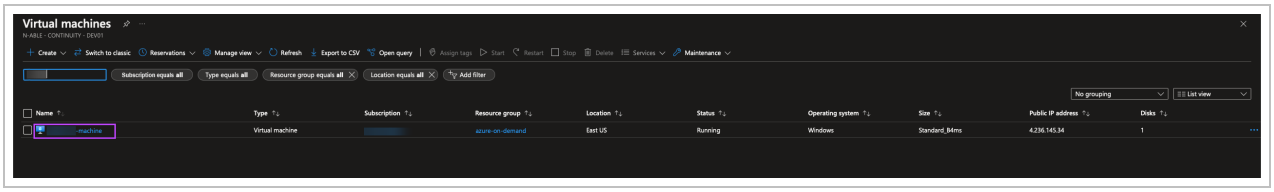
In order for restores to successfully create Virtual Machine's in Azure, Owner permissions must be given to the Recovery Location VM.

> Without these permissions, the restores will start, but will fail when the recovery service attempts to manipulate Azure resources.

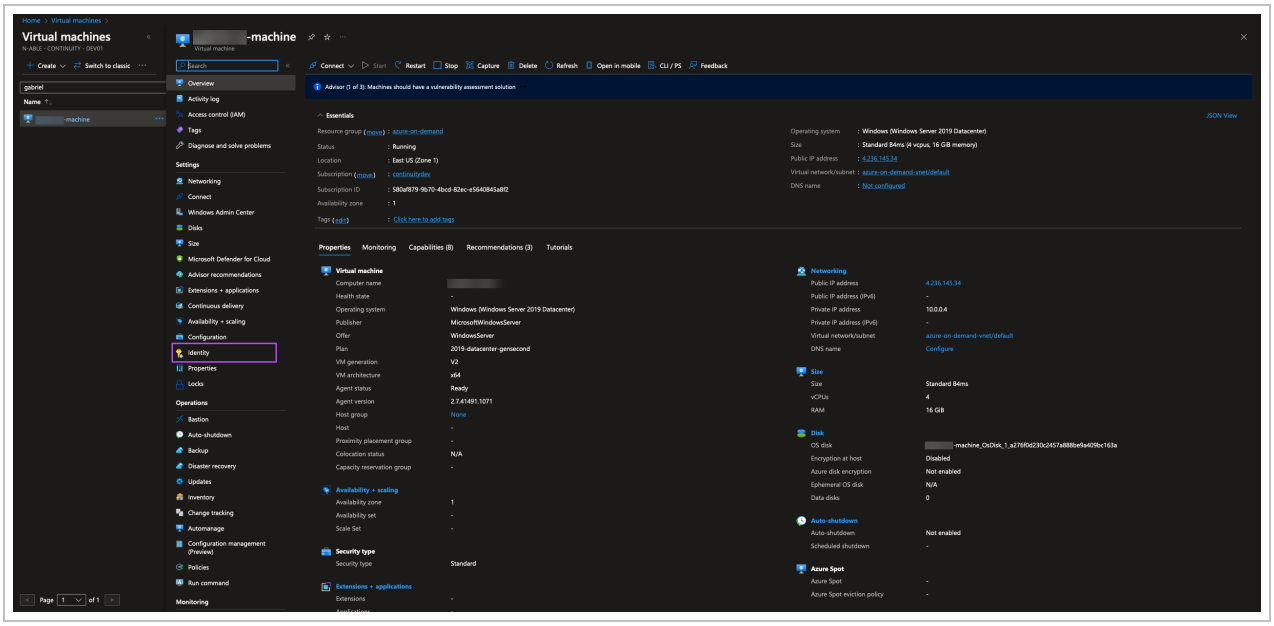
1. Login to the Azure portal
2. Using the search bar within the Azure Portal, type **Virtual Machines**, then select the **Virtual Machines service** from the results



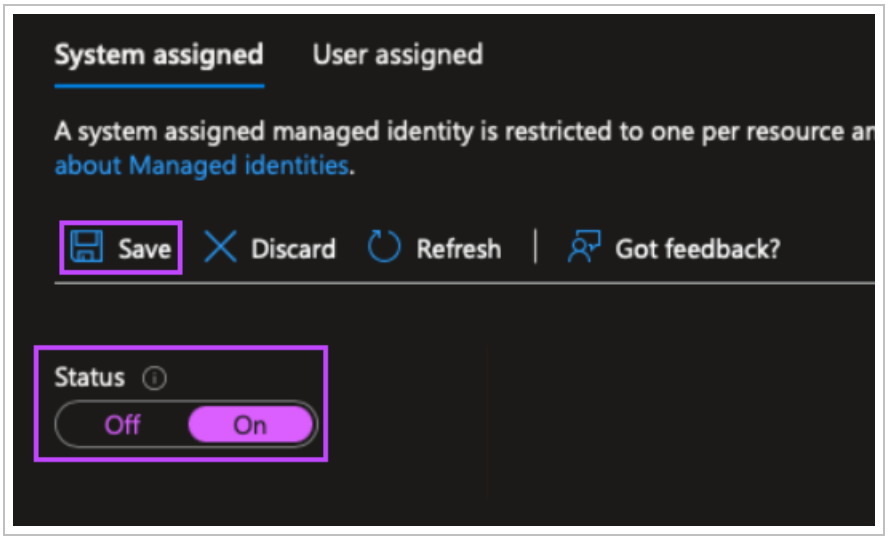
3. On the Virtual Machines page, find the virtual machine created in Step 2 where you will install the Recovery Agent in Step 4 and click the VM name



4. In the Virtual Machine, click the dropdown by the search bar and click **Identity**

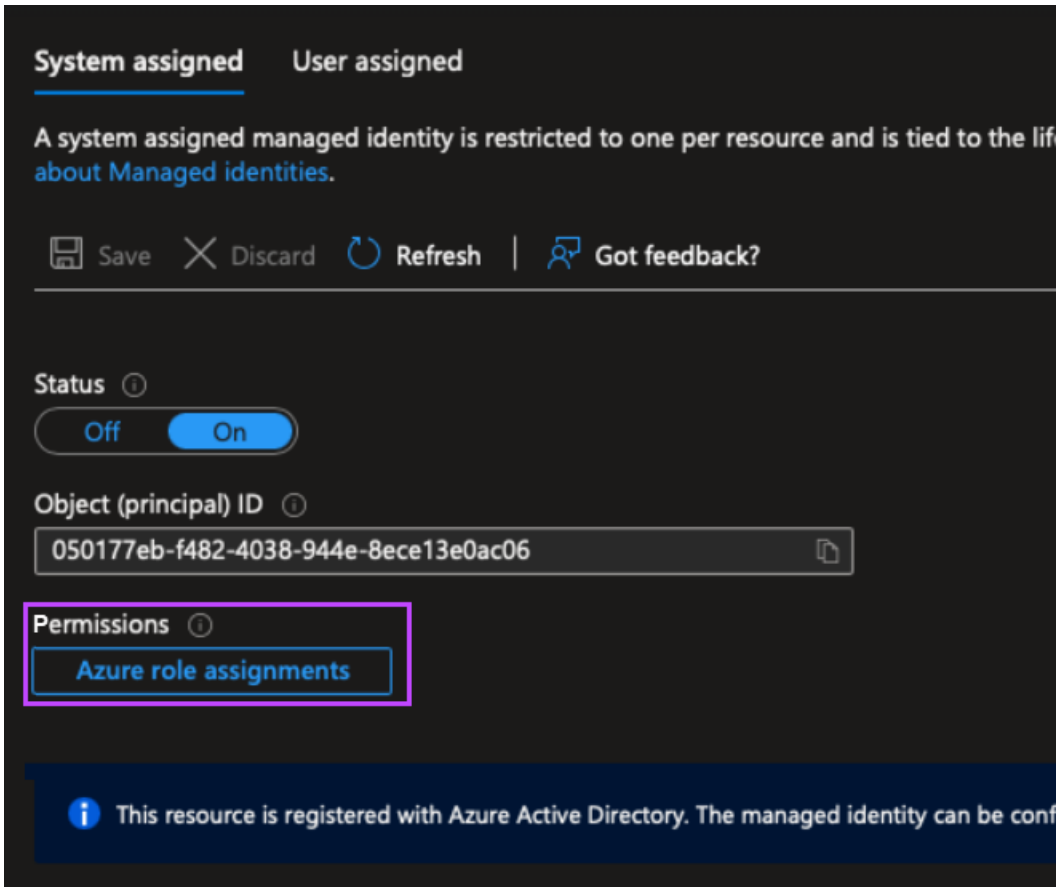


5. In the System Assigned tab, set the **Status** to **ON**



6. Click **Save**

7. Select **Azure role assignments**



8. Click **Add role assignment (Preview)** at the top of the page
9. In the Add role assignment (Preview) window, set the following:
   a. **Scope**: Resource Group
   b. **Subscription**: Select the subscription selected for the Recovery Location VM in Step 2: 4
   c. **Resource Group**: Select the resource group selected for the Recovery Location VM in Step 2: 4
   d. **Role**: Owner

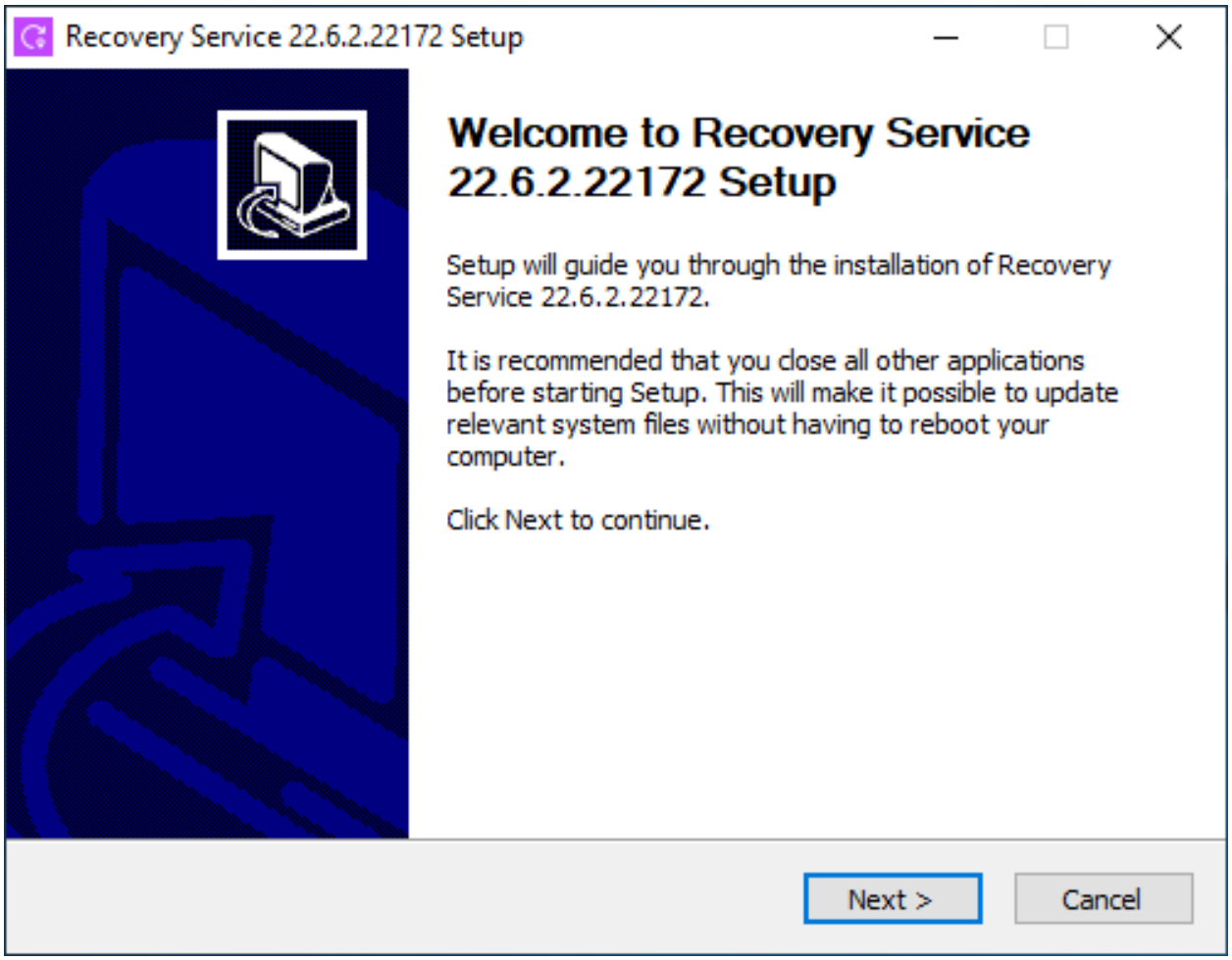
   > If you see a warning message that states "You don't have permissions to add role assignments…", please make sure you have the proper access right to assign roles to the VM.

10. Click **Save**
11. Once complete you will see the role assigned in the **Azure Role Assignments** table
12. To restore to resource groups other than the Recovery Location resource group, or to use virtual networks from other resource groups to place target VMs, you must add role assignments for those groups as well. To do this, repeat step 9 and step 10 for each group

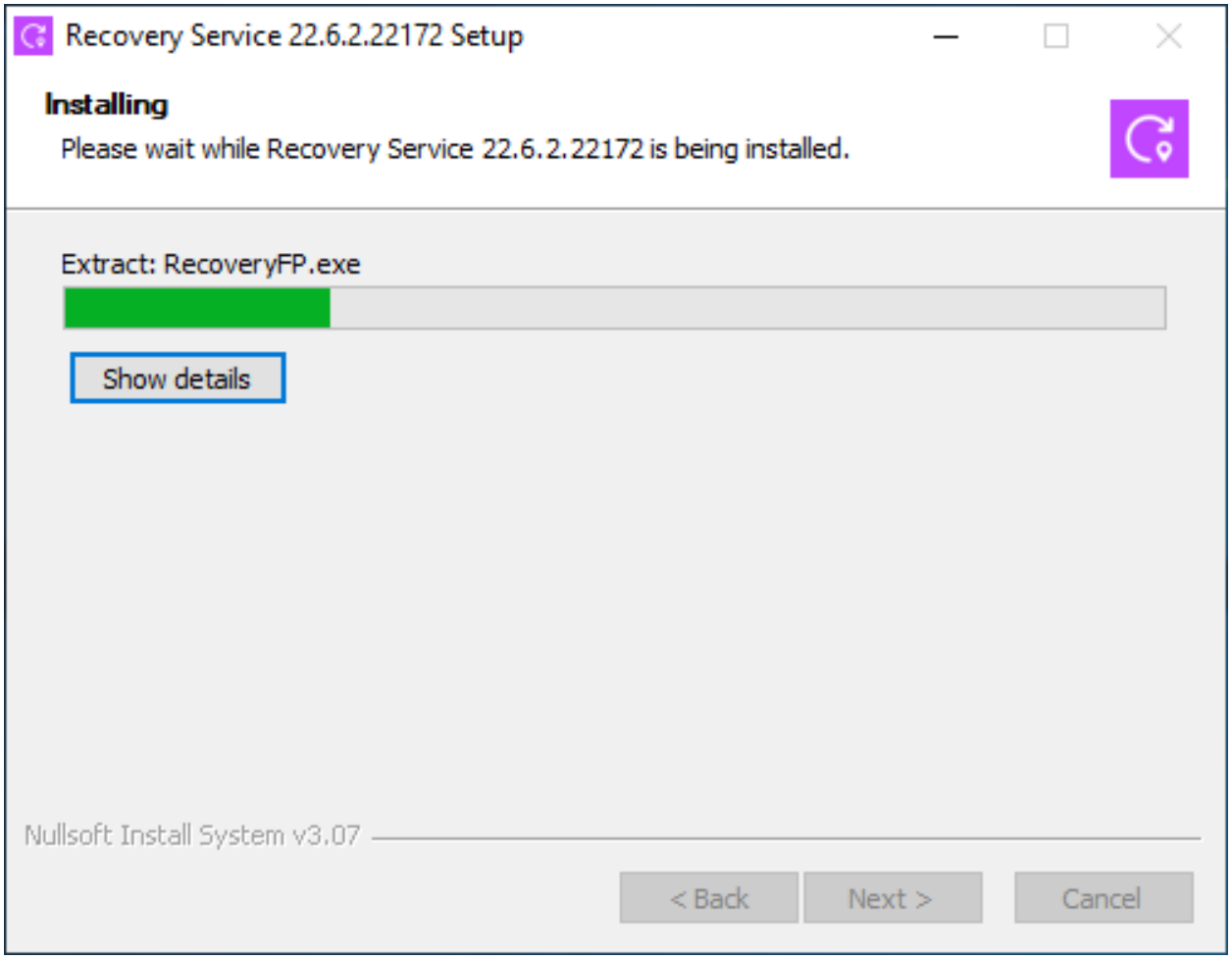
    > If you try to restore to a resource group without the role assignment the restore will fail

Step 4: Install the Recovery Service on the Recovery Location VM

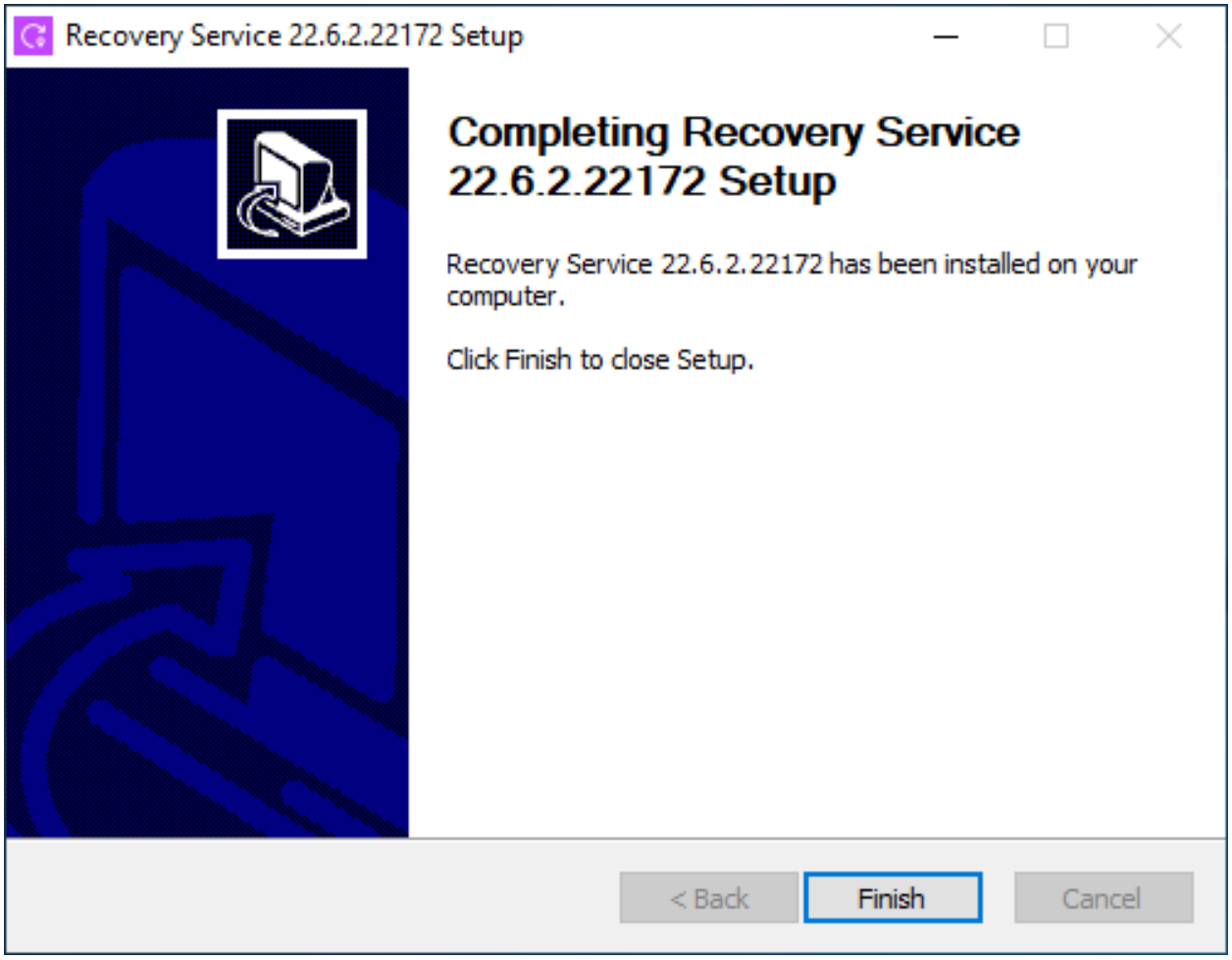
1. Connect to the Recovery Location VM created in Step 2 via RDP or Bastion
2. Copy the Recovery Service downloaded in Step 1:6 from it's location onto the VM
3. Double-click the executable on the Recovery Location VM to run
4. Click **Next** to begin setup



5. Wait for installation to complete



6. Finish the installation and close the wizard



7. After a few minutes, the Recovery Location will appear on the Management Console's Recovery Locations dashboard and can be used to in the One-Time Restore to restore data to Azure

Step 5: Add Antivirus Exclusions

To help speed up Azure restores by up to three times (3x), add the following processes and folders to your Antivirus Exclusions:

Processes

- **AuthTool.exe** - [file location] SYSTEM_DRIVE:\Program Files\Recovery Service*\AuthTool.exe
- **unified_entry.exe** - [file location]. SYSTEM_DRIVE:\Program Files\Recovery Service*\unified_entry.exe
- **RecoveryFP.exe** - [file location] SYSTEM_DRIVE:\Program Files\Recovery Service*\BM\RecoveryFP.exe
- **VdrAgent.exe** - [file] SYSTEM_DRIVE:\Program Files\Recovery Service*\BM\VdrAgent.exe
- **ProcessController.exe** - [file location] SYSTEM_DRIVE:\Program Files\Recovery Service*\BM\ProcessController.exe
- **RecoveryProcessController.exe** - [file location] C:\Program Files\Recovery Service*\BM\RecoveryProcessController.exe

- **ClientTool.exe** - [file location] SYSTEM_DRIVE:\Program Files\Recovery Service*\BM\ClientTool.exe
- **VdrTool.exe** - [file location] SYSTEM_DRIVE:\Program Files\Recovery Service*\VdrTool.exe

Folders

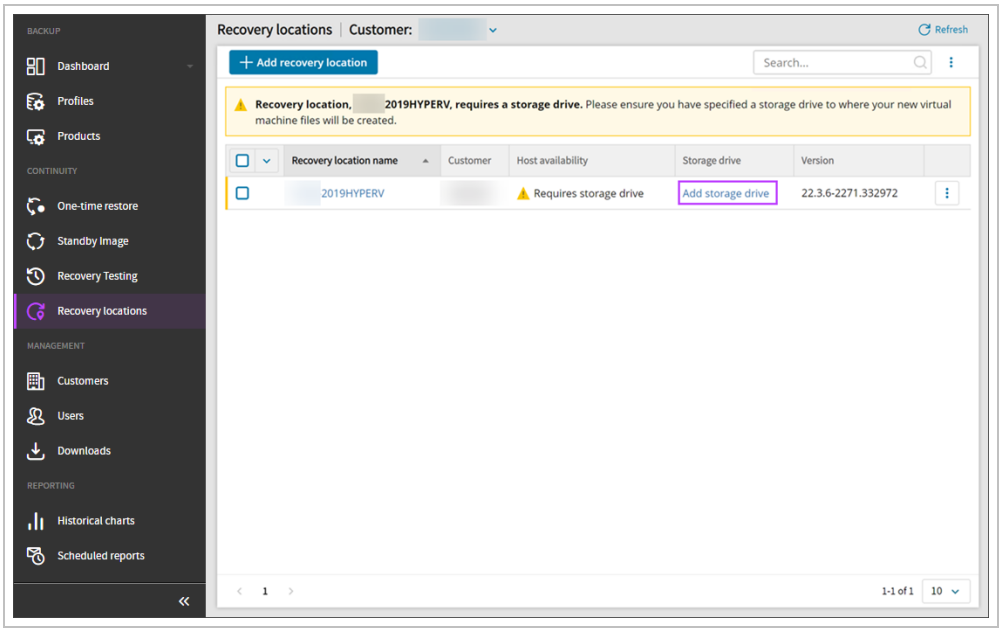
- **StandbyImage** - STORAGE_LOCATION_PATH\StandbyImage
- **OnDemandRestore** - STORAGE_LOCATION_PATH\OnDemandRestore

Step 6: Configure Recovery Location in Management Console

1. Login to the Management Console under a SuperUser account
2. Navigate to **Continuity** > **Recovery Locations**

   > The new recovery location will now be displayed in the list of locations under the customer selected in Step 1: 4

3. Enter the storage drive to assign where the target VM(s) metadata, needed for recovery, will be stored by clicking **Add storage drive** and entering the drive location. E.g. `C:\`



Check recovery location

When the Recovery Location set up is completed you will be able to find it in the drop-down at the first step of One-Time Restore wizard (or on the Recovery Locations Dashboard) and proceed with the restore: Configure One-Time Restore to AzureBefore starting a One-Time Restore to Azure, ensure you have checked all requirements and limitations, including setting up an Azure recovery location.From Backup DashboardLog in to the Management Console under a SuperUser accountIn the Backup Dashboard, tick the checkbox to the left of the device(s) to restoreClick One-Time Restore Select the Azure targetSelect the CustomerSelect the Azure Recovery Location for the restore or click + Add recovery Location to follow the steps to create a new Azure Recovery LocationIf adding a recovery location from here, you will be taken to the Add Azure Recovery Location wizard, where Azure will be automatically selected as the recovery type. Follow the Azure Recovery Location installation instructions from Step #4 onwards.Click NextConfirm compatibility of device(s) and click NextEnter the security code/encryption key or passphrase for the device(s). This can be either:Private encryption key -

Created by yourself when installing Backup Manager on the device. If you have lost the encryption key/security code for the device, you will need to Convert devices to passphrase-based encryptionPassphrase encryption - These are generated on demand for automatically installed devices. You can find information on this hereIf you are logged in as a security officer, this will be detected automatically.Click NextSelect the date and time of the backup session to restoreDuring this step, all available sessions for all devices listed will be loaded in the backup session column. Please allow time for these to load, if the load of sessions fails, a message stating so will be displayed with a refresh button to try again.If you wish to protect the device according to its existing backup schedule, enable Backup target VMIf the Backup Target VM option is enabled for one or more devices, be aware that if the backup agent is still running in backup mode on the source VM, this will lead to corrupted backup data for both the source and target VMs.If you wish to skip all data drives, enable Restore OS disk onlyEnabling Restore OS disk only will help to speed up restores as the only thing being restored is the Operating SystemClick NextConnect to Microsoft Azure by either:Allow permissions to the Azure user account to consent for apps access,or;Login using Application Administrator accessEnsure you have at minimum Reader role access to the subscription containing the Recovery Location VMAccept the required permissions If you do not see the authentication page, make sure your browser is not blocking pop-up windows.Supply the Azure VM settings:SubscriptionThis cannot be changed as the subscription is set in the Recovery Location configurationResource GroupVirtual Machine nameRegionThis cannot be changed as the subscription is set in the Recovery Location configurationAvailability optionsVM sizeIf the VM size selected exceeds the size limit set within the Subscription, a warning will be displayed and you cannot proceed. You must either increase the regional vCPU quota on the Subscription, or decrease the VM size selected in the Azure VM Settings.OS disk type Set to Premium SSD to speed up the Azure restore. This can be changed in Azure laterData disk(s) typeSet to Premium SSD to speed up the Azure restore. This can be changed in Azure laterVirtual NetworkSubnetStop target VM after recoveryAssign NSG and public IPClick NextClick Next to progress to the Report window to enter one or more email addresses to receive a report when: The recovery is complete (Successful or Failed)The recovery was successfulThe recovery failedMultiple addresses should be separated using a comma or semi-colonIf you do not want to add an email address to receive reports, click Skip this stepTo remove all branding from the reports, use the Remove Cove branding toggle per device, or above the device list to apply the changes to all devices in this windowReview and confirm the restore details for each device and click ConfirmOnce the restore has been started, a green banner will be displayed and a notification in the top right-hand corner of the screen to confirm. Click Finish to close the restore wizard and return to the DashboardFrom One-Time Restore OverviewLog in to the Management Console under a SuperUser accountNavigate to the One-Time Restore overview by selecting Continuity > One-time Restore from the vertical menu on the left hand sideClick One-time restore from the top barThe wizard will open to target selection window, follow the above steps from Step #4 onwardsRecovery ReportsWhen the device(s) assigned to the plan have Successful recovery report email or Failed recovery report email recipient address(es) configured, and once the test has completed, those recipients will receive the report in their email inbox. Here is an example report with Cove branding:Here is an example without Cove branding:.

Configure N-able Recovery Service on ESXi Host Server

Installing the Recovery Locations recovery service on an ESXi Host Server requires additional configuration during the setup of the environment:

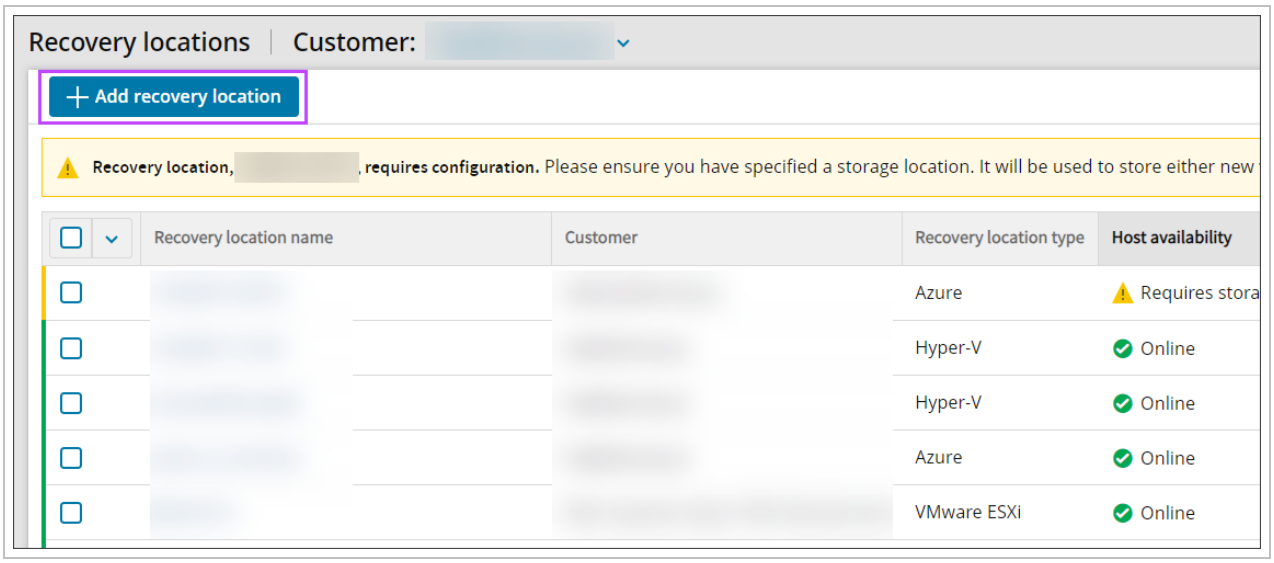
- Check the Requirements
- Configuration
  - Step 1: Download the Recovery Service
  - Step 2: Create vSphere Client User
  - Step 3: Create Recovery Location Virtual Machine
  - Step 4: Install Recovery Service On VM
  - Step 5: Add Storage Location and Server Connections
  - Step 6: Add device to Standby Image plan

Configuration

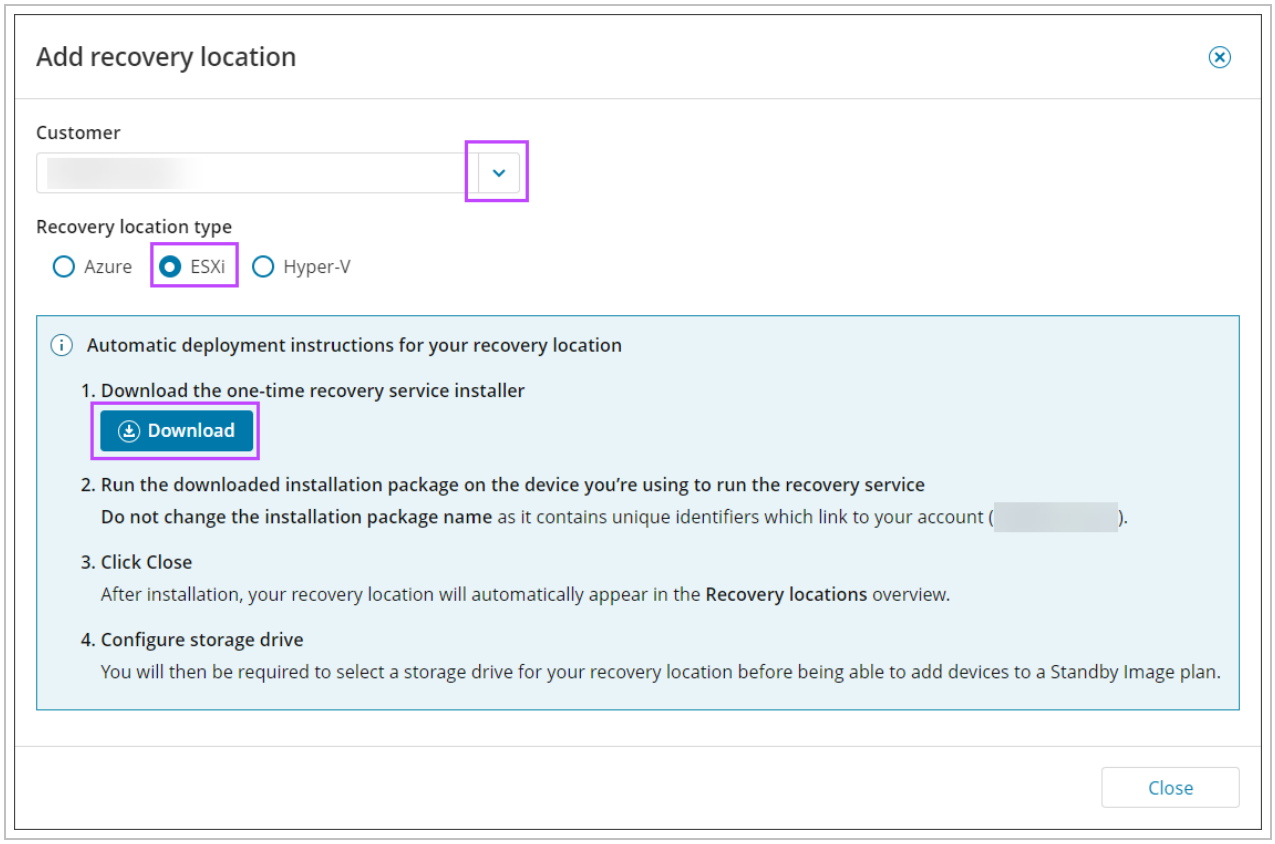
> It is important to follow the installation steps in the order below.

Step 1: Download the Recovery Service

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Click **Add recovery location** at the top of the page



4. In the **Add Recovery Location wizard**, select the customer to attribute the recovery location to from the dropdown



5. Select **ESXi** as the recovery location type
6. Download the recovery service installer

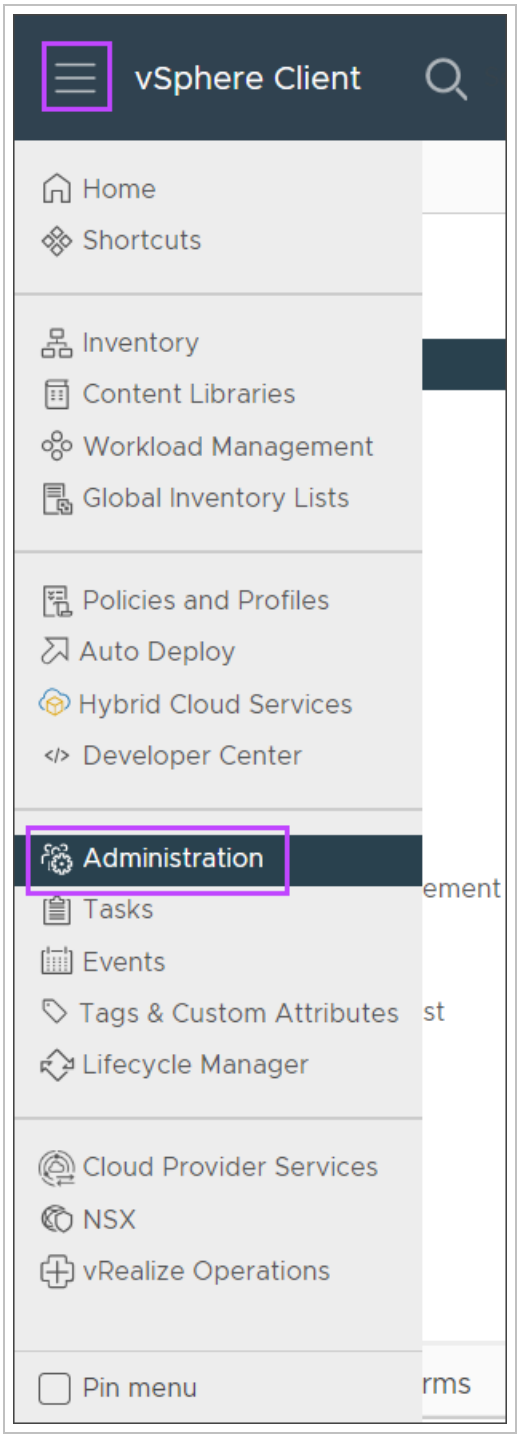
> Do **not** change the installation package name. The installation package name contains unique identifiers to your account.
>
> This is a one-time installer and can only be used to install a single instance of the recovery service. The installer will fail if you attempt to use the same package for another installation.

Do **not** run the installer at this point, there are additional changes that are required first.

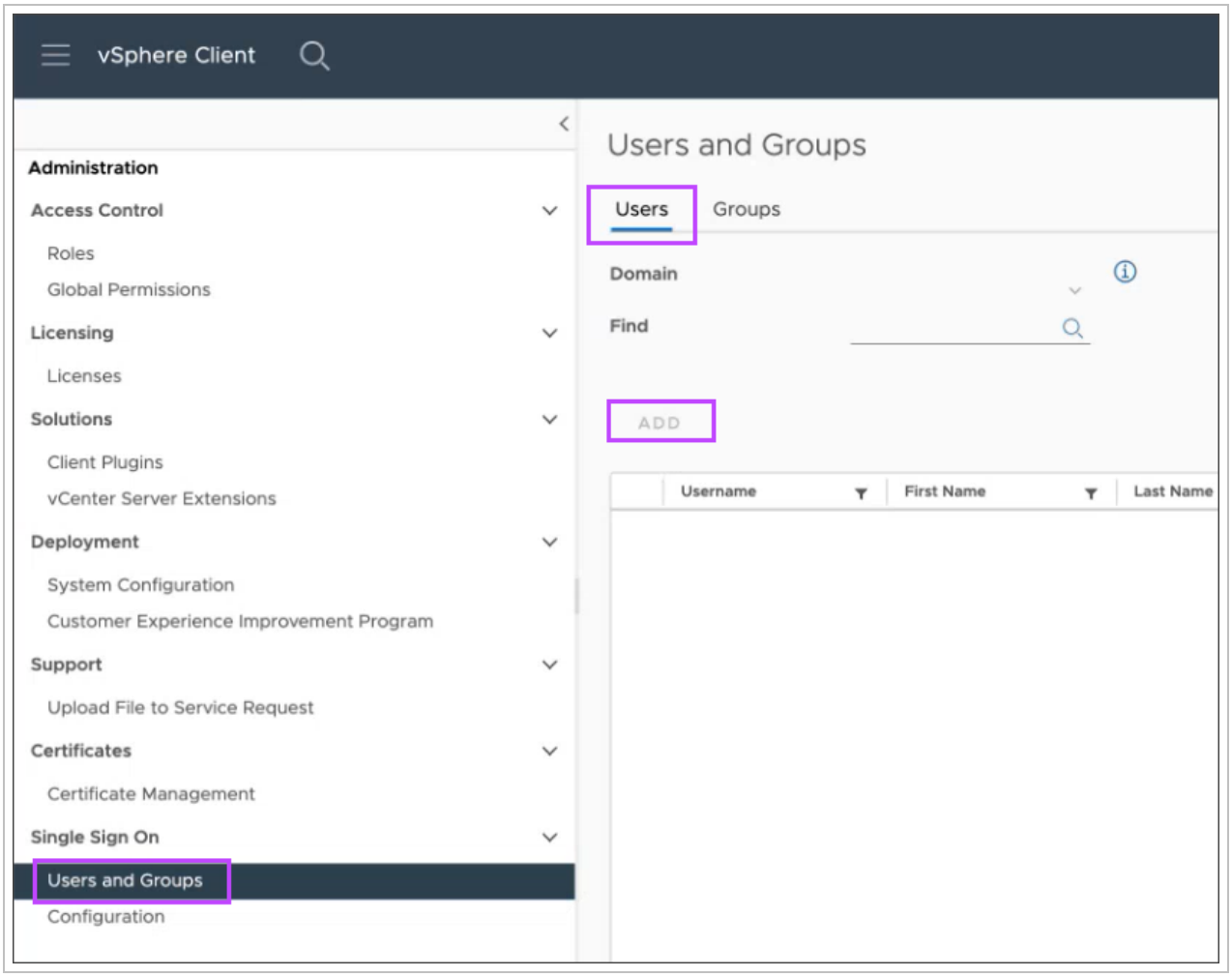
If you want to restore to Local VMDK format go now to Step 4. As you will not restore to an ESXi server, is not obligatory to configure vSphere Client user and Virtual Machine in vCenter.

Step 2: Create vSphere Client User

1. Login to the **vCenter Server** by using the **vSphere Client**
2. Open the menu and navigate to **Administration**



3. In the **Users and Groups** page, select the **Users** tab and click **Add**



4. Fill in the user details and **Save** the new user
5. Once the new user has confirmed access, assign the **Administrator** role to the user

> The user **must** be assigned the Administrator role for Standby Image to ESXi to function appropriately. Do **not** use a custom role with lesser privileges.

There are two options for where to install the Recovery Service:

1. Create a recovery location Virtual Machine within the ESXi server/host (recommended)

> This option is recommended as performance is increased as data doesn't have to transfer over the network during the restore

> To use this option, follow the instructions in Step 3: Create Recovery Location Virtual Machine

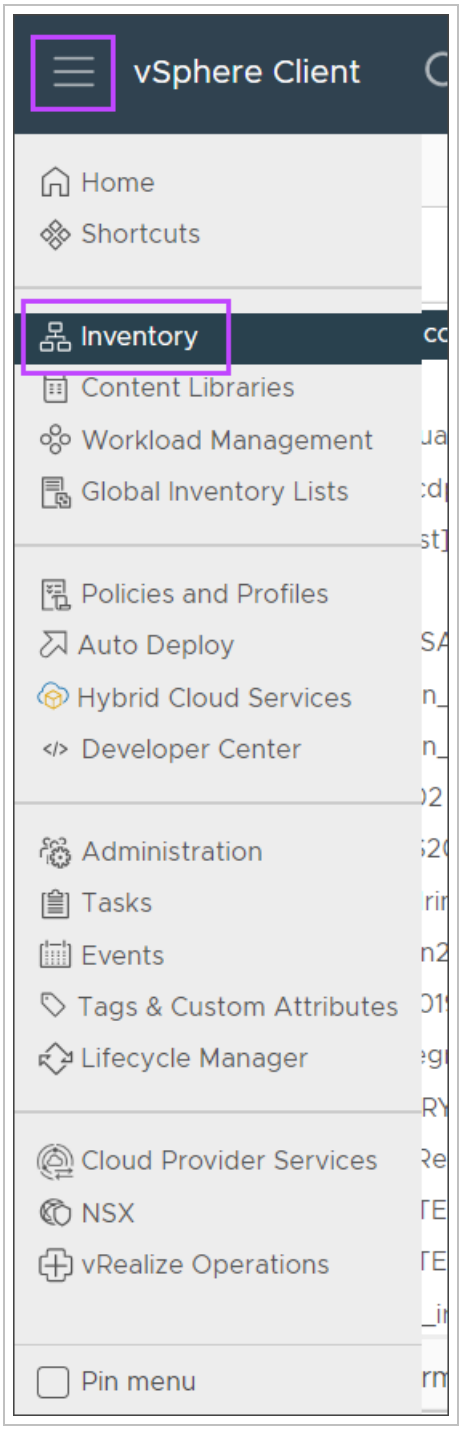
2. If you have multiple vCenter servers and want to restore to multiple ESXi servers/hosts directly (not to vSphere) it is recommended to create a recovery location on a dedicated server/host

   This option doesn't require the server to be stored anywhere but it **must** have access to vSphere

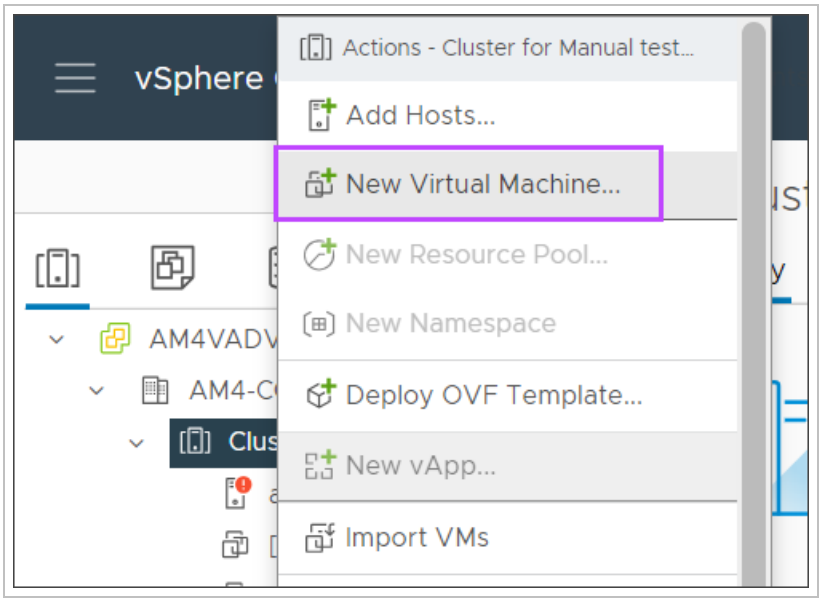
   To use this option, skip straight to Step 4: Install Recovery Service On VM

Step 3: Create Recovery Location Virtual Machine

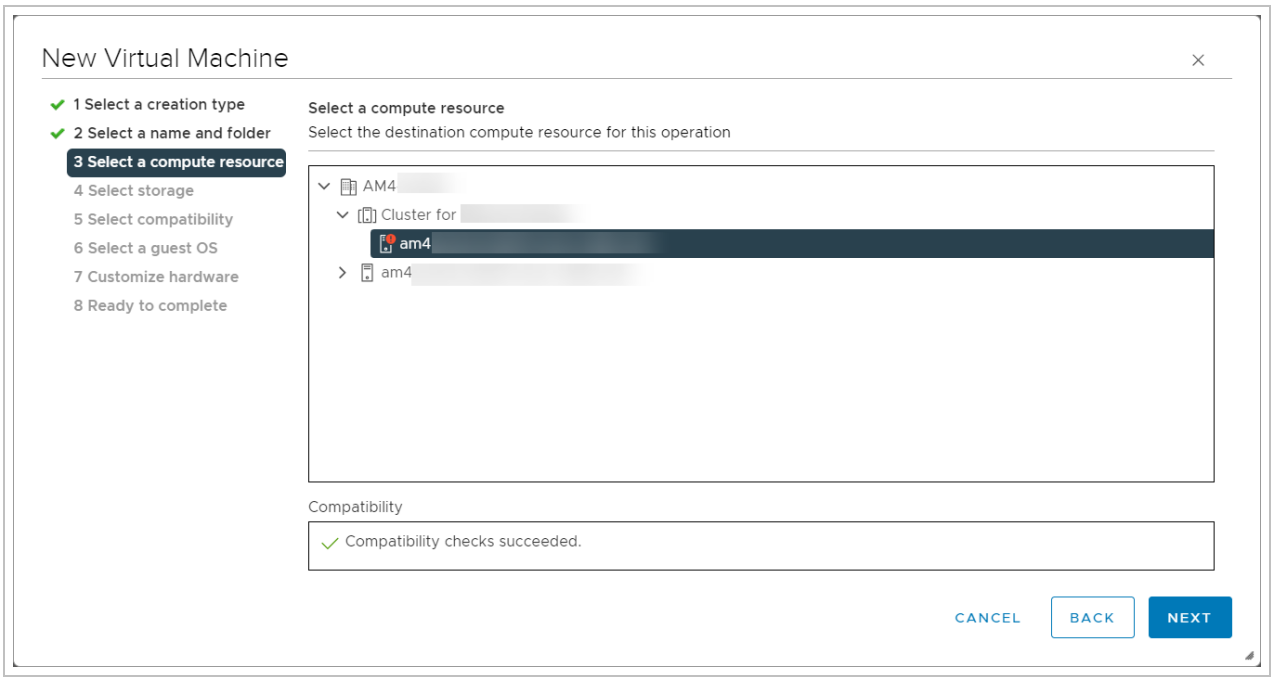
1. In the **vCenter Server** now navigate to **Inventory** in the menu



2. Right click the cluster and select **New Virtual Machine**

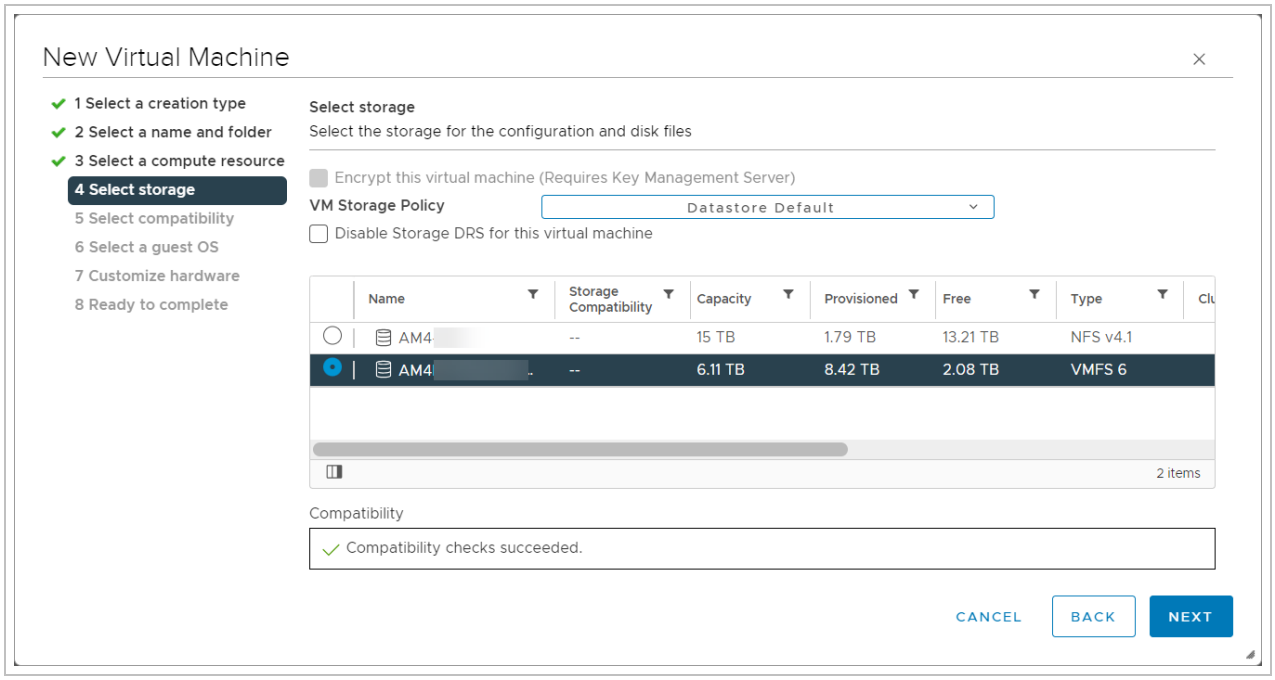


3. In the Creation Type list, select **Create a new virtual machine** then click **Next**
4. Give the Virtual Machine a name and select a location for the virtual machine from the resource tree
5. Click **Next**
6. From the resource tree, select a compatible destination compute resource and click **Next**



7. Select the data store from the available options for the configuration and disk files and click **Next**

> The selected storage **must** have enough capacity to run the restores and store Virtual Machine data



8. Select the ESXi version to ensure the new Virtual Machine is compatible with the host in your environment and click **Next**
9. Configure the guest Operating System from the dropdowns provided and click **Next**

> **Microsoft Windows Server 2019** is recommended

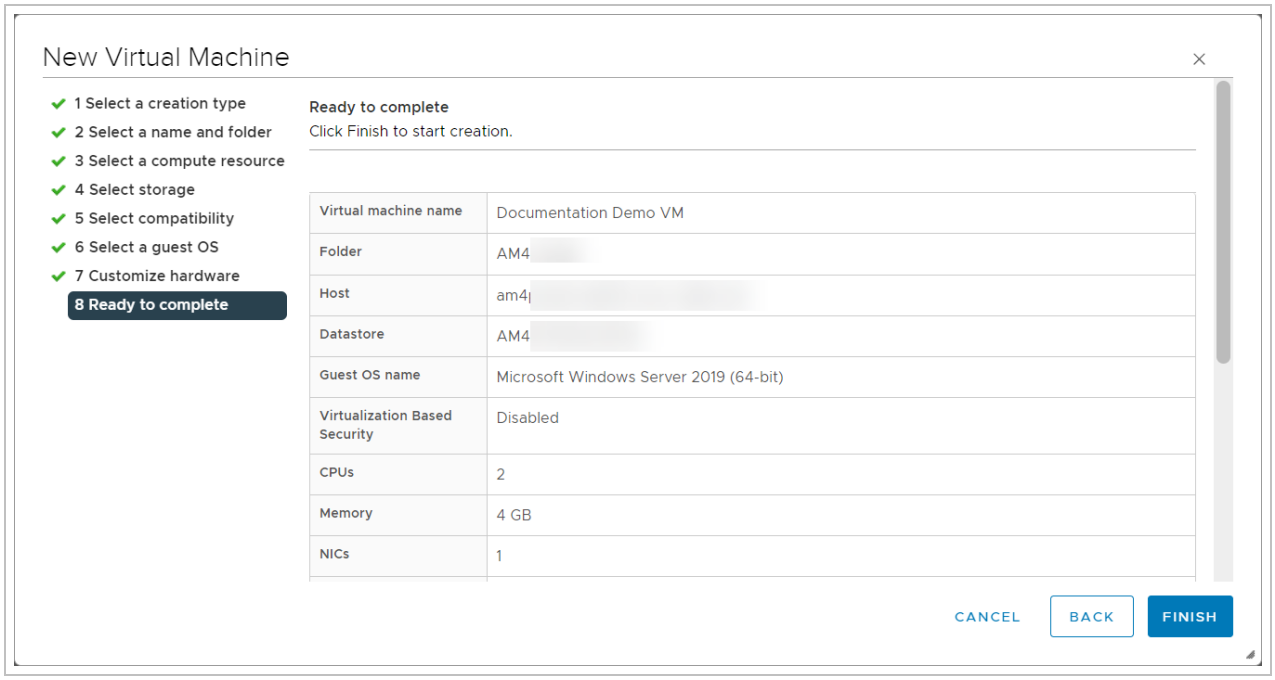
10. Customize the virtual hardware as per our requirements:

> See the Minimum Requirementsfor our default hardware configuration recommendations

> It is possible to run multiple parallel restores so long as the virtual hardware is configured to handle this amount of traffic

11. Click **Next**

12. Confirm the details of the new Virtual Machine and click **Finish** to begin creation of the new Virtual Machine



Step 4: Install Recovery Service On VM

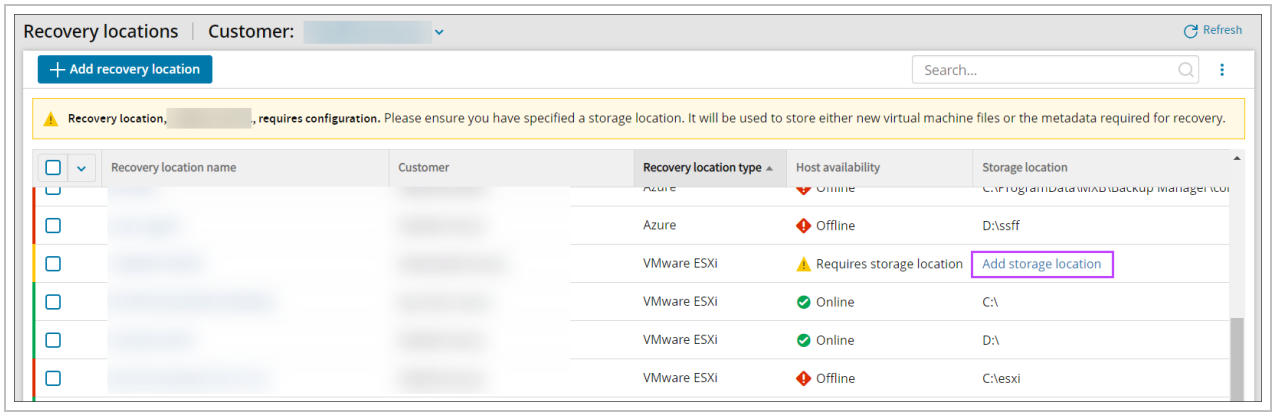
1. Select the newly created Virtual Machine from Step 3 in the **Inventory** list, power it on and click **Launch remote console** or move to the dedicated server/host if restoring to the ESXi server/host directly
2. Transfer the downloaded recovery service file to the machine
3. Run the installation package

> The recovery location will appear in the list on the Management Console after installation is complete

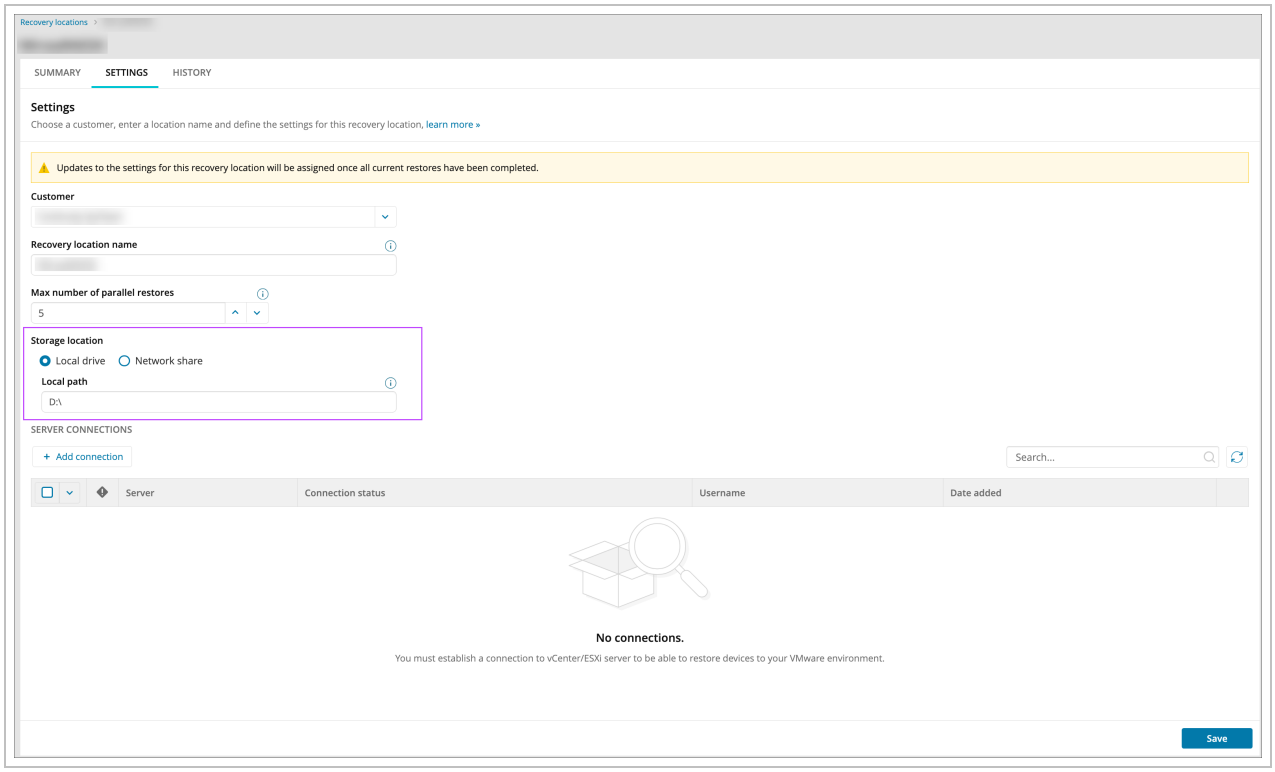
Step 5: Add Storage Location and Server Connections

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**

3. Find the new recovery location in the list and click **Add storage location**

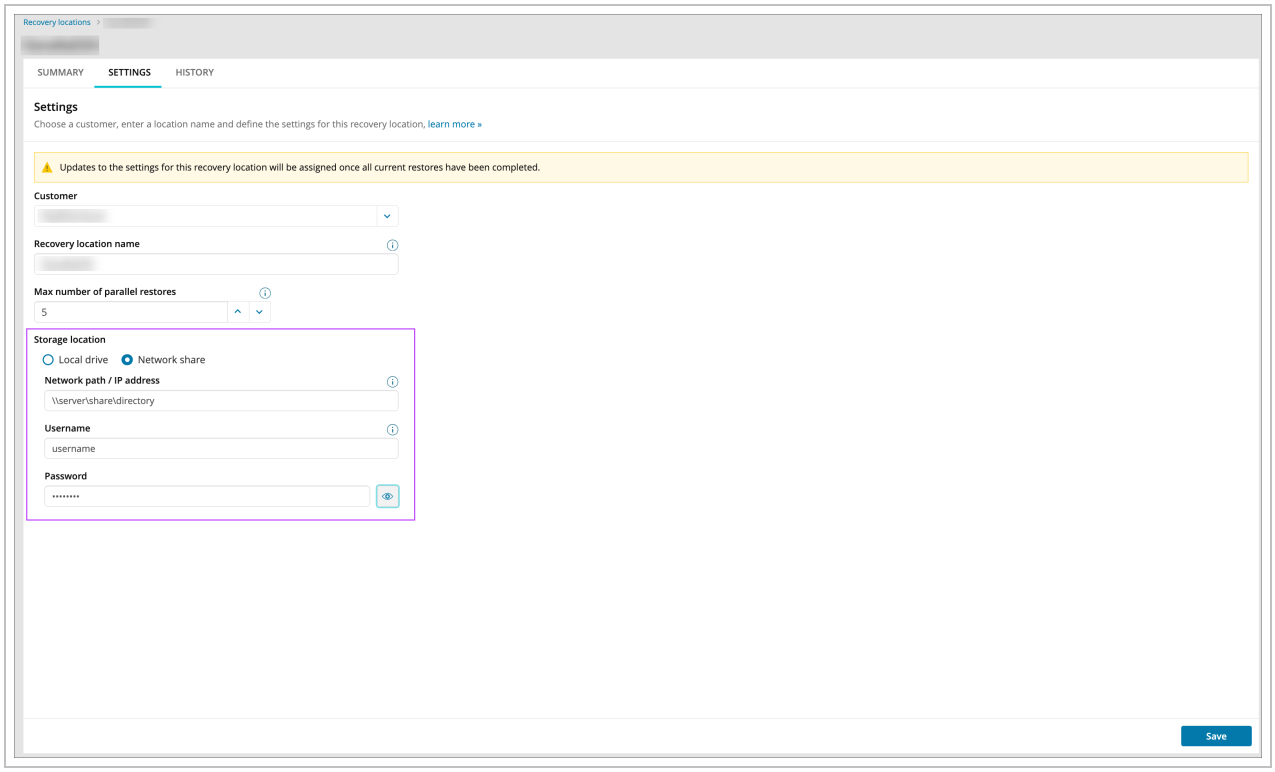


4. Provide local file path for the storage location
   - Local Drive (only available for Hyper-V and ESXi locations):



> Without a storage location, connections **cannot** be made to any of the added servers. If you want to restore to Local VMDK is not obligatory to configure server connections. The VMDK file will be restored directly to the storage path, and not on the ESXi server.

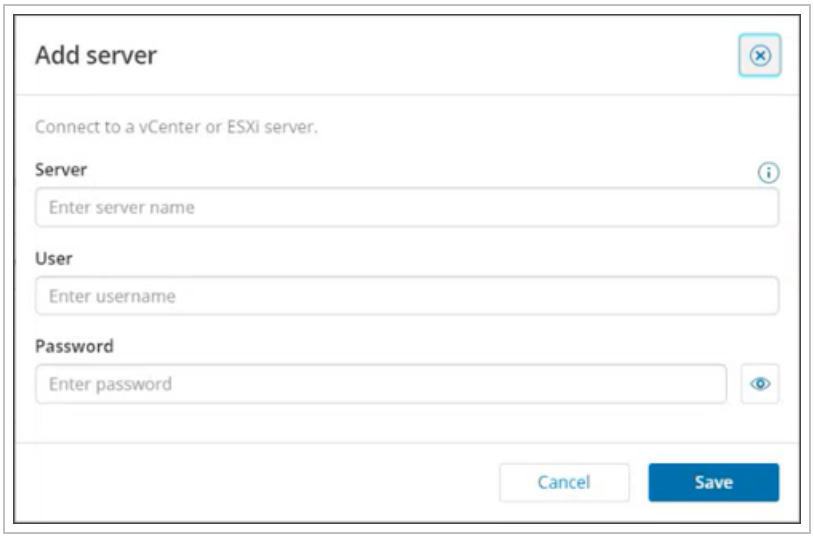
- Network Share:



> Recovery Locations using **Network Shares** will **not** see the option to configure any server connections as the restore will not be done on an ESXi server, and will be done on the Network Share to a Local VMDK restore format.

5. Click **Add Connection** to connect to the vCenter or ESXi server

> If using a connection to the vCenter server, you will be able to restore to any ESXi host connected to the vCenter server



6. Enter the vCenter or ESXi **server name** or **IP address**, and your username and password for this
7. Click **Save**

> Multiple server connections can be added to the recovery location, but must be done one at a time. Doing so will allow you to connect and restore to several ESXi hosts which are not connected to one vCenter Server

> You must click the **refresh** button to above the list of server connections to update the status from 'connecting' to 'connected'. The connection may take a few minutes.

Step 6: Add device to Standby Image plan

Once the server connections are added, you may now add devices to the Standby Image to ESXi recovery plan by following the instructions in Top bar menu

Configure N-able Recovery Service on Hyper-V Server 2019

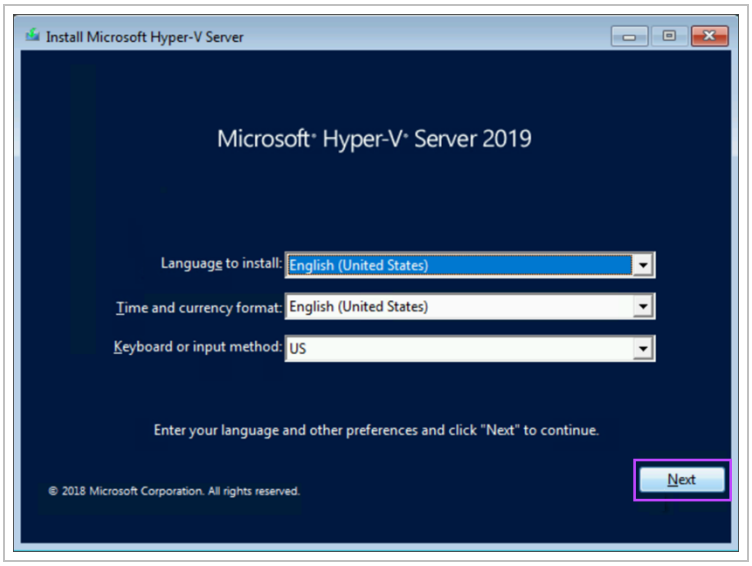
Installing the Recovery Locations recovery service on a Hyper-V Server 2019 requires additional configuration during the setup of the Hyper-V:

- Check the Requirements
- Configuration
  - Step 1: Install the Hyper-V Server
  - Step 2: Configure the Hyper-V Server
  - Step 3: Download the Recovery Service
  - Step 4: Add a role for Hyper-V
  - Step 5: Install and Configure the Recovery Location

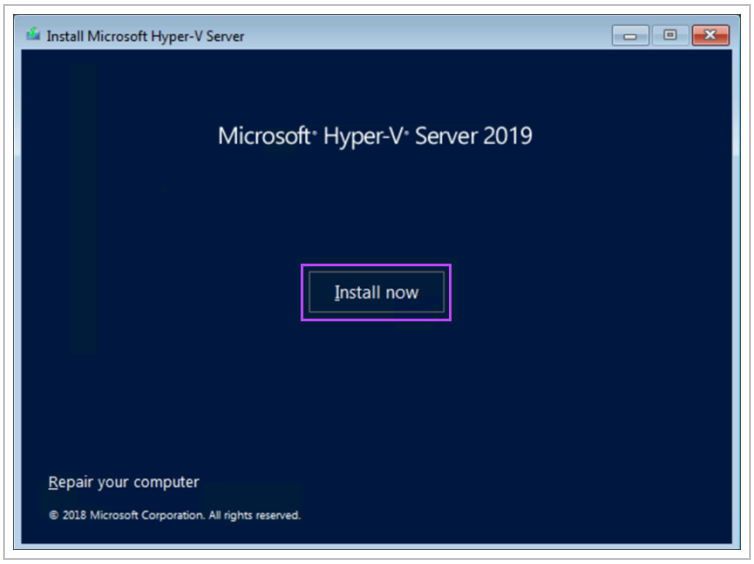
Configuration

Step 1: Install the Hyper-V Server

1. Open the Microsoft Evaluation Center
2. Download the **Hyper-V Server 2019** ISO
3. Create bootable media (e.g. USB drive)
4. Ensure the recovery machine will boot from the bootable media
5. Begin the installation of Hyper-V Server 2019
6. Select your preferred language, time and currency format and keyboard or input method, then click **Next**

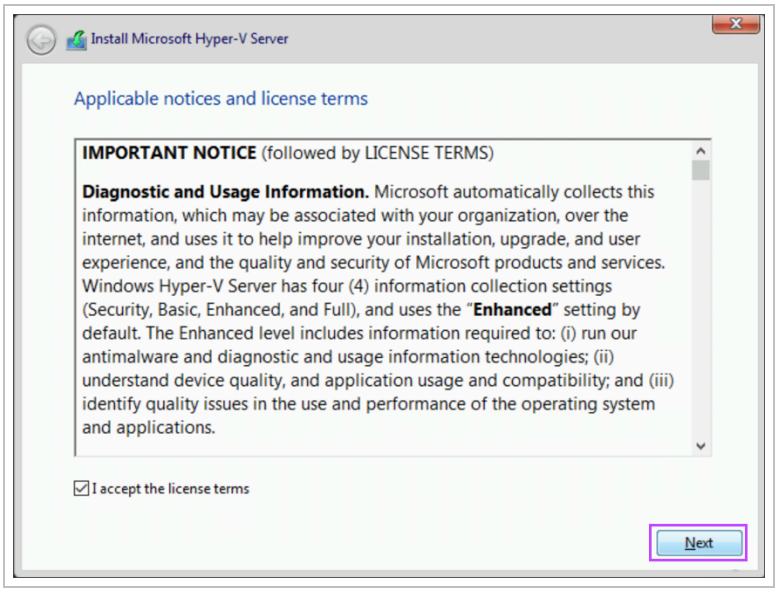


7. Click **Install Now**

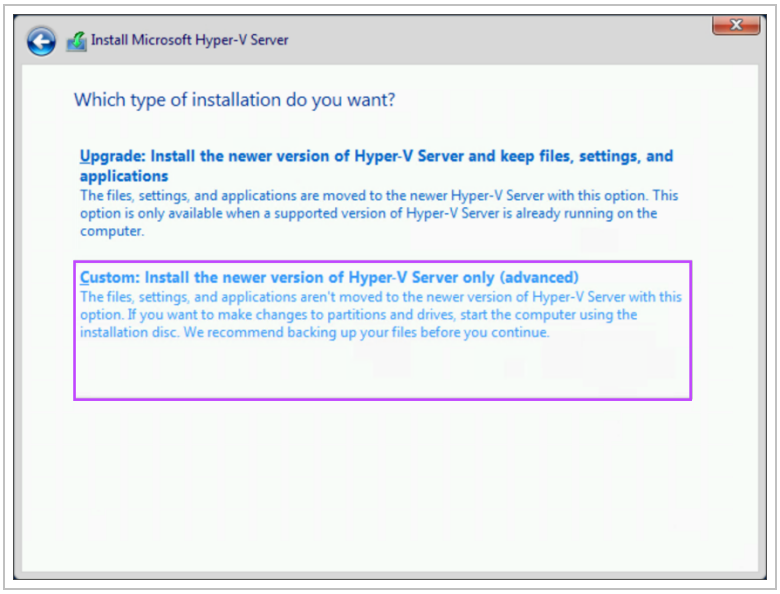


8. Accept the notices and license terms

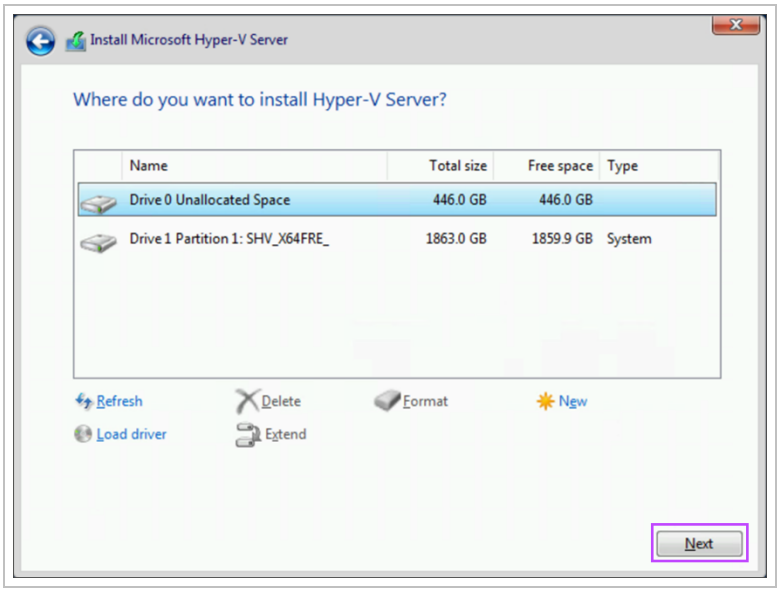
9. Click **Next**



10. On the Installation type screen, select **Custom**



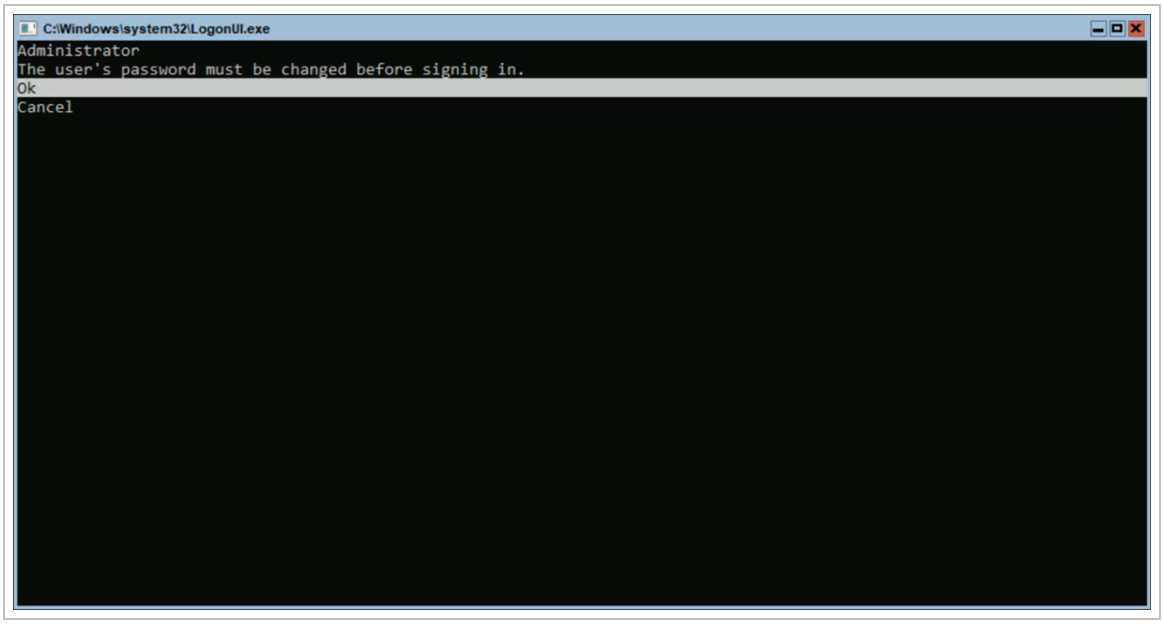
11. Select the drive you want top install the Hyper-V Server on



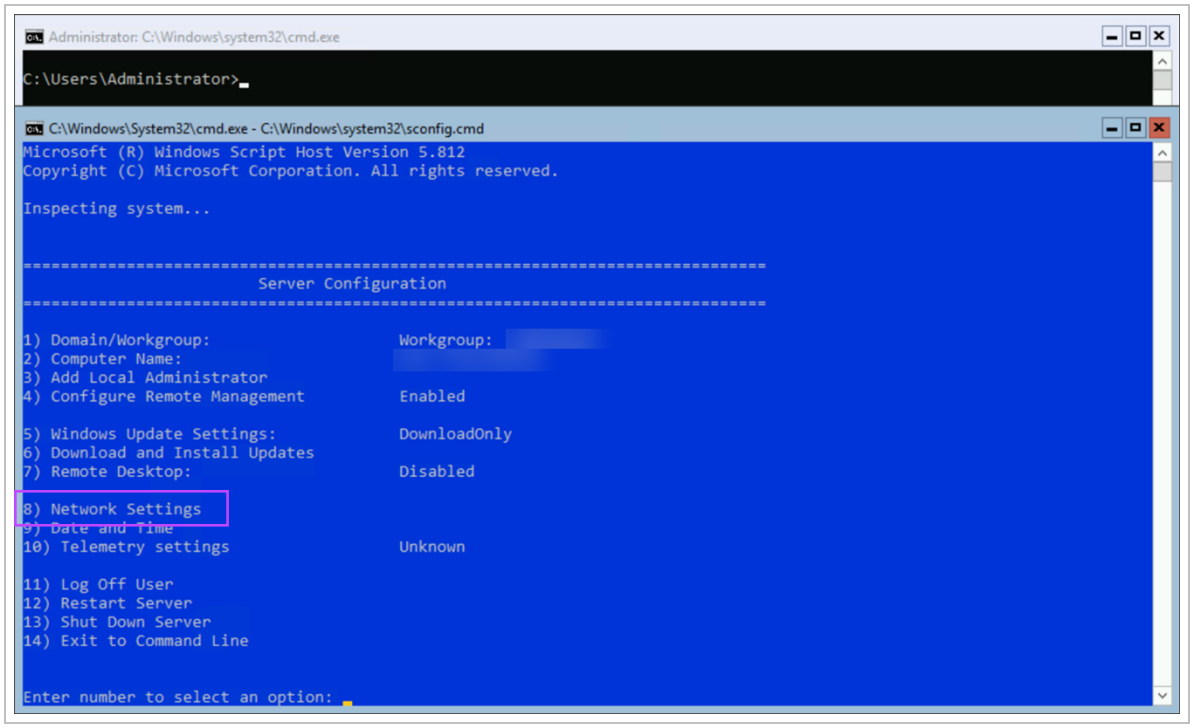
12. The installation will now run, the machine will restart to finalize the installation

Step 2: Configure the Hyper-V Server

1. When the machine boots after Hyper-V Server installation, follow the instructions on screen to set an Administrator Password

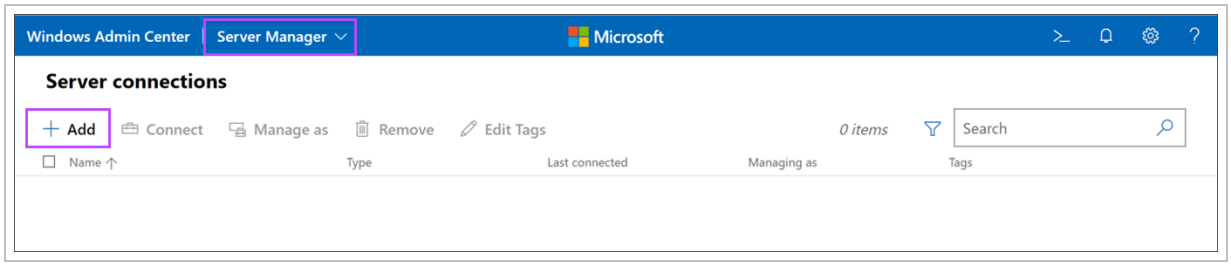


2. Ensure the Network Settings are configured correctly. These can be found under **option 8** of the Server Configuration



> Setup of the recovery service will **not** be successful without an internet connection

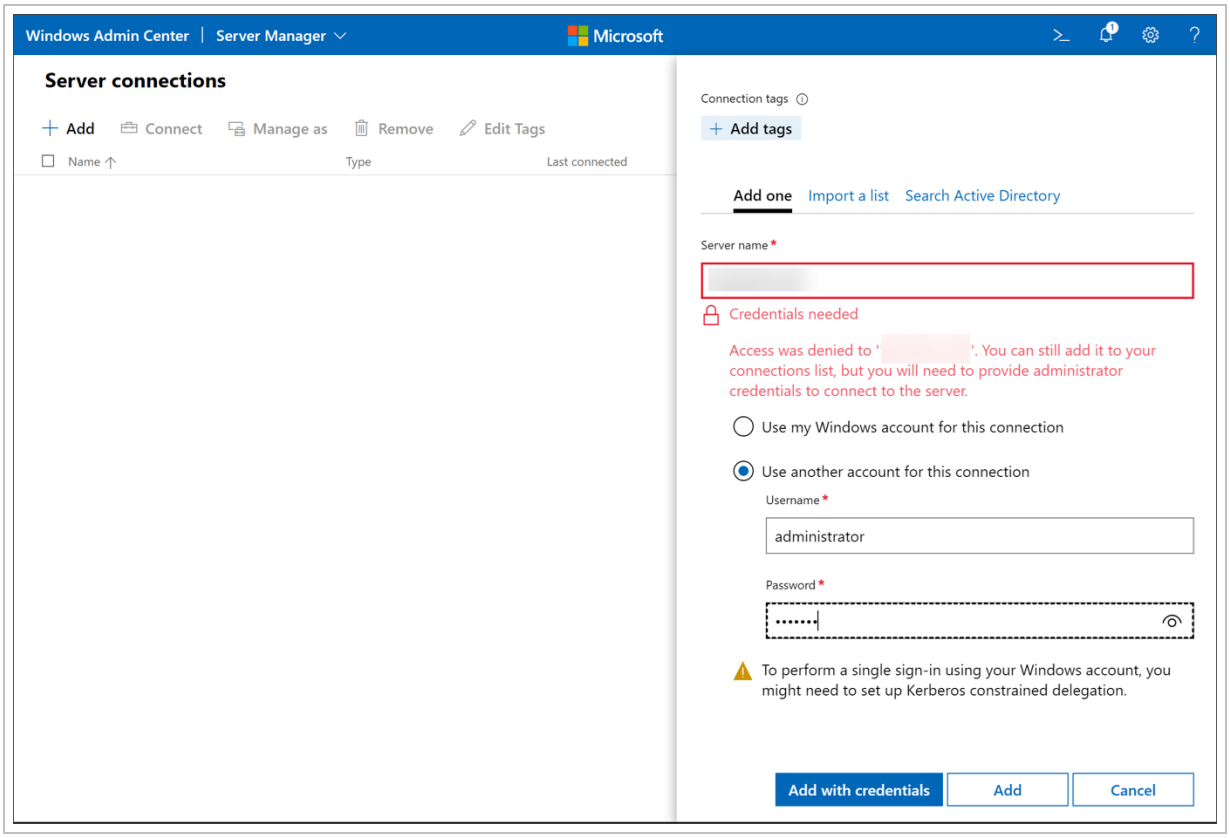
3. Use **option 14** to exit the command line once all configuration has been completed
4. Start the **Windows Admin Center** on the management machine
5. Navigate to **Server Manager** then into **Server Connections**
6. Click **Add** to add the Hyper-V Server



7. Enter the details of the Hyper-V server:
   - **Server Name:** Enter the IP address of the Hyper-V Server

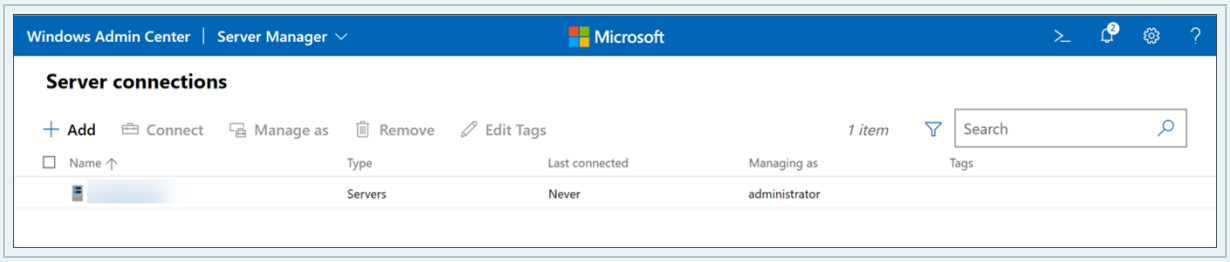
     > You will be required to provide access credentials to connect to the server, click **Use another account for this connection**

   - **Username:** Enter Administrator
   - **Password:** Enter the password configured in Step 2:1



8. Click **Add**

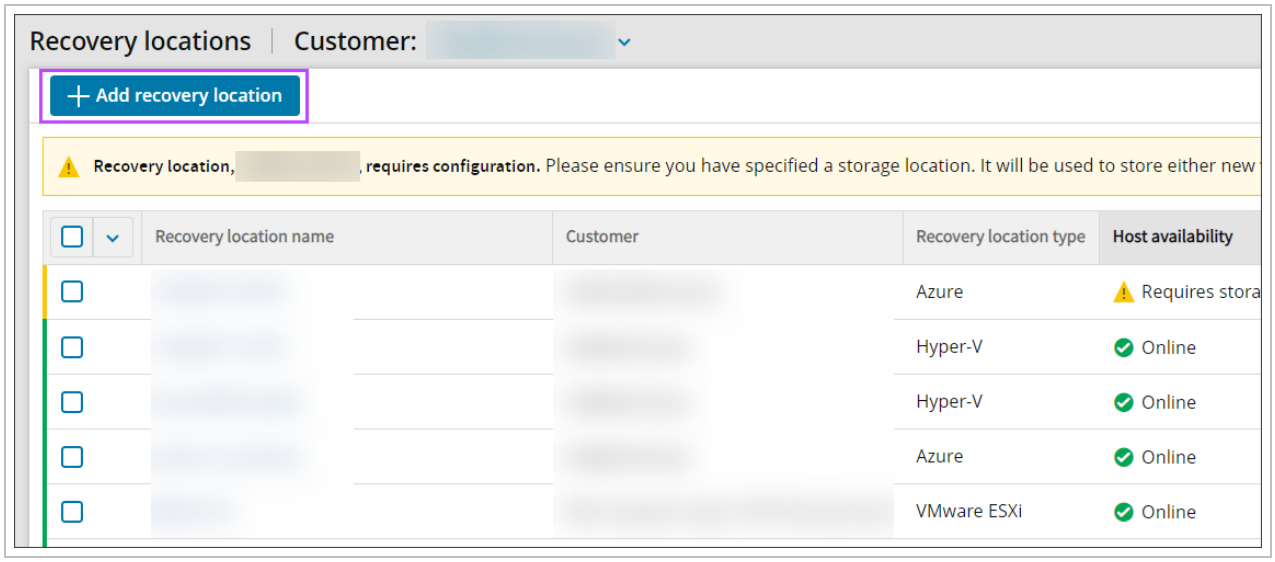
> Once added, the Hyper-V Server will be displayed in the list of connections



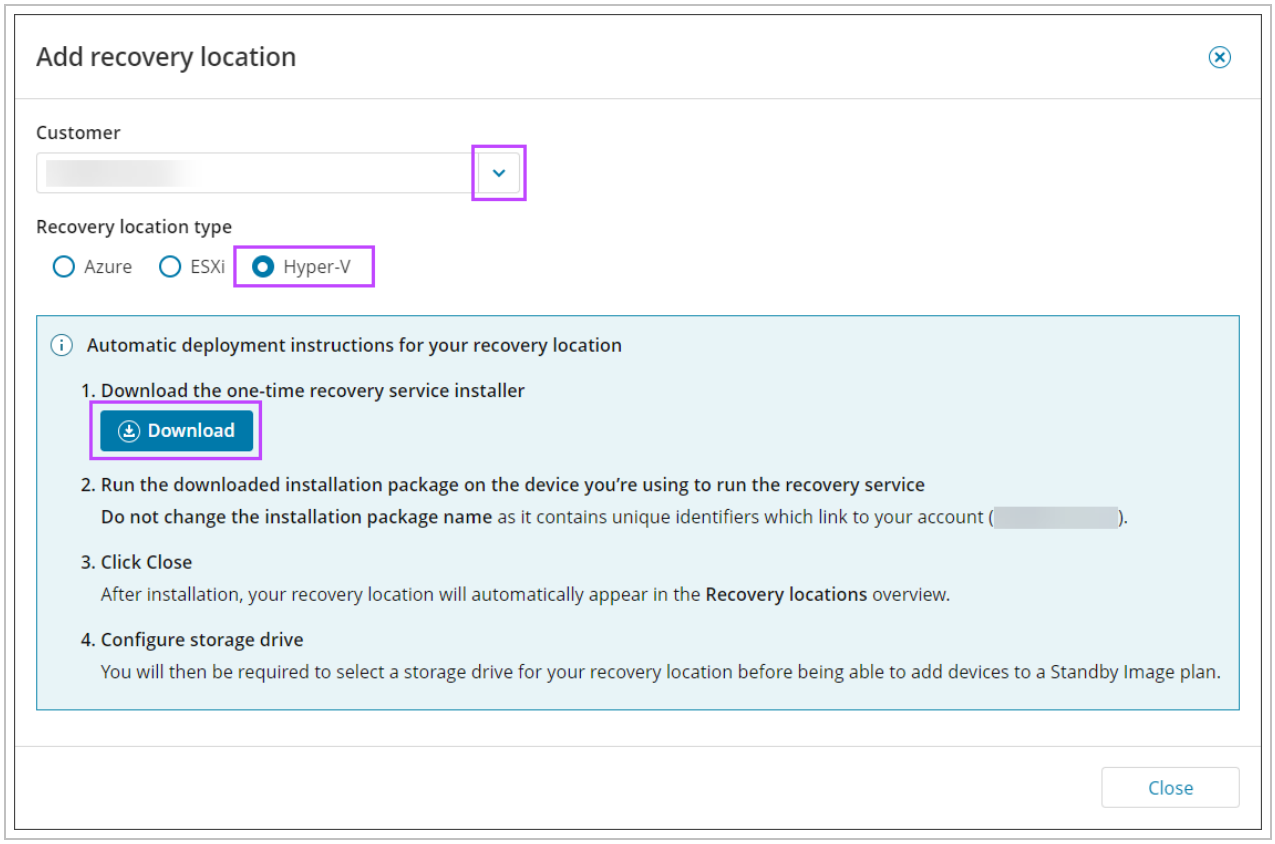
> You can view an overview of information related to the device by clicking the server name/IP address in the list.

Step 3: Download the Recovery Service

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Recovery** > **Recovery Locations**
3. Click **Add recovery location** at the top of the page



4. In the **Add Recovery Location wizard**, select the customer to attribute the recovery location to, from the dropdown



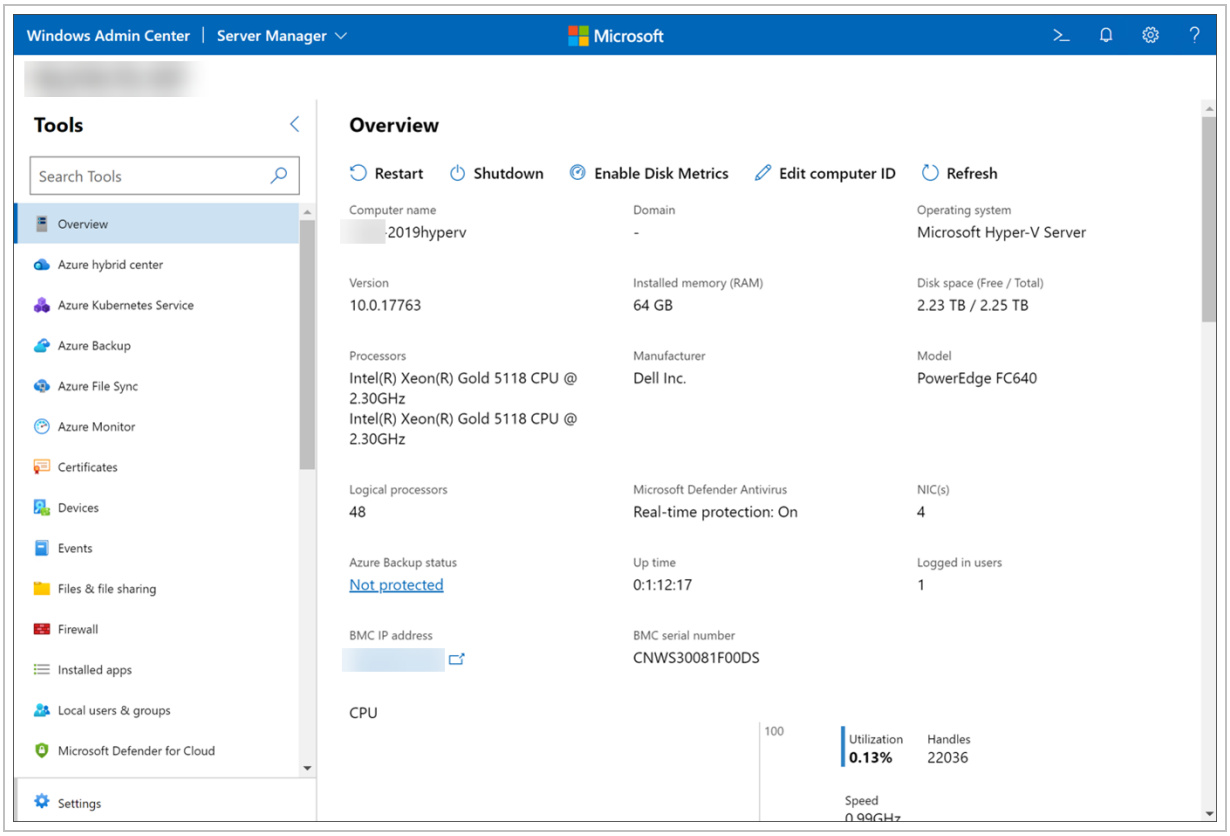
5. Download the recovery service installer and save it to your USB drive

> Do **not** change the installation package name. The installation package name contains unique identifiers to your account.
>
> This is a one-time installer and can only be used to install a single instance of the recover service. The installer will fail if you attempt to use the same package for another installation.

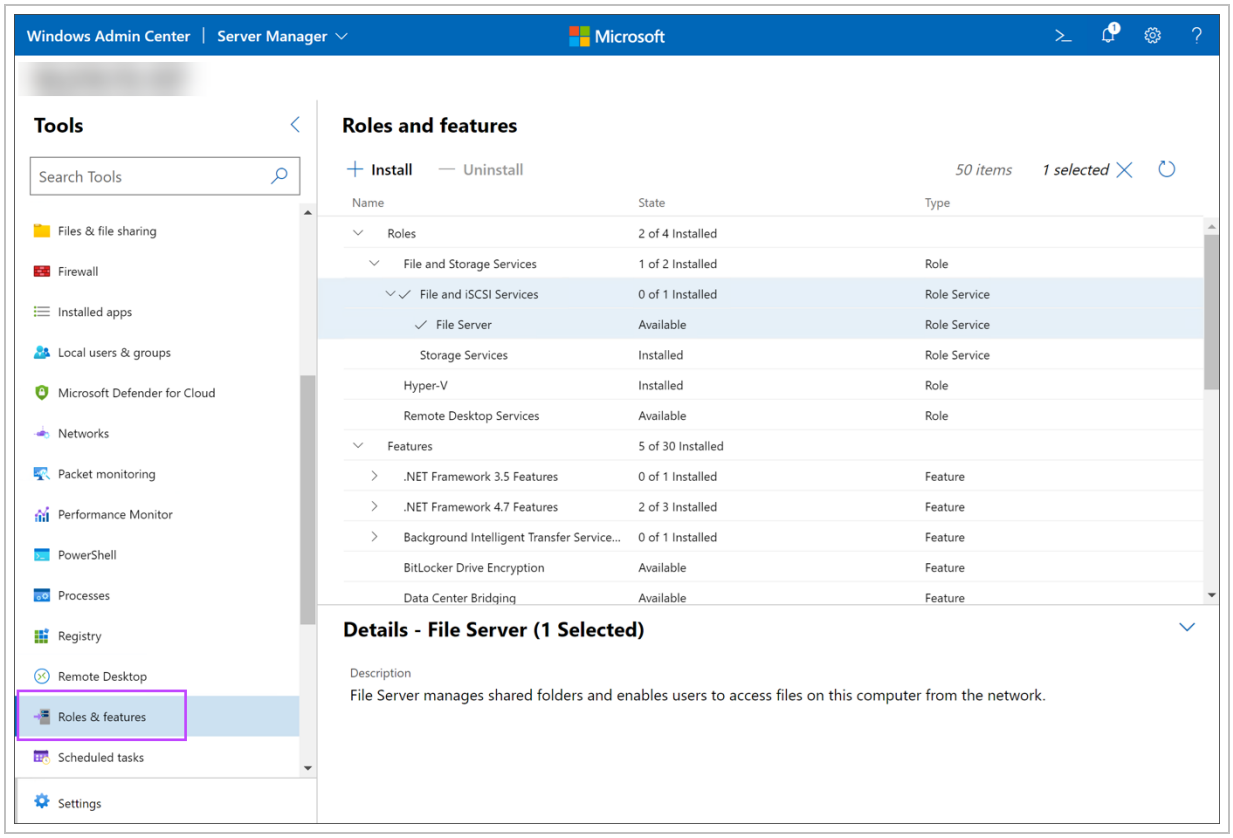
> Do **not** run the installer at this point, there are additional changes that are required first.

Step 4: Add a role for Hyper-V

1. Return to the **Windows Admin Center** on the management machine
2. Navigate to **Server Manager** then into **Server Connections**
3. Open the overview the Hyper-V server from the list of connections by clicking the server name/IP address in the list

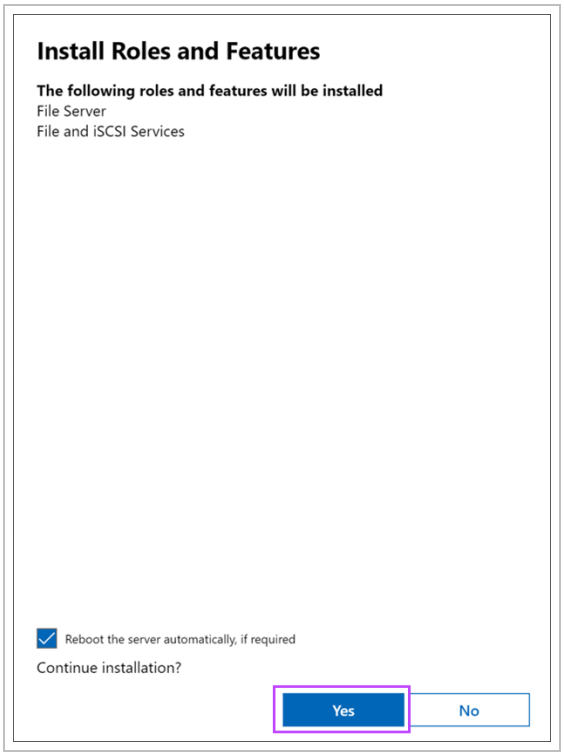


4. In the left-hand **Tools** menu, select **Roles and features**



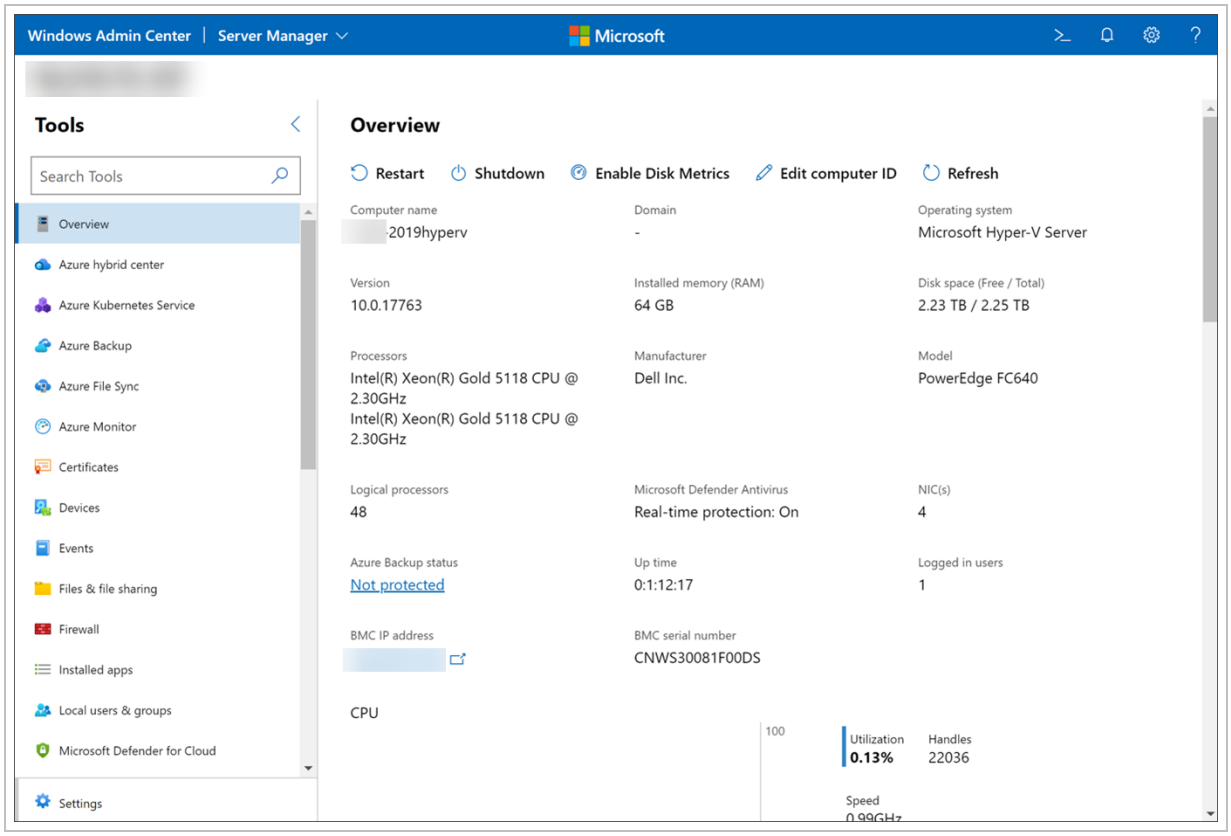
5. Expand **Roles > Files and Storage Services**, select **File abd iSCSI Services**
6. Click **Install**

7. Confirm role installation



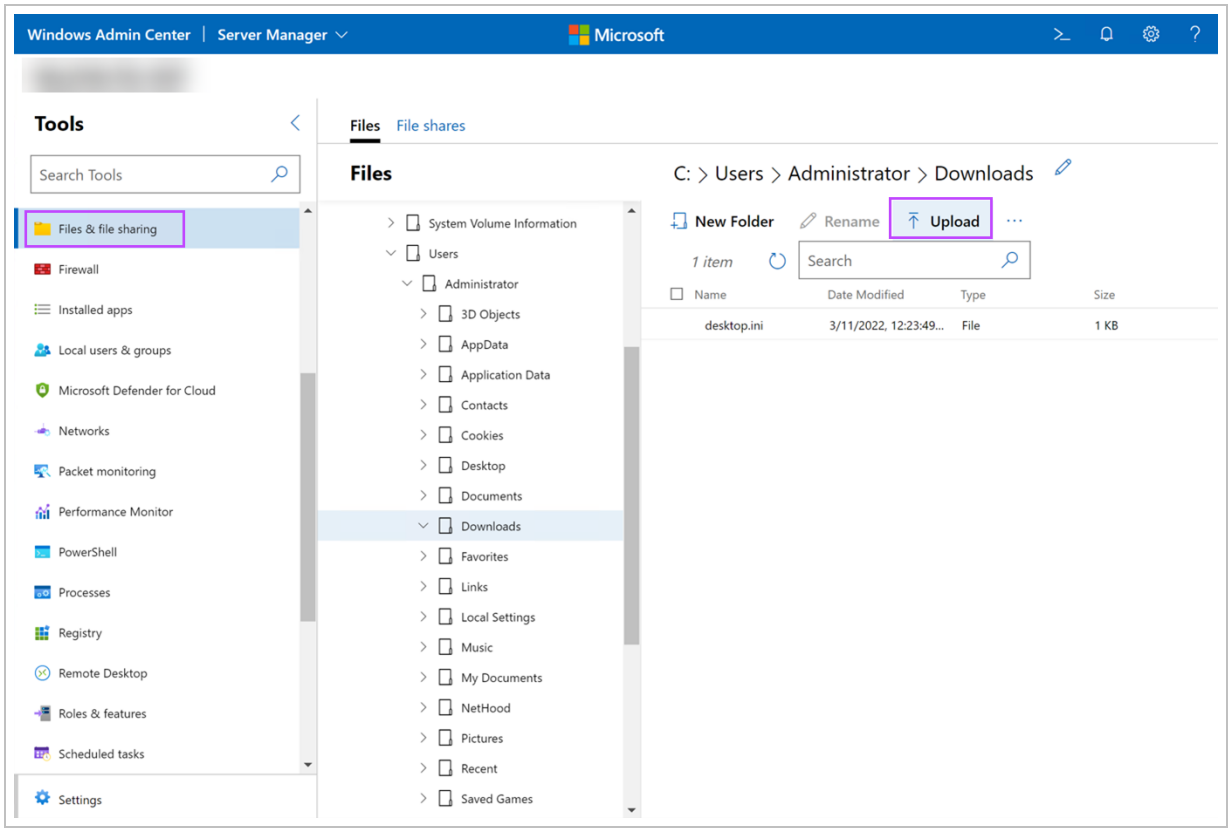
Step 5: Install and Configure the Recovery Location

1. In the **Windows Admin Center**, navigate to **Server Manager** then into **Server Connections**
2. Open the overview the Hyper-V server from the list of connections by clicking the server name/IP address in the list



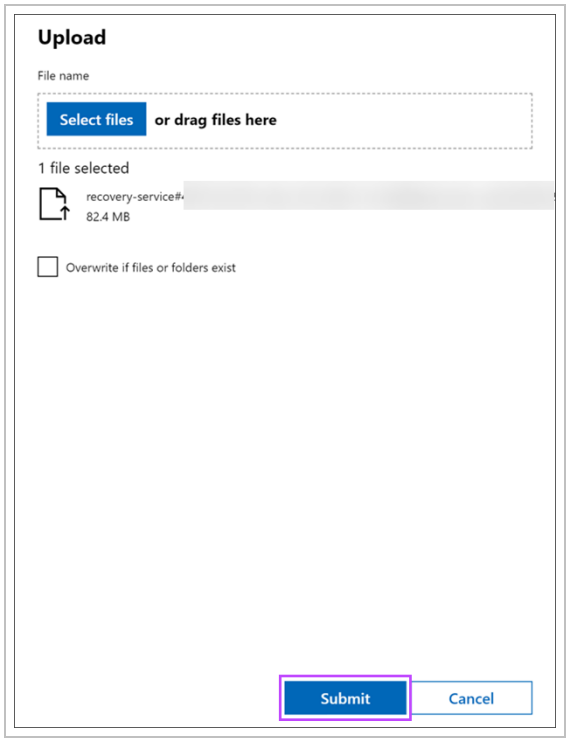
3. In the left-hand **Tools** menu, select **Files & file sharing**

4. Using the file structure, browse to the folder you want to upload the Recovery Location's recovery service installer to on the Hyper-V Server



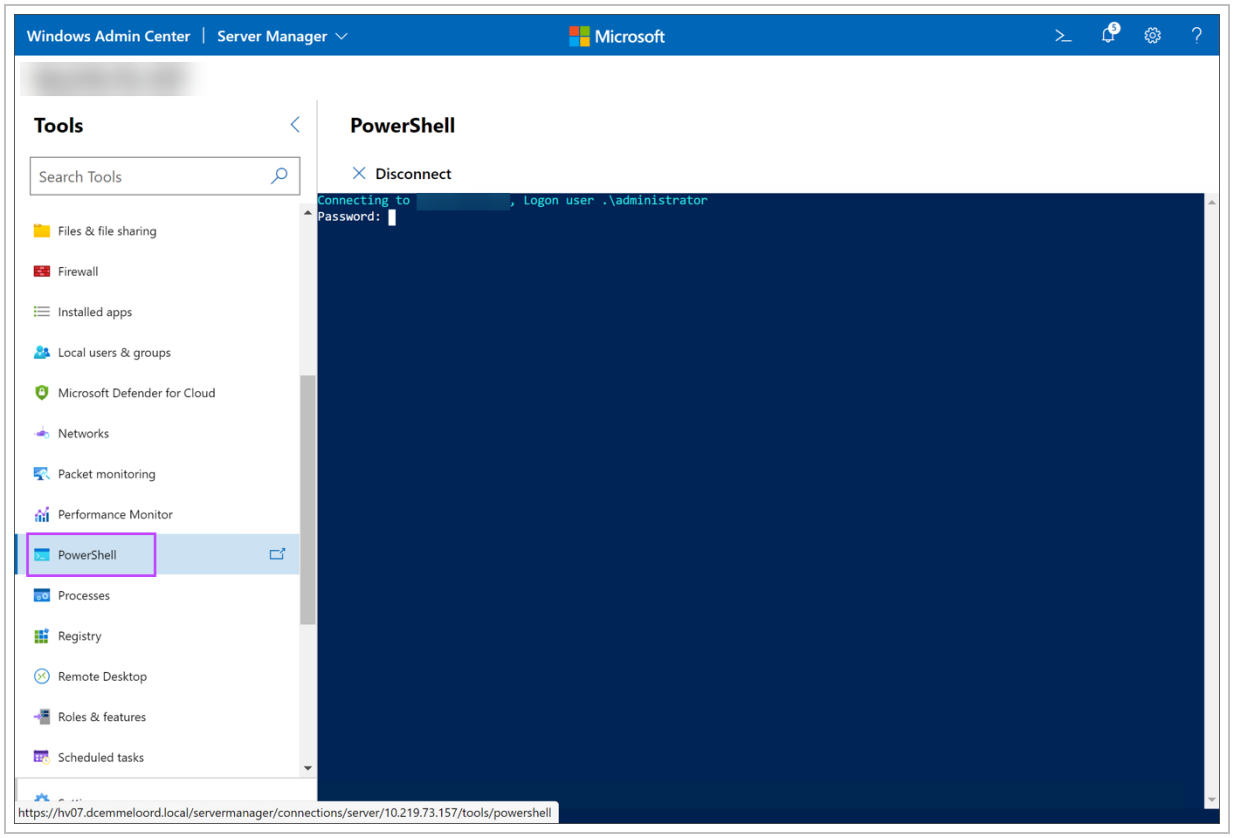
5. Click **Upload**
6. Browse to the downloaded installer file from Step 3:5 and click **Open** to begin the upload to the Hyper-V server

7. Once the file appears in the upload window, click **Submit**



8. Once the upload completes, select **PowerShell** from the left-hand **Tools** menu

9. Login using the **Administrator** credentials



10. Browse to the directory selected in the upload in Step 5:4 using the `cd` command
11. Enter the installer filename

> You can enter `.\re` and press **TAB**, this will populate the full name automatically, so long as no other file in this location begins with `re`

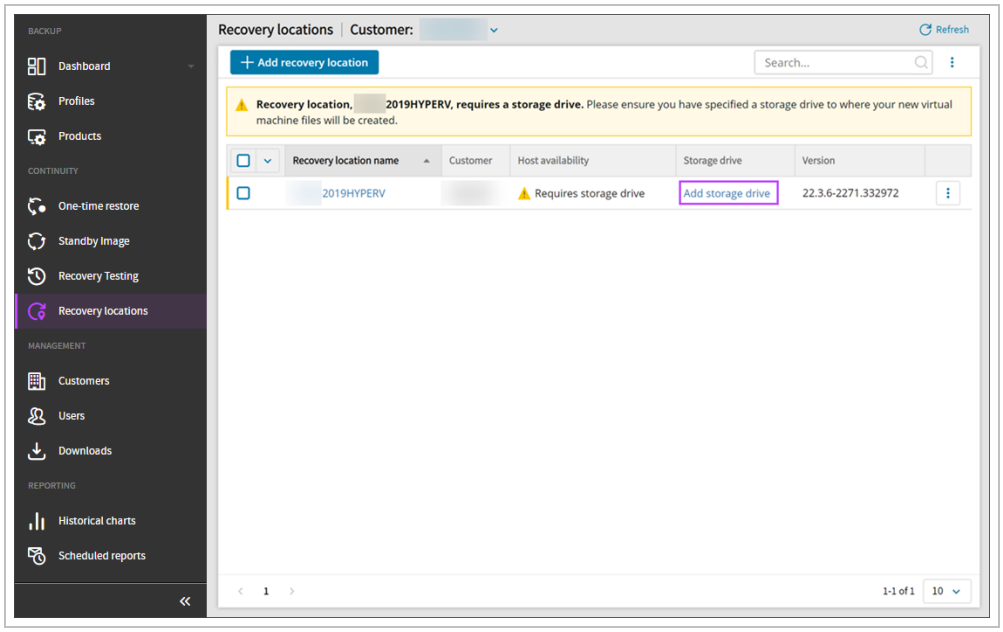
12. Make sure to add `/S` (case sensitive) after the installer filename, or the installation will not complete
13. Press **Enter**

> Once the execution of the installer has been confirmed, PowerShell will return to the standard prompt (`PS C:\Users\Administrator\Downloads>`).

> Depending on the performance of the machine, this can take between a few seconds and a few minutes. Do not try to speed up the process by hitting enter multiple times or closing out of the PowerShell.

14. Exit the PowerShell and navigate to **Installed Apps** in the left-hand **Tools** menu. **Recovery Service** will be listed in the Installed Apps page
15. Log in to the Management Console under a **SuperUser** account

16. Navigate to **Recovery** > **Recovery Locations**. The new Recovery Location will now be displayed in the list of locations under the customer selected in Step 3:4
17. Enter the storage drive to assign where the Standby Images are going to be restored to by clicking **Add storage drive** and entering the drive location. E.g. `D:\`



18. You can now add devices using the Standby Image plan using this Recovery Location

Manage Recovery Locations

> Permissions to modify storage locations to a Network Share are available for Reseller level and lower, for SuperUsers with Security Officer permissions *only*.

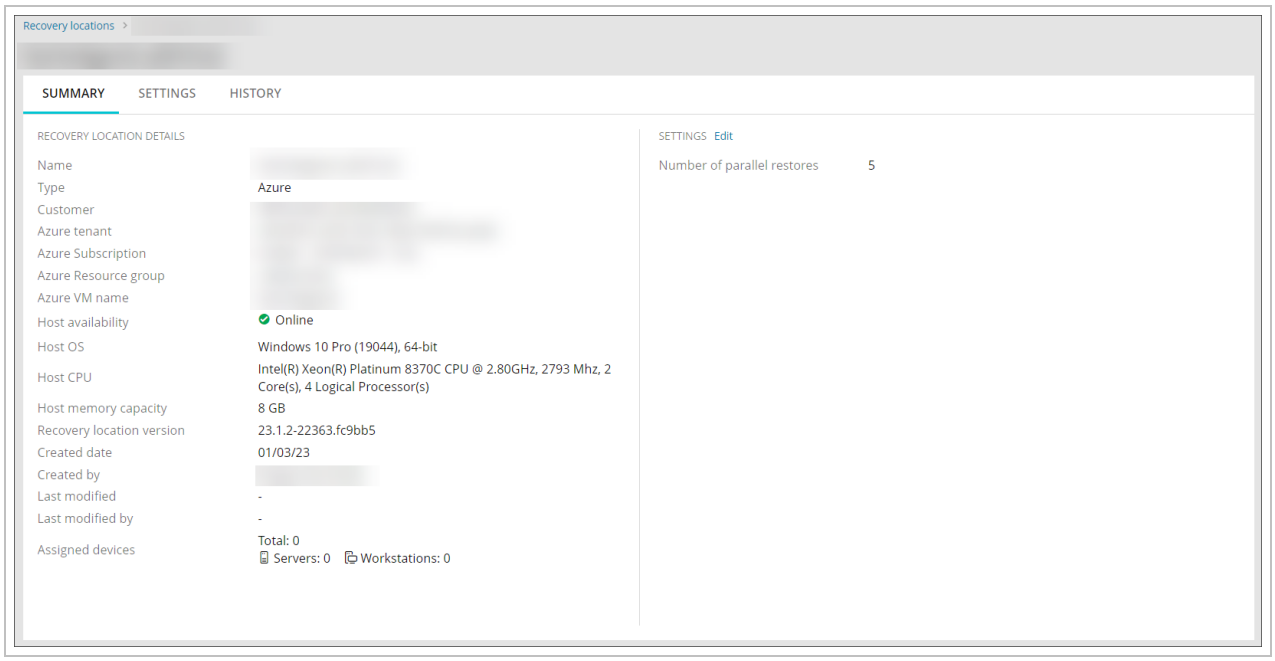
View Recovery Location Summary

A summary of information relating to each Recovery Location can be viewed one at a time from the **Continuity** > **Recovery Locations** page using one of four methods for both Self-hosted (for Standby Image) and Azure location types.

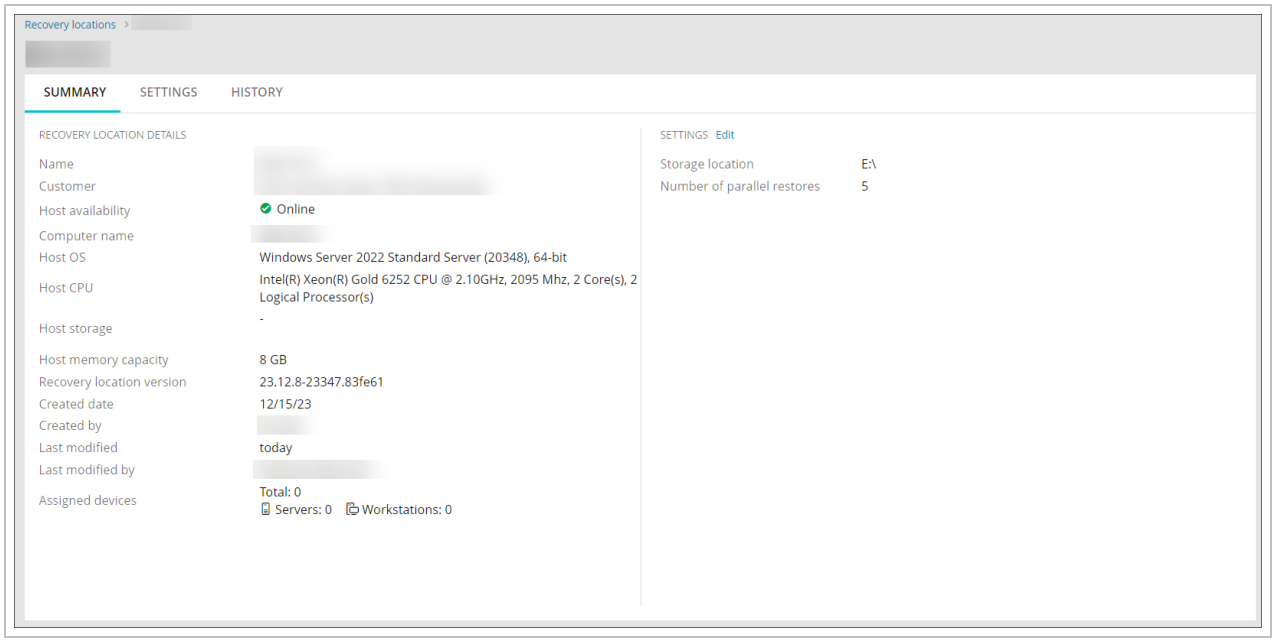
1. Recovery Location name
   a. Select the recovery location name to open the Summary page
2. Top bar menu
   a. Select the checkbox for the Recovery Location
   b. At the top of the Recovery Locations page, select **Edit**
   c. Switch to the **Summary** tab
3. Location context menu
   a. Right-click on the Recovery Location to edit
   b. Select **Edit**
   c. Switch to the **Summary** tab

4. Right hand menu
    a. Click the action menu for the Recovery Location, seen as three dots in a vertical line to the right of the location's version
    b. Select **Edit**
    c. Switch to the **Summary** tab

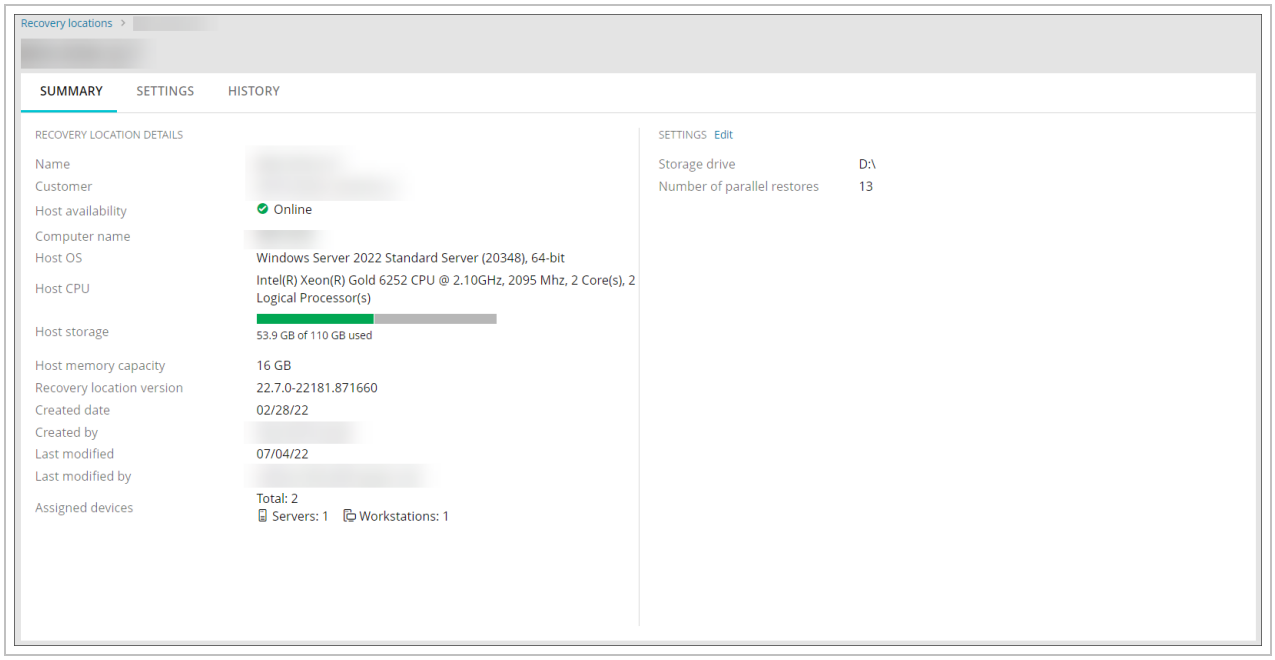
Azure:



ESXi:



Hyper-V:

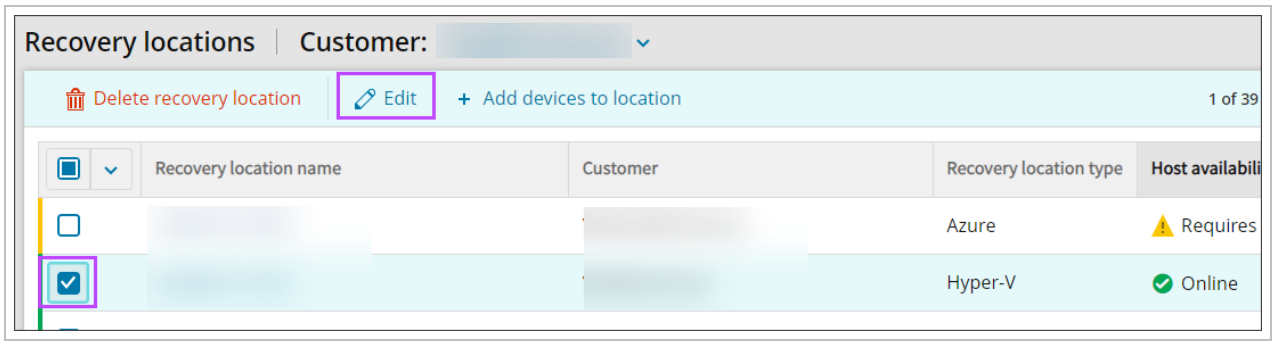


Edit Recovery Location

Recovery Locations can be edited one at a time from the **Continuity** > **Recovery Locations** page using one of four methods for Azure, ESXi and Hyper-V location types.

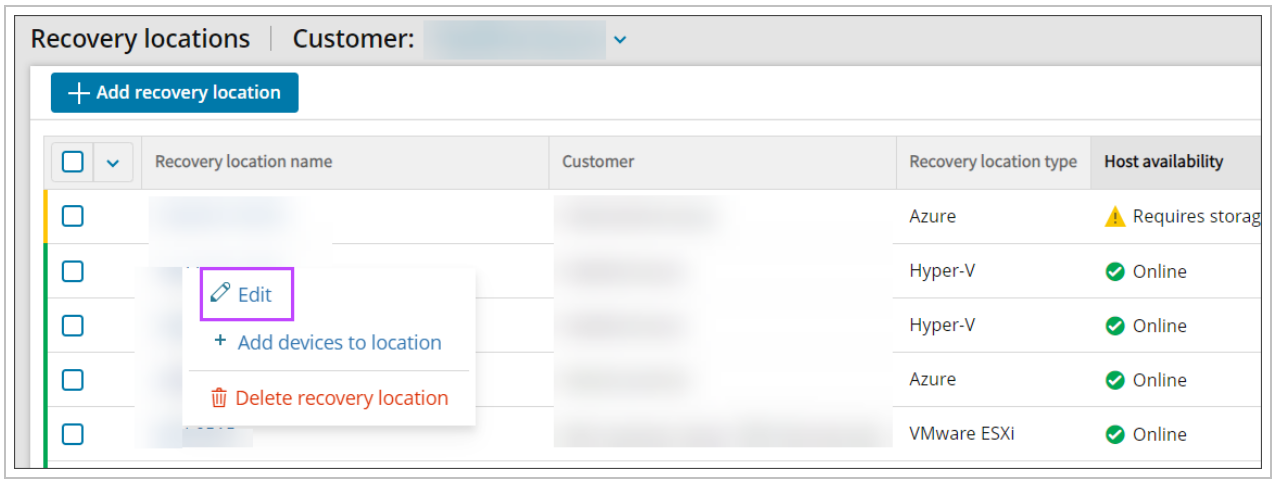
1. Recovery Location name
    a. Select the recovery location name to open the Summary page
    b. Switch to the **Settings** tab
    c. Make any required changes to the following aspects of the recovery location:
        - **Customer** - change the customer the storage location belongs to
        - **Recovery Location Name** - change the name of the machine or server used to store your device restores
        - **Max number of parallel restores** - manage the workload on the recovery machine by limiting the number of concurrent restores that can take place
        - **Storage Location** - set the recovery location to the appropriate type
            - **Local Drive** - The local path to the folder where your virtual machine files will be stored. This can be either a location at a drive, Cluster Shared Volume, or the drive itself. Examples:
                - C:\Virtual_Machines
                - D:\
            - **Network Share**(available only for Hyper-V and ESXi) - Only available if all devices assigned to this recovery location are being restored to Local VHDX / Local VMDK files, remove any devices restoring to Hyper-V or ESXi on the recovery location to use Network Share
                - Network path / IP address
                - Username
                - Password
        - **Server Connections** (Available only for ESXi) - see Step 5: Add Storage Location and Server Connections for instructions on connecting to the vCenter or ESXi Server
    d. Click **Save**

2. Top bar menu
   a. Select the checkbox for the Recovery Location to edit
   b. At the top of the Recovery Locations page, select **Edit**



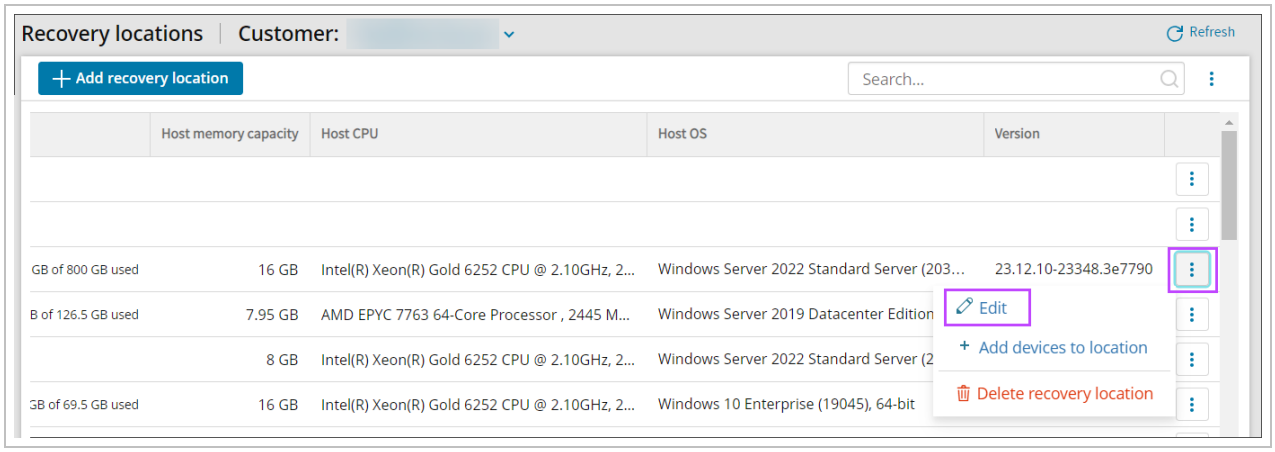
   c. Make any required changes to the following aspects of the recovery location:
      - **Customer** - change the customer the storage location belongs to
      - **Recovery Location Name** - change the name of the machine or server used to store your device restores
      - **Max number of parallel restores** - manage the workload on the recovery machine by limiting the number of concurrent restores that can take place
      - **Storage Location** - set the recovery location to the appropriate type
        - **Local Drive** - The local path to the folder where your virtual machine files will be stored. This can be either a location at a drive, Cluster Shared Volume, or the drive itself. Examples:
          - C:\Virtual_Machines
          - D:\
        - **Network Share**(available only for Hyper-V and ESXi) - Only available if all devices assigned to this recovery location are being restored to Local VHDX / Local VMDK files, remove any devices restoring to Hyper-V or ESXi on the recovery location to use Network Share
          - Network path / IP address
          - Username
          - Password
      - **Server Connections** (Available only for ESXi) - see Step 5: Add Storage Location and Server Connections for instructions on connecting to the vCenter or ESXi Server
   d. Click **Save**

3. Location context menu
   a. Right-click on the Recovery Location to edit
   b. Select **Edit**



   c. Make any required changes to the following aspects of the recovery location:
      - **Customer** - change the customer the storage location belongs to
      - **Recovery Location Name** - change the name of the machine or server used to store your device restores
      - **Max number of parallel restores** - manage the workload on the recovery machine by limiting the number of concurrent restores that can take place
      - **Storage Location** - set the recovery location to the appropriate type
        - **Local Drive** - The local path to the folder where your virtual machine files will be stored. This can be either a location at a drive, Cluster Shared Volume, or the drive itself. Examples:
          - C:\Virtual_Machines
          - D:\
        - **Network Share**(available only for Hyper-V and ESXi) - Only available if all devices assigned to this recovery location are being restored to Local VHDX / Local VMDK files, remove any devices restoring to Hyper-V or ESXi on the recovery location to use Network Share
          - Network path / IP address
          - Username
          - Password
      - **Server Connections** (Available only for ESXi) - see Step 5: Add Storage Location and Server Connections for instructions on connecting to the vCenter or ESXi Server
   d. Click **Save**

4. Right hand menu
   a. Click the action menu for the Recovery Location, seen as three dots in a vertical line to the right of the location's version
   b. Select **Edit**

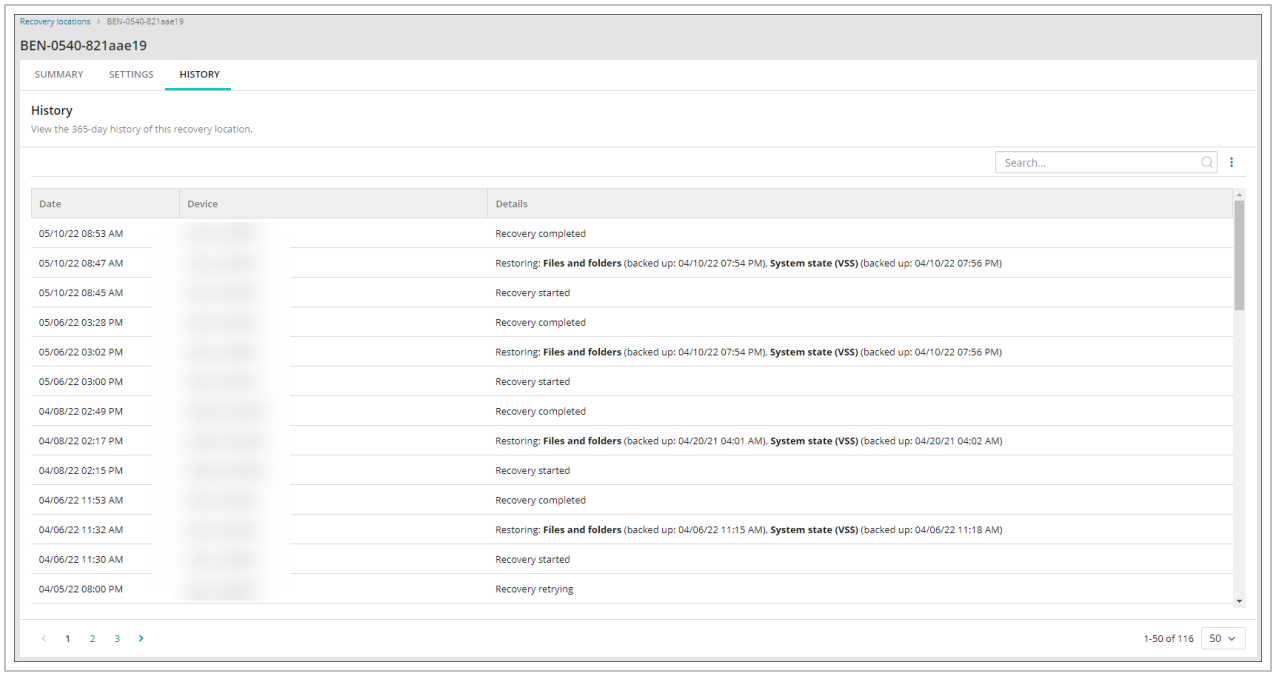


   c. Make any required changes to the following aspects of the recovery location:
      - **Customer** - change the customer the storage location belongs to
      - **Recovery Location Name** - change the name of the machine or server used to store your device restores
      - **Max number of parallel restores** - manage the workload on the recovery machine by limiting the number of concurrent restores that can take place
      - **Storage Location** - set the recovery location to the appropriate type
        - **Local Drive** - The local path to the folder where your virtual machine files will be stored. This can be either a location at a drive, Cluster Shared Volume, or the drive itself. Examples:
          - C:\Virtual_Machines
          - D:\
        - **Network Share**(available only for Hyper-V and ESXi) - Only available if all devices assigned to this recovery location are being restored to Local VHDX / Local VMDK files, remove any devices restoring to Hyper-V or ESXi on the recovery location to use Network Share
          - Network path / IP address
          - Username
          - Password
      - **Server Connections** (Available only for ESXi) - see Step 5: Add Storage Location and Server Connections for instructions on connecting to the vCenter or ESXi Server
   d. Click **Save**

View and Search Recovery Location History

A history of restores relating to each Recovery Location can be viewed one at a time from the History tab when looking from **Continuity** > **Recovery Locations**.

1. Open the Recovery Location by clicking the Recovery Location name
2. Switch to the **History** Tab



3. Using the search bar, it is possible to search by the content in the **Device** column

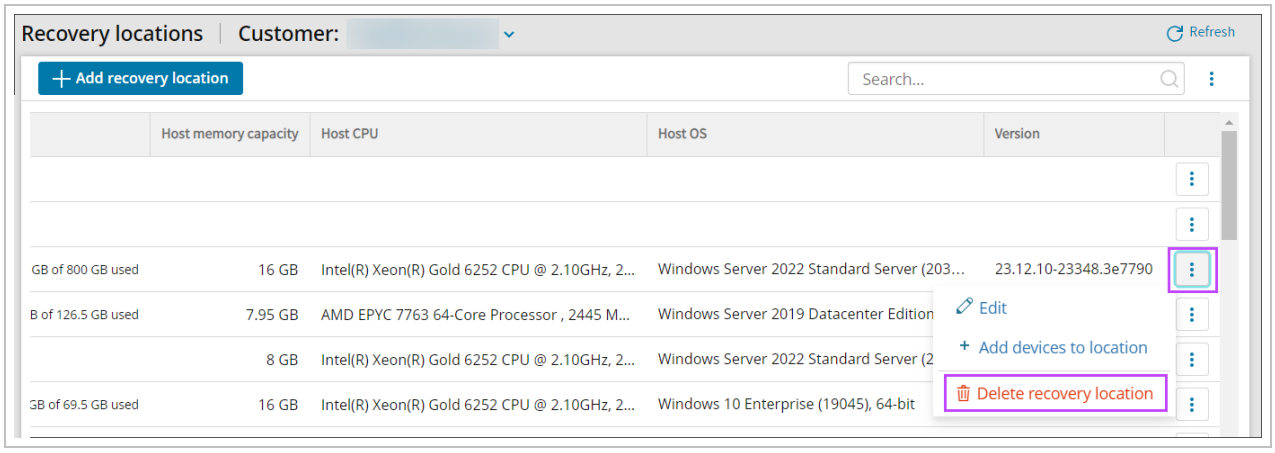
Delete Recovery Location

> Deleting a recovery location will **uninstall** the recovery service and all devices which were using the deleted recovery location will be **unassigned** from the Standby Image plan.

To delete a single recovery location:

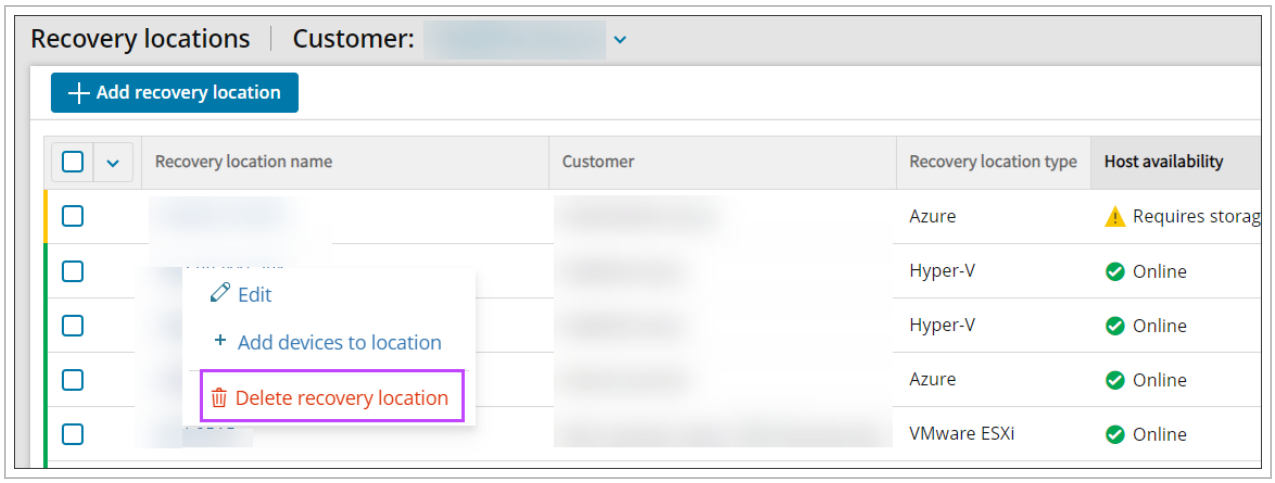
1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Click the action menu for the Recovery Location, seen as three dots in a vertical line to the right of the location's version, or right-click the recovery location to view the context menu

4. Select **Delete recovery location**



Or,

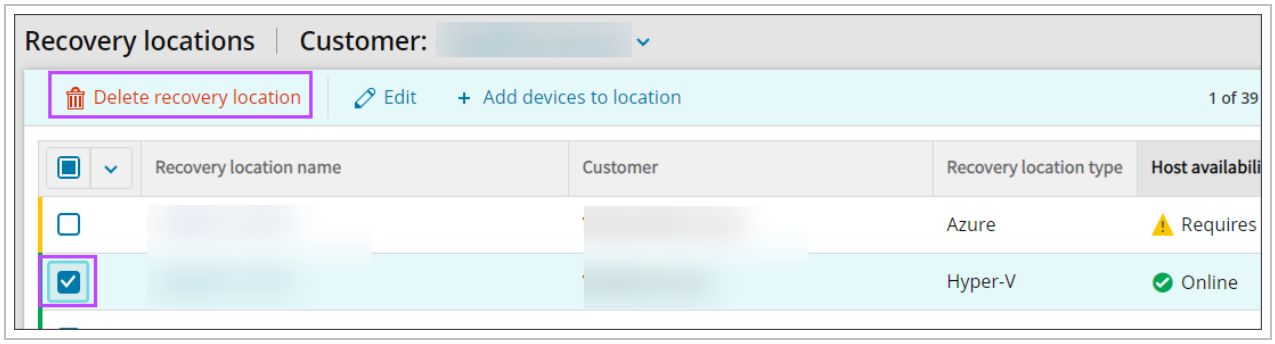
1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Right-click on the Recovery Location to remove
4. Select **Delete recovery location**



Or to delete single or multiple recovery locations:

1. Log in to the Management Console under a **SuperUser** account
2. Navigate to **Continuity** > **Recovery Locations**
3. Select the checkboxes of any locations you wish to delete

4. At the top of the page click **Delete recovery location**



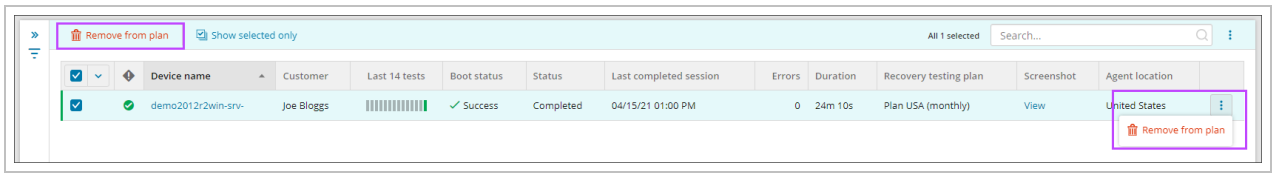
> Deleting a Recovery Location does **not** delete previously stored data. This restored data is kept on the device until manually deleted by the user.

Disabling Recovery Services

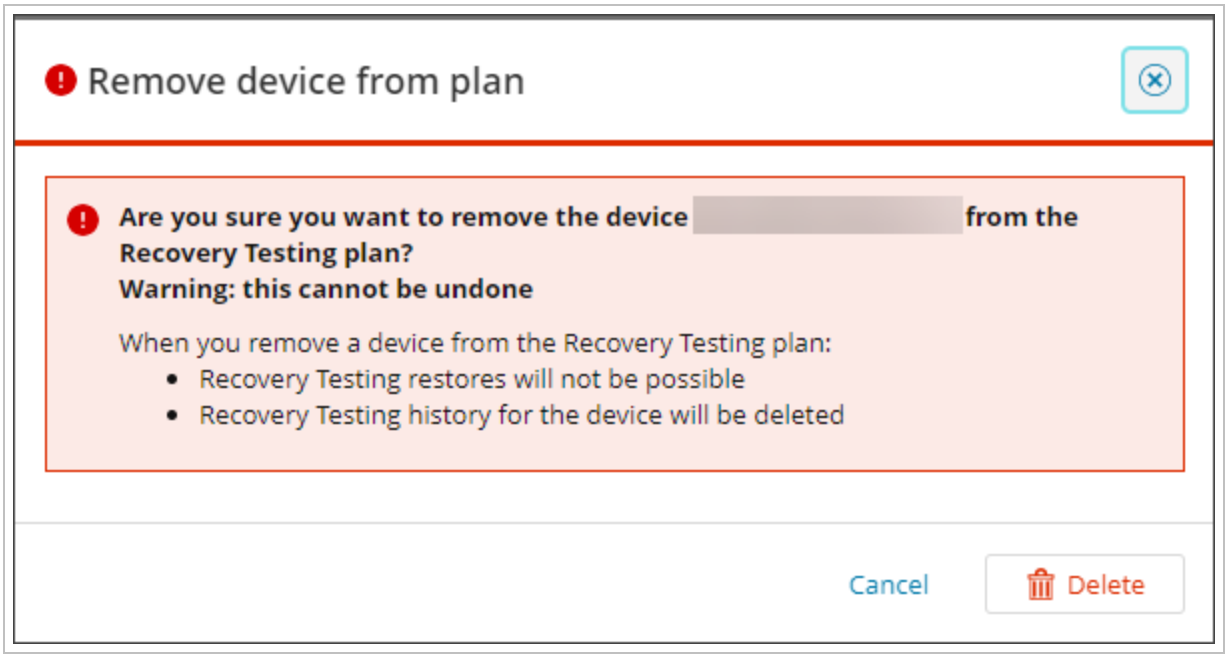
> Removing a plan does not affect previously restored data.

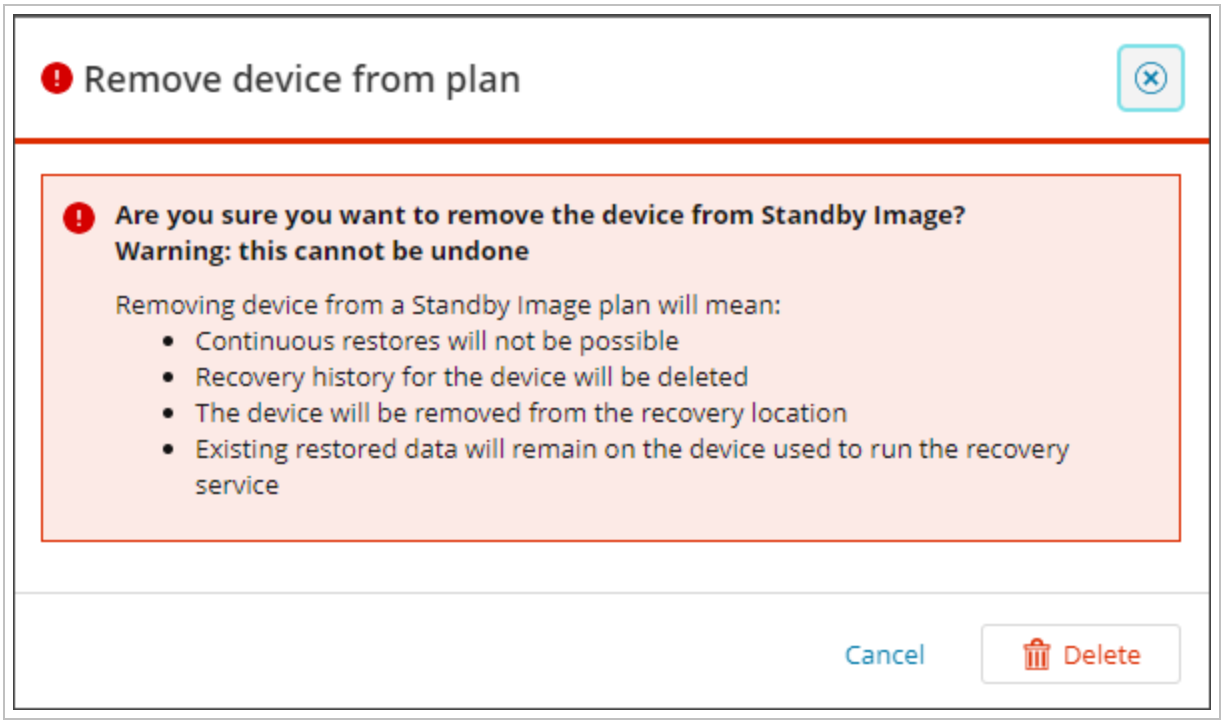
Removing devices from Recovery Testing or Standby plans can be done from the dedicated Recovery Testing and Standby Image Overviews by following the below steps:

1. Log in to the Management Console under a **SuperUser** or **Manager** account
2. Navigate to **Continuity** > **Recovery Testing/Standby Image**
3. Select the device(s) you wish to remove the plan from using the checkboxes to the left of the device name, right clicking the device name or use the three dots to the far right of the screen to open the action menu
4. Select **Remove from plan**



5. Confirm your intention to remove the device from the recovery plan by clicking **Delete**





Recovery Console Guide

The Recovery Console is used for **virtual-to-virtual** and **physical-to-virtual** recoveries of Windows servers and workstations. It is a multi-instance recovery tool that enables you to set up **proactive data recovery** from servers and workstations to any location. It can be used to perform an on-demand or continuous restore straight into Hyper-V or VMware hypervisor, or to a .vhdx/.vmdk image file format.

The Recovery Console lets you recover data belonging to the following data sources:

- Files and Folders
- System State (through virtual disaster recovery)
- Microsoft Exchange
- Hyper-V
- VMware
- Microsoft SQL
- Network shares

Critical Restore? We're not the judge of when a recovery is especially time critical–you are.

Critical Restore is our partner-driven fast escalation process. Just let us know on your initial support call, email, or chat message that a specific recovery is especially time sensitive, and we'll bring all hands on deck immediately to help you get your customer back up and running ASAP.

For more details please see the Critical Restore FAQ's.

Recovery Console installation

Requirements

Recovery Console is available for Windows OS's only. You can install it on the following operating systems:

- Windows 8 / 8.1
- Windows 10
- Windows 11
- Windows Server 2012 / 2012 R2 (limited[1])
- Windows Server 2016 (limited[2])
- Windows Server 2019 (limited[3])
- Windows Server 2022 (limited[4])

Exclusions

Add the following to the exclusions list of your Antivirus software to ensure there are no restrictions on the Recovery Console:

Before adding any of the below to your Antivirus software, we recommend confirming whether the files exist in `C:\Program Files\` or `C:\Program Files (X86)\` and adjusting the paths as required

- `C:\Program Files\RecoveryConsole`
- `C:\Program Files\RecoveryConsole\BackupFP.exe`

---

[1]New features such as Docker-based containers, Storage Spaces Direct and Shielded VMs are not.
[2]Only the features compatible with Windows Server 2012 R2 are supported.
[3]Only the features compatible with Windows Server 2012 R2 are supported.
[4]Only the features compatible with Windows Server 2012 R2 are supported.

- `C:\Program Files\RecoveryConsole\BackupIP.exe`
- `C:\Program Files\RecoveryConsole\BackupUP.exe`
- `C:\Program Files\RecoveryConsole\RecoveryConsole.exe`
- `C:\Program Files\RecoveryConsole\ProcessController.exe`
- `C:\Program Files\RecoveryConsole\ClientTool.exe`
- `C:\Program Files\RecoveryConsole\vddk`

Instructions

1. Download an installer for your system (32- or 64-bit)

   > This can be found from the Downloads page in Management Console, or from the Backup Downloads page on our website.

2. Start the installer

3. Change the default installation folder if needed
4. Click **Install** to start the installation
5. When the installation process is completed, click **Finish**

   > The Recovery Console will automatically open once the installation completes

Starting and quitting Recovery Console

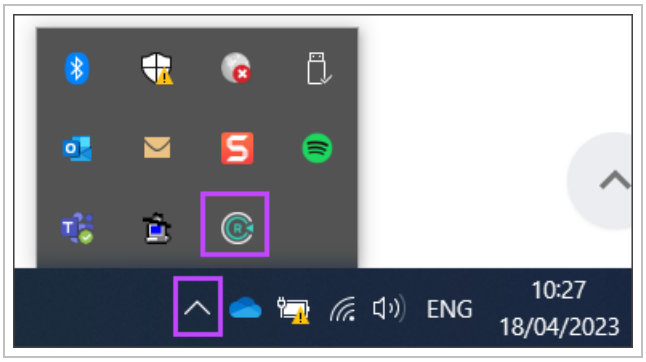
The Recovery Console starts automatically after you complete the installation (unless you uncheck the **Run Recovery Console** option at the final step of the installation wizard). You can start it manually at any time using the Windows **Start** menu.

When you click the **Close** icon it the upper-right corner, the application gets minimized to the notification area, but active recovery sessions will still be processed.

How to Quit

> This will stop all active recovery sessions

1. In the notification area, open the taskbar. Right-click on the Recovery Console icon



2. Choose **Quit** from the menu that opens
3. Confirm your intention to quit the app

> Please note, the windows account must be a computer admin to open Recovery Console

Stop Recovery Console Opening Automatically

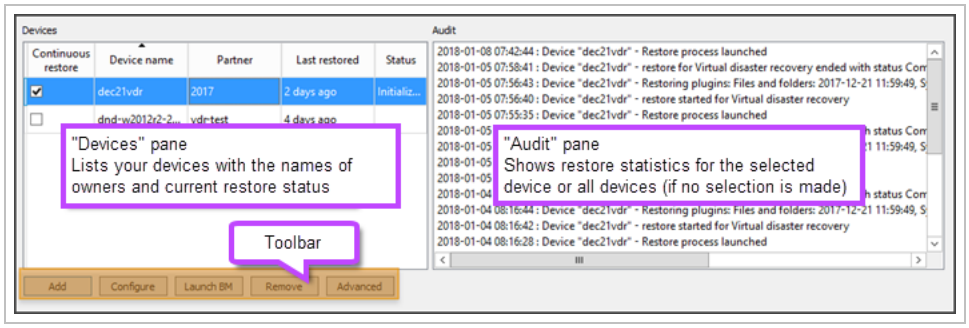
If you want to stop the Recovery Console from opening automatically at startup of the device:

1. Open the Task Manager on the device
2. Switch to the **Startup** tab
3. Disable Recovery Console's ability to show on Startup
4. Now open **Services** on the device my typing `services.msc` into the start bar
5. Search for the Recovery Console Service
6. Right click and select **Properties**
7. Change the **Startup type** to **Manual**, or **Disabled**
8. Click **Apply** and **OK** to save the changes and close out of the service properties

Recovery Console interface

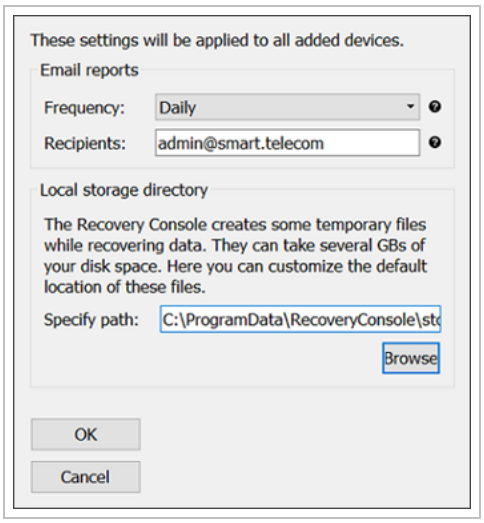
The main application window is divided into 2 panes:

1. The **Devices pane** - this is where your devices are listed
2. The **Audit pane** - this is where you can view restore statistics for the device selected on the Devices pane



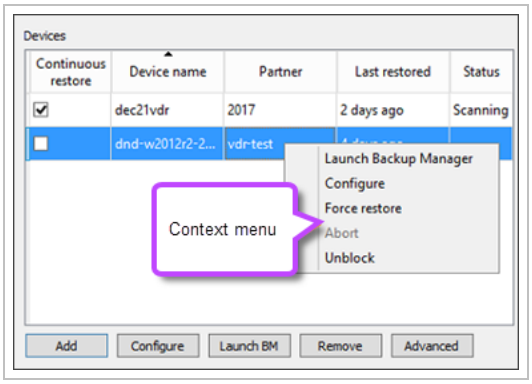
At the bottom you can see a **toolbar**, it provides access to the main functions:

- **Add** - add a new device to the Recovery Console
- **Configure** - edit settings for the selected device
- **Launch BM** - open a restore-only Backup Manager for the selected device
- **Remove** - remove the selected device from the Recovery Console
- **Advanced** - edit common settings for all devices: enable email notifications on the statuses of recent recovery sessions or change the default local storage directory



Additional options can be accessed through a **context menu**.

- **Force restore** - start data recovery for the selected device right now (without waiting for a new backup session). If there is no data available for recovery, the option will be unavailable
- **Abort** - terminate all active recovery sessions related to the device. If there are no such sessions, the option will be unavailable



Enabling recovery in Recovery Console

To enable data recovery for a backup device, add it to the Recovery Console and specify recovery settings for it.

Keep in mind a few points before you get started:

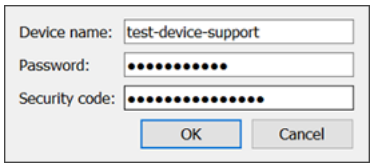
- Devices are added one at a time and cannot be added in bulk
- The number of devices you can add is unlimited, but take into account the available resource on the system running the Recovery Console
- The devices you add must not be installed in Backup Manager on the same computer (this would result in a conflict)
- You can add only those devices that you have access to (full access details are required)

To perform recovery through the Recovery Console:

1. Start the Recovery Console on the host system
2. If the device already exists, move to step #3. If the device is not listed, you should add it first.

   ## To add a device:

   a. Click **Add**

   b. Fill in the device details:

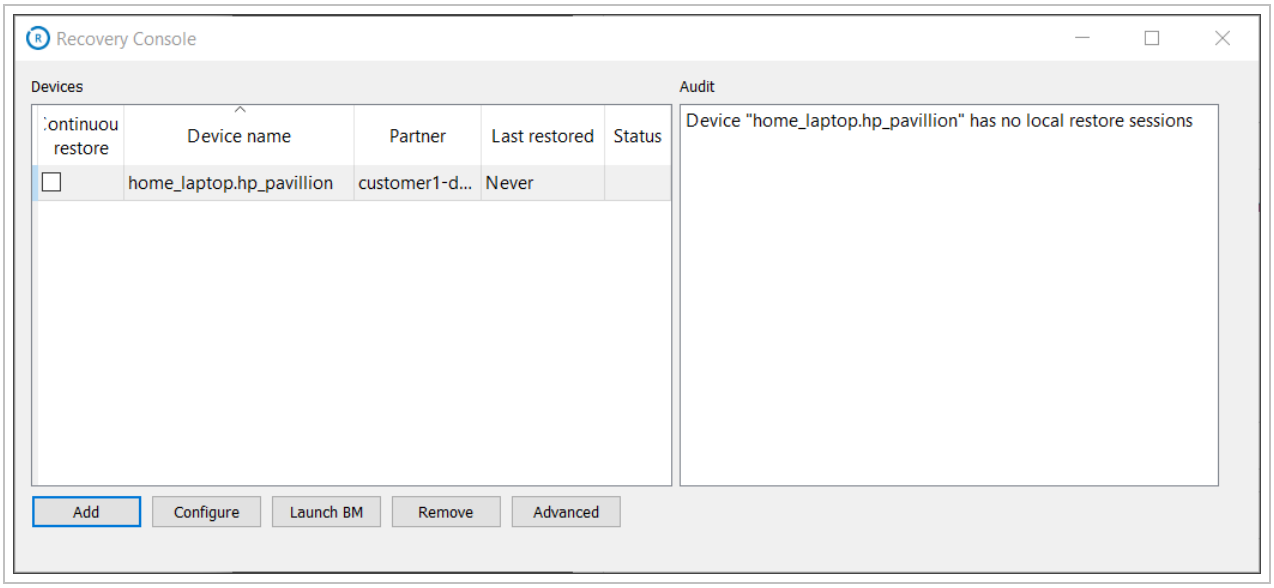
      - **Device name** - The device name as was given when Backup Manager was initially installed. This can be found on the Settings tab of the device in the Management Console
      - **Password** - The device's Installation Key which can be found on the Settings tab of the device in the Management Console
      - **Security code** - This Is also known as the **Encryption Key** or **Passphrase** if the device was automatically installed or you have converted the device to use passphrase-based encryption

        ### Device passphrases

        To find the device name, passphrase etc. for automatically installed devices, please see Getting passphrases for automatically installed devices.

        If you do not know the Encryption Key or Security Code for a regularly installed device, you will need to retrieve this information before progressing. This can be done by converting the device to use passphrase-based encryption. See Convert devices to passphrase-based encryption for full details.

   c. Click **OK**

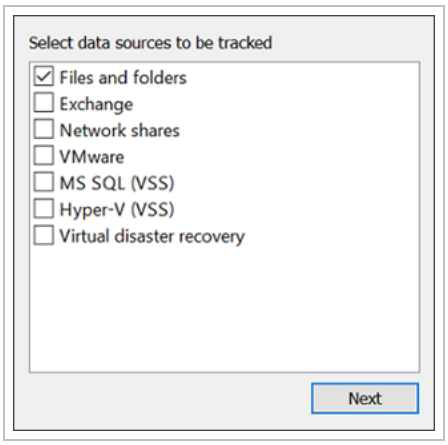


If the source device is already added but the sources are not configured, select the device from the devices panel and then click **Configure**

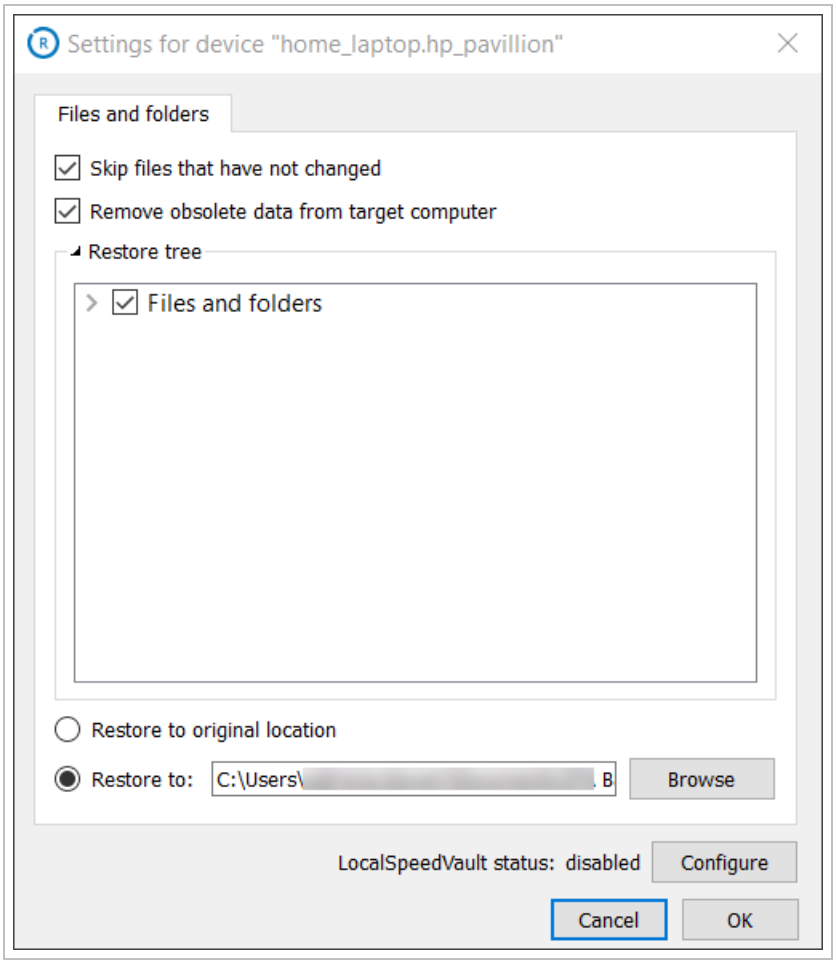
3. Select the data sources that you want to enable recovery for

> The list may contain up to 7 data sources, the selection depends on the product settings.

> Selected data sources can be edited later.



4. Configure settings for the data sources



5. Click **Next** to proceed to the next one
6. Click **OK** to finish and apply the settings once all the selected data sources have been configured
7. If all the settings have been configured, you will get a message offering you to start data recovery. Click **Yes** to enable the continuous recovery mode or **No** if you do not want to start the recovery right now

> If you click **No** to add the device without beginning data recovery, you will be able to do this any time using the **Continuous restore** checkbox

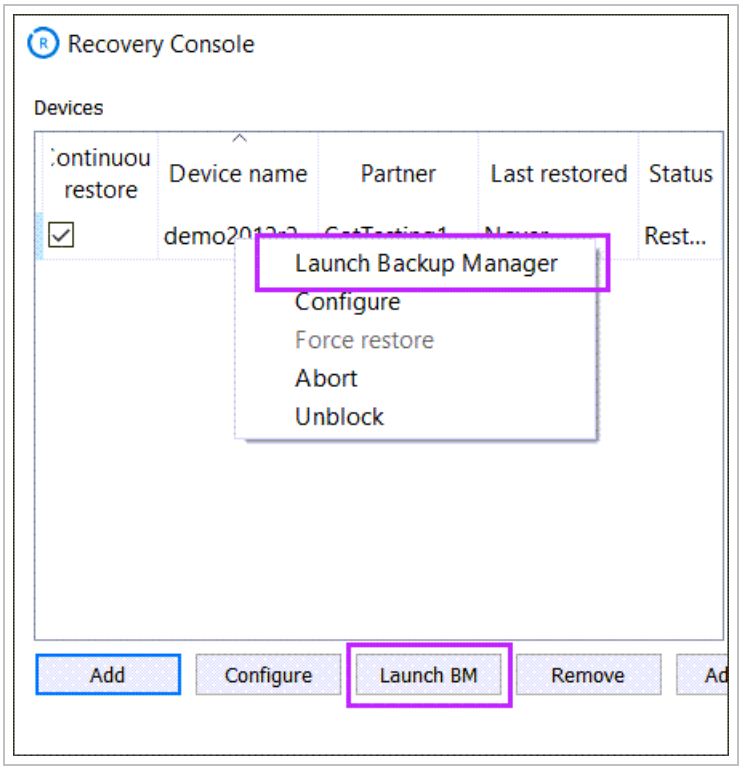
> We do not recommend specifying a Network Share as the storage location when initializing a device on Recovery Console even temporarily as it can be unreliable.

The length of time the recovery takes depends on the size of the system you are restoring, the data transfer speed, and the performance of your computer.

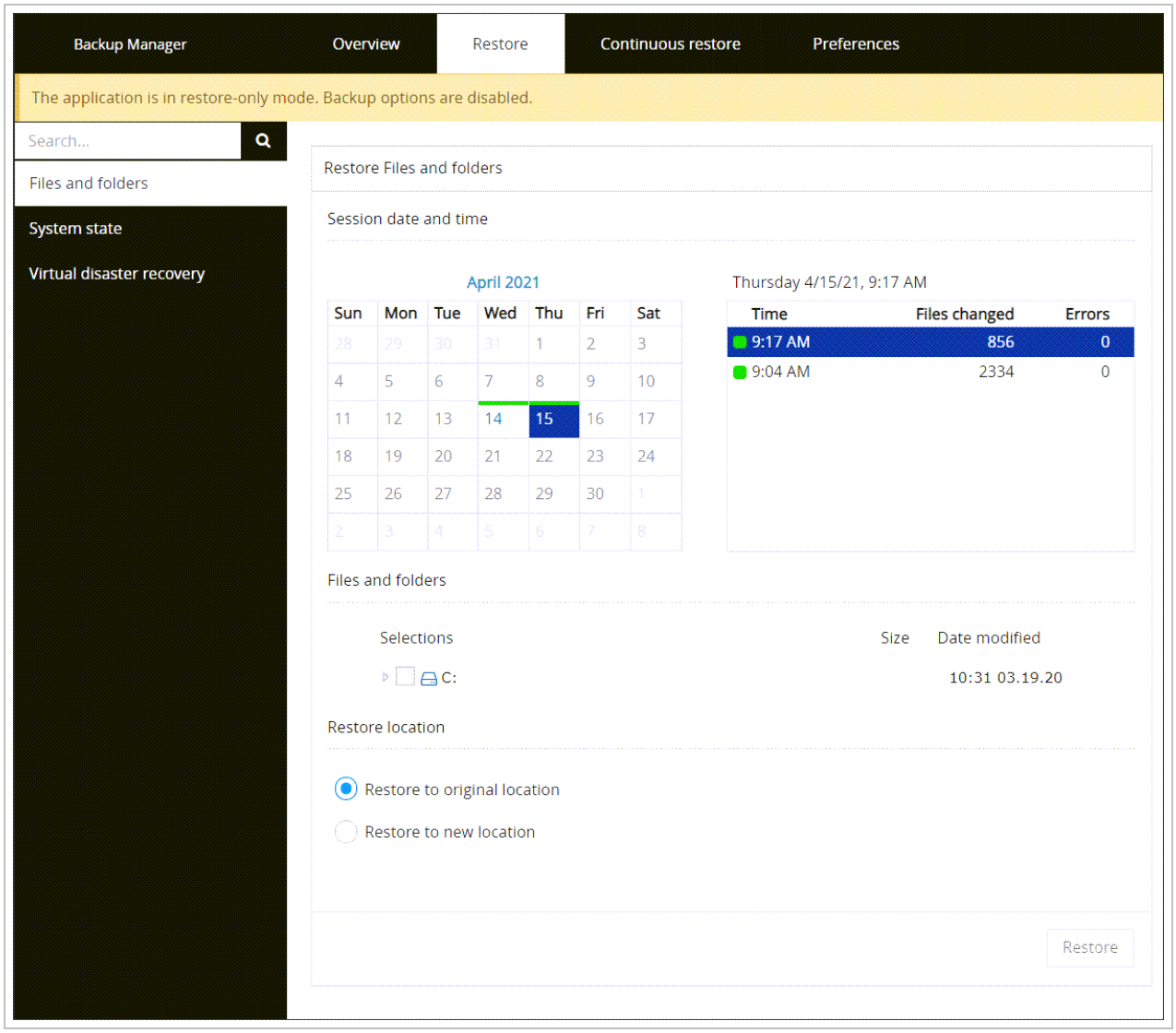
> The Recovery Console must be **open or minimized** to keep functioning. If you have active devices, do not shut down the Recovery Console application and do not power off the computer.

Restore from date/time session

If you wish to restore from a specific session in the past and not from the most recent backup, this can be done by adding the device as above then clicking **Launch Backup Manager** or **Launch BM** from the Recovery Console Devices panel.



1. Once open, the Backup Manager will show in restore-only mode



2. Open the **Restore** module, and then select a data source from the vertical menu to the left. The selection includes all data sources that have been backed up at least once on the current device
3. Select the backup session you want to restore
   - **(A)** next to the name of a session means that the session is archived (more on backup session archiving)
   - **(L)** means that the session has been saved locally in the LocalSpeedVault and the data is not synchronized with the cloud yet
4. Select the data you want to restore. For some data sources like Files and folders you can expand the file tree and select individual files or directories. For other data sources only the root folder can be selected
5. Specify where to restore the selected data: to the original location or to a new one. Enter the target location, if applicable
6. Click **Restore** and wait until the restore process is completed. You can close Backup Manager in the browser while the recovery is in progress (it will continue in background)

Continuous Restore in Recovery Console

Virtual Disaster Recoveries can be performed **on request** or set it to the **Continuous Restore** mode where data recovery is synchronous with backups performed in the source system.

Requirements

> The Continuous Restore requires a dedicated computer or virtual machine that must not be used for other purposes (learn more).

Device passphrases

To find the device name, passphrase etc. for automatically installed devices, please see Getting passphrases for automatically installed devices.

If you do not know the Encryption Key or Security Code for a regularly installed device, you will need to retrieve this information before progressing. This can be done by converting the device to use passphrase-based encryption. See Convert devices to passphrase-based encryption for full details.

Enabling the Continuous Restore mode

Continuous Restore can be enabled either in Recovery Console or by installing Backup Manager in restore-only mode. Information on configuring this from Backup Manager can be found here: Continuous restore in Backup Manager.

Recovery Console instructions

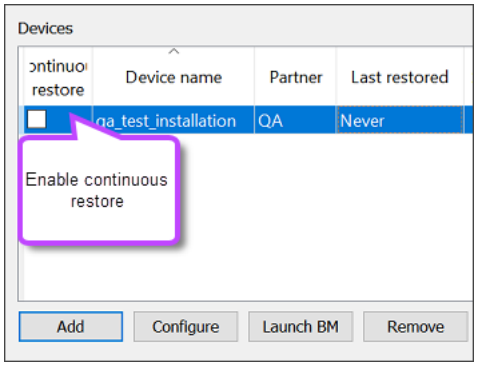
> This can be found from the Downloads page in Management Console, or from the Backup Downloads page on our website.

The Continuous Restore mode[1] is the predefined option in the Recovery Console. You can manage the setting for each device through the **Continuous Restore** checkbox to the left of each device name.

1. Add the device to the Recovery Console following these steps
2. Once the device has been added and configured correctly, tick **Continuous Restore** which can be found to the left of the device name in the Devices panel

---

[1]Repeated data recovery to a computer or virtual machine that is specifically allocated for that purpose. The recovery is synchronous with backups performed in the source system.



3. The Virtual Disaster Recovery will now begin running in Continuous Restore mode. If you need to amend any settings, this can be done by launching Backup Manager for the device and changing settings from **Continuous restore > Virtual disaster recovery**

> If you click 'Launch BM' before configuring continuous restore as above, you will find the content of the tab is greyed out and you cannot make any changes. Enable continuous restore first before launching the Backup Manager client.

Using virtual machines in-between restore sessions

The target virtual machine **is not supposed to be in use** while the Continuous Restore mode is active. If your recovery software detects that the virtual machine was started in-between restore sessions, further restores **are blocked** and a warning message appears. This is done to prevent possible data loss.

Unblocking the Continuous Restore

There are several ways to **unblock the Continuous Restore process:**

1. Click the **Unblock** button in the warning message
2. In Backup Manager, go to **Continuous restore > Virtual disaster recovery** and then click **Restore**. This will initiate a quick delta restore that will overwrite the changes at the target location (if any)
3. In the Recovery Console, right-click the device and choose **Unblock** from the context menu

After this is done, the continuous restore process will be fully functional again.

> If the virtual machine may contain changes that you want to keep, please make a copy of it before you unblock the Continuous Restore mode.

Disabling virtual machine checks

The recovery software checks if the virtual machine has been in use before each virtual disaster recovery session. If you are sure no important data is added to the virtual machine, you can **disable these checks** and have the previous version overwritten without warning messages. To do it, add `VdrRestorePolicyForceOverwrite=1` to the `[General]` section of the configuration file belonging to your recovery software.

- Backup Manager instructions
- Recovery Console instructions

> The setting applies to **all** backup devices installed on the current computer (one device for the Backup Manager or multiple devices for the Recovery Console).

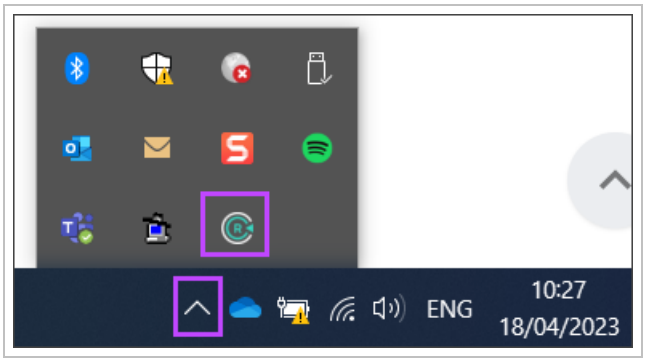
Advanced settings in Recovery Console

You can access some advanced settings through a configuration file belonging to the Recovery Console (*config.ini)*. The file is created automatically during the Recovery Console installation.

Editing configuration file

1. Open the Recovery Console installation folder. Find the configuration file found at the appropriate Config.ini location for your operating system
2. Enter appropriate settings to the `[General]` section
3. **Save** the changes and close the file
4. Restart the Recovery Console to apply the settings

   The only way to quit the application is by right-clicking the "R" icon in the notification area and then clicking **Quit** in the context menu that opens



Required settings for Recovery configuration file

```
[General]
InteractiveConfigurationRequired=0
InstallationId=372da5d2fa048be724831
AzureDefaultCredentialsFile=
AzureDefaultUsername=
AzureDefaultPassword=
```

When you edit the file, make sure the parameters stay in the original sections. The table below lists frequently used parameters.

Home section	Parameter	Definition	Supported values
`[General]`	`InteractiveConfigurationRequired`	Is any configuration required by the user during installation	▪ `=0` no (Default) ▪ `=1` yes
`[General]`	`InstallationId`	A unique identifier auto-	Text

Home section	Parameter	Definition	Supported values
		matically assigned to the current Recovery Console installation.	

Optional Parameters

Home section	Parameter	Definition	Supported values
`[Logging]`	`LoggingLevel`	The level of logging information you require the device to take	▪ `Log` ▪ `Error` ▪ `Warning` (Default) ▪ `Debug`
`[General]`	`VdrRunningFpLimit`	The number of Continuous Restores allowed to run at a time	▪ Any whole number ▪ 5 (Default) ▪ Recommended no higher than the number of available CPU Cores minus 2

For VMware ESXi and Hyper-V targets

Parameter	Definition	Unit of measurement	Supported Values
`VdrCheckReportSystemLogCount`	Use this setting to customize the number of system log events to display in email notifications created after the completion of a virtual disaster recovery session. The count starts from the newest events. To create a notification, you need to enable the **Start the virtual machine after restore and take screenshot** setting in your virtual disaster recovery settings and then create an	Log Count	▪ Any whole number ▪ Recommend 100

Parameter	Definition	Unit of measurement	Supported Values
	event-based notification rule in the Cloud Management Console.		
`VdrVmBootDelayInSeconds`	Use this setting to customize the Virtual Machine boot delay	Seconds	Whole numbers (1 or more)
`VdrVmBootTimeoutInSeconds`	Use this setting to customize the Virtual Machine boot timeout	Seconds	Whole numbers (1 or more)

Enable debug logging

Here is how to enable debug logs:

1. Open the configuration file as above
2. Add a new section with the following content to the bottom of the configuration file:

```
[Logging]
LoggingLevel=Debug
```

3. Restart the Recovery Console
4. Try to reproduce the issue

Bare metal recovery guide

Bare Metal Recovery is used when you want to restore an existing device's data to new hardware. No prior Operating System installation is necessary. The Bare Metal Recovery allows you to recover a device's **full system state**, **applications** and **files and folders** at the same time. The technology relies on a custom recovery distribution running from a **bootable media** (e.g. USB or disk).

The Bare Metal Recovery is a **Windows** *only* technology. It involves several different computers:

- The **source computer** - the backup device whose hardware has failed or requires replacement for some other reason
- The **host computer** - the hardware on which a bootable media is created for bare metal recovery purposes. The host computer can be the source computer
- The **target computer** - the hardware that you want to recover the source system to

> Please carefully check the Bare metal recovery requirements and limitations before moving on to the Bare metal recovery instructions.

Alternative solutions

If the target computer does not meet the requirements or if you cannot allocate a separate computer for the recovery, please consider the following alternatives:

- Performing virtual disaster recovery. This feature is based on virtual disk creation and does not have any particular hardware requirements
- Installing the operating system on the target computer manually and then performing standard data recovery (any data sources except for the System State)

> **Critical Restore?** We're not the judge of when a recovery is especially time critical—you are.
>
> **Critical Restore** is our partner-driven fast escalation process. Just let us know on your initial support call, email, or chat message that a specific recovery is especially time sensitive, and we'll bring all hands on deck immediately to help you get your customer back up and running ASAP.
>
> For more details please see the Critical Restore FAQ's.

Bare metal recovery requirements and limitations

Jump straight to:

- Source system requirements
- Host system requirements
- Target computer requirements
- USB drive requirements
- USB drive limitations

Source system requirements

Supported operating systems

Only Windows systems are subject to bare metal recovery. The bare metal recovery tool supports the following versions:

- Windows 8[1], 8.1, 10, 11 – Pro and Enterprise editions only (due to Microsoft licensing limitations)
- Windows Server 2012[2], 2012 R2, 2016, 2019 and 2022 – Standard and Data-center editions only (due to Microsoft licensing limitations)

System configuration

Though it may be possible to restore a Virtual Machine using the Bare Metal Restore tool, it is **not recommended**. As the Bare Metal Recovery tool is not designed to be used with virtual environments, our support teams cannot troubleshoot issues that may occur.

If you would like to restore Virtual Machines, you need to use our Virtual Disaster Recovery tool.

---

[1]If the source machine is booted from a GPT disk (UEFI firmware), virtual disaster recovery must be performed from a recent version of Windows: Windows 8.1, Windows 10, Windows Server 2012 R2 or Windows Server 2016.
[2]If the source machine is booted from a GPT disk (UEFI firmware), virtual disaster recovery must be performed from a recent version of Windows: Windows 8.1, Windows 10, Windows Server 2012 R2 or Windows Server 2016.

> Environments with third-party boot loaders, dual-boot systems or systems build with OEM recovery partitions are not supported.

Systems containing **dynamic disks** are suitable for bare metal recovery. The dynamic disks are converted to basic disks. Dynamic disks made up of stripes of multiple smaller disks are replaced with a single large disk.

> If a disk uses the **MBR** partition table, the total size of its volumes must not exceed **2TB**.

Mixed MBR/GPT partitions on the same disk are not supported. **Mixed MBR/GPT disks** can cause issues. If you have such a disk, recover only the boot drive through the bare metal recovery. Then restore the data drive separately, if needed.

Minimum backup requirements

The following data from the source system must be backed up. This is the minimum requirement.

- The "System State" data source: all data
- The "Files and Folders" data source: **the whole system disk (`C:\` or any other depending on the configuration of your computer)**

You can back up any other data that is important to you as well. Data belonging to the "Files and Folders" data source can be recovered together with the system disk. Other data sources can be recovered after the bare metal recovery process is completed.

Host system requirements

Software requirements

You can create a bootable media for bare metal recovery on the following Windows systems:

- Windows 8[1], 8.1, 10, 11 – Pro and Enterprise editions only (due to Microsoft licensing limitations)
- Windows Server 2012[2], 2012 R2, 2016, 2019 and 2022 – Standard and Data-center editions only (due to Microsoft licensing limitations)

Hardware requirements

The CPU must be **64-bit** capable (all recent hardware generations meet this requirement).

Target computer requirements

The target computer must be the same as the source computer (same **model** and **configuration**). Any differences in the manufacturer, processor, architecture, network interface controller, storage controller etc. may prevent the bare metal recovery process from completing successfully. In particular, it is strongly recommended not to go from **single-processor to multiprocessor** environments due to OS licensing restrictions. The same can be said when going from one **OEM** to another, since the operating system is licensed to the OEM license.

---

[1] If the source machine is booted from a GPT disk (UEFI firmware), virtual disaster recovery must be performed from a recent version of Windows: Windows 8.1, Windows 10, Windows Server 2012 R2 or Windows Server 2016.
[2] If the source machine is booted from a GPT disk (UEFI firmware), virtual disaster recovery must be performed from a recent version of Windows: Windows 8.1, Windows 10, Windows Server 2012 R2 or Windows Server 2016.

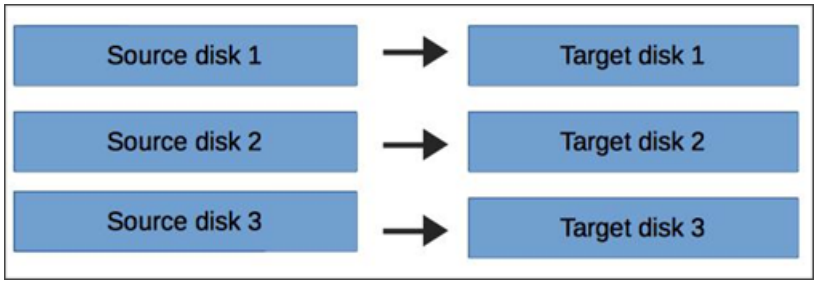
Below is the full list of **critical requirements** to the target computer.

CPU

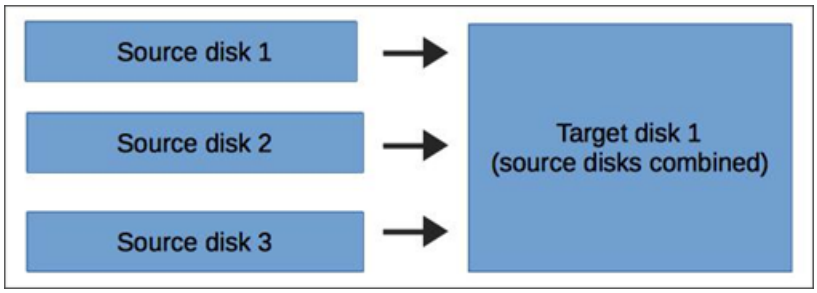
The CPU must be **64-bit capable** (all recent hardware generations meet this requirement). This requirement applies to version 18.2 and later.

Number of disks

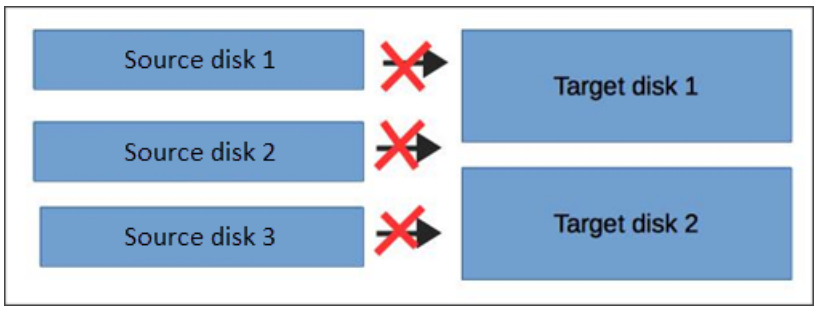
The **number** of physical disks on the target computer must equal or exceed the number of disks on the source computer.



It is also possible to use **one large physical disk** for bare metal recovery. The disk is automatically formatted using the same partition table (GPT/MBR) that was used on the system disk of the source computer.



The feature works if the target machine contains **only one** physical disk. For example, it is not currently possible to restore 3 physical disks to a machine with 2 physical disks.



Firmware

The firmware on the target computer must be compatible with the configuration of the source disks.

- If the physical disks on the source computer have the **GPT** partition table, the target computer must have **UEFI** firmware and must be booted in the UEFI mode.
- If the physical disks on the source computer have the **MBR** partition table, then both of the firmware types - **BIOS and UEFI** - are supported on the target computer.

The table below summarizes the firmware requirements as dependent on the source disk partition table.

Source partition table	BIOS (Target firmware)	UEFI (Target firmware)
GPT	Incompatible	Compatible
MBR	Compatible	Compatible (legacy BIOS-compatibility mode)

Disk size

The physical disks on the target computer must be of the **same size** as the original disks or larger.

If the total size of a source disk exceeds the size of the replacement disk on the target computer, the Bare Metal Recovery tool will try to shrink it. This is possible if the **last partition** on the source disk has enough free space.

> The physical disks on the target computer must be **clean**, meaning there must be no data and no partition into logical disks. If you are not sure whether an existing disk partition has been completely removed, please start cmd.exe as administrator and run the `diskpart clean all` command.

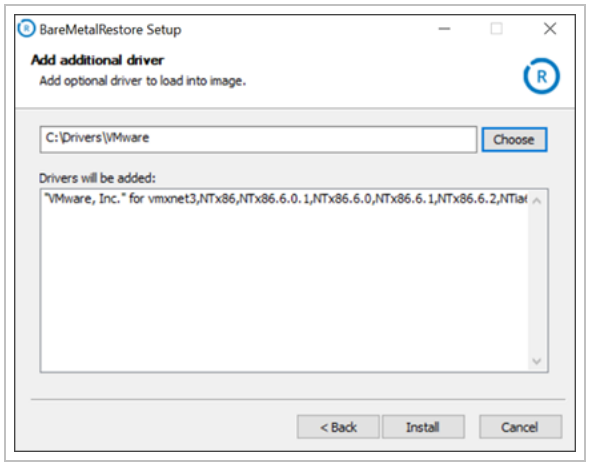
Internet access

The target computer must be connected to the Internet using a **network cable**.

Dissimilar hardware

Dissimilar hardware (USB controllers, chipset, NIC, video, storage, etc.) is supported, assuming that the source system contains **drivers** for it. Without the drivers, the recovered system may not be able to access the external network or USB ports.

To avoid such issues, you can inject missing drivers into the image during the creation of the boot disk (Step 2.4 of the instructions).



USB drive requirements

You need a USB drive that is recognized as **removable media**. The drive must have at least **512 MB** of free disk space.

If the session you are restoring was created by Backup Manager version **17.3** or earlier or if you are using the Bare Metal Recovery tool version 17.3 or earlier, the minimum of **8 GB** of free space is required on the USB drive.

> All data on the USB drive will be **overwritten** so please make sure the drive does not contain any important files.

USB drive limitations

Devices where BitLocker is enabled will not be able to create the Bare Metal Restore USB device.

> To create the BMR USB, please disable BitLocker and try again.

Bare metal recovery instructions

Steps to take:

- Step 1: Download recovery software
- Step 2. Create a bootable media
- Step 3. Boot the target machine
- Step 4: Recover the source system
- Step 5. Recover other data (if applicable)

> Before beginning the Bare Metal Recovery, all requirements **must** be met including Disk size

Step 1: Download recovery software

The Bare Metal Recovery tool comes in two formats:

1. EXE - for USB drives and removable storage devices
2. ISO - for CDs, DVDs and virtual machines

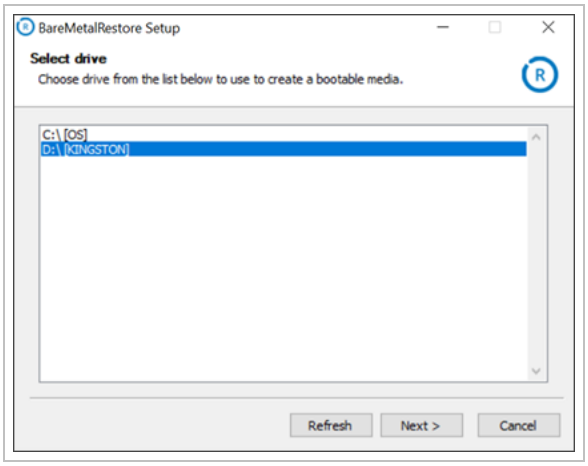
> This can be found from the Downloads page in Management Console, or from the Backup Downloads page on our website.

Step 2. Create a bootable media

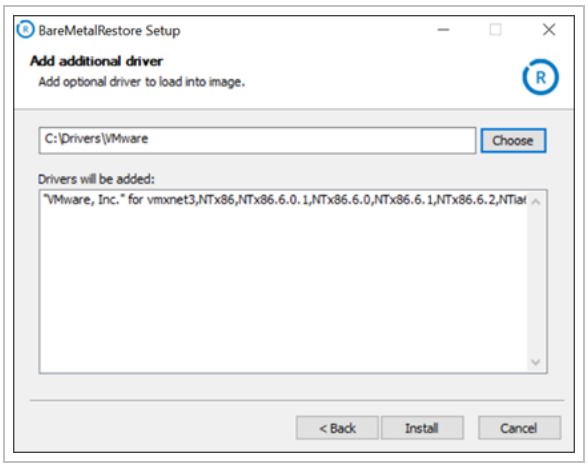
Option A: Create a USB drive

1. Start the source computer or another Windows computer that meets the host system requirements
2. Connect the USB drive to that computer
3. Start the EXE installer downloaded at step 1, and then select the USB drive for the installation

   > **Important:** be careful with the selection because the contents of the drive will be overwritten.



4. Specify drivers to inject into the image (if they are not available on the target machine)



5. When the installation is completed, disconnect the USB drive from the computer

> The flash drive is formatted to the **FAT32** file system that can be booted both in the UEFI and BIOS mode.

Option B: Create a bootable CD/DVD

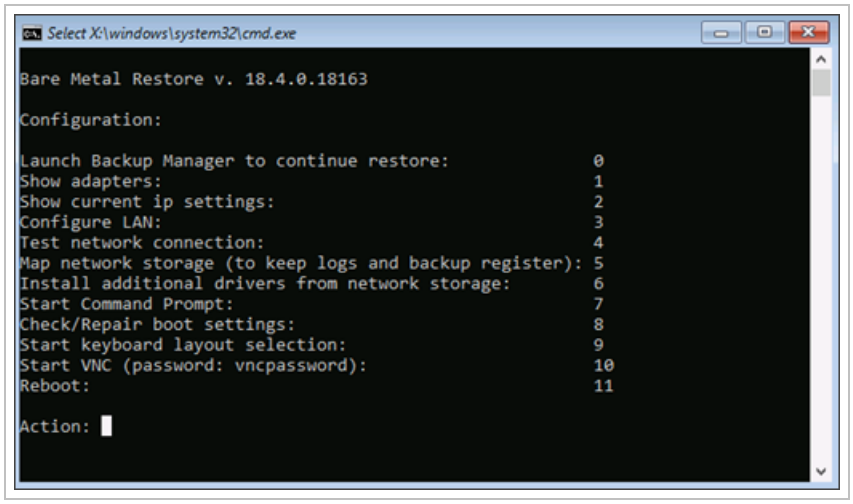
1. Start the source computer or another Windows computer that meets the host system requirements
2. Insert blank CD media into an attached burner
3. Burn the ISO file downloaded at step 1 to blank media using a third-party CD burning tool
4. When the process is complete, eject the optical media

> You will be able to inject **additional drivers** when you boot the target machine at the next step.

Step 3. Boot the target machine

1. Insert the created Boot CD or connect the USB drive to the target computer
2. Turn on the computer and boot it from the CD or USB drive

Make sure you boot in the appropriate mode (BIOS or UEFI). If you boot in a mode that is not compatible with the firmware used on the source computer, there will be a warning message when you get down to recovery.



The Bare Metal Recovery boot menu has the following options:

- **Show adapters** - check the network adapters detected on the current computer. For each adapter, a state and type is provided
- **Show current IP settings** - check the current Windows IP configuration (adapter, connection-specific DNS suffix, IPv6 address, subnet mask and gateway)
- **Configure LAN** - configure IP settings for network adapters
- **Test network connection** (available starting from version 18.4) - make sure connection to the Cloud is available (this is crucial for the completion of recovery)
- **Start Command Prompt** - this lets you reach some options outside of the Bare Metal Recovery boot menu (for example, run the DiskPart utility or edit the hosts file)
- **Check/repair boot settings** (available starting from version 18.4) - scan all disks for Windows installations. If a boot error is detected, the Bare Metal Recovery tool tries to repair it
- **Start keyboard layout selection** - select another language for the keyboard layout. Reload the current screen to apply the new selection to it
- **Start VNC** (available starting from version 18.4) - enable VNC to be able to connect to the current machine remotely using its IP address
- Reboot the computer

Additional boot options for ISO images:

- **Map network storage**. Configure a path to a local network resource where temporary data will be written (logs, Backup Register, etc.). If you skip the setting, operational memory will be used, which may be insufficient. Also, additional drivers can be injected into the restored system and current WinPE image
- **Install additional drivers from network storage** (available starting from version 18.4) . Before enabling the feature, create the **Additional drivers** directory on a network resource, put required drivers there (.inf and .sys files for each driver) and configure access to that resource using the **Map network storage** feature

Enable debug logging

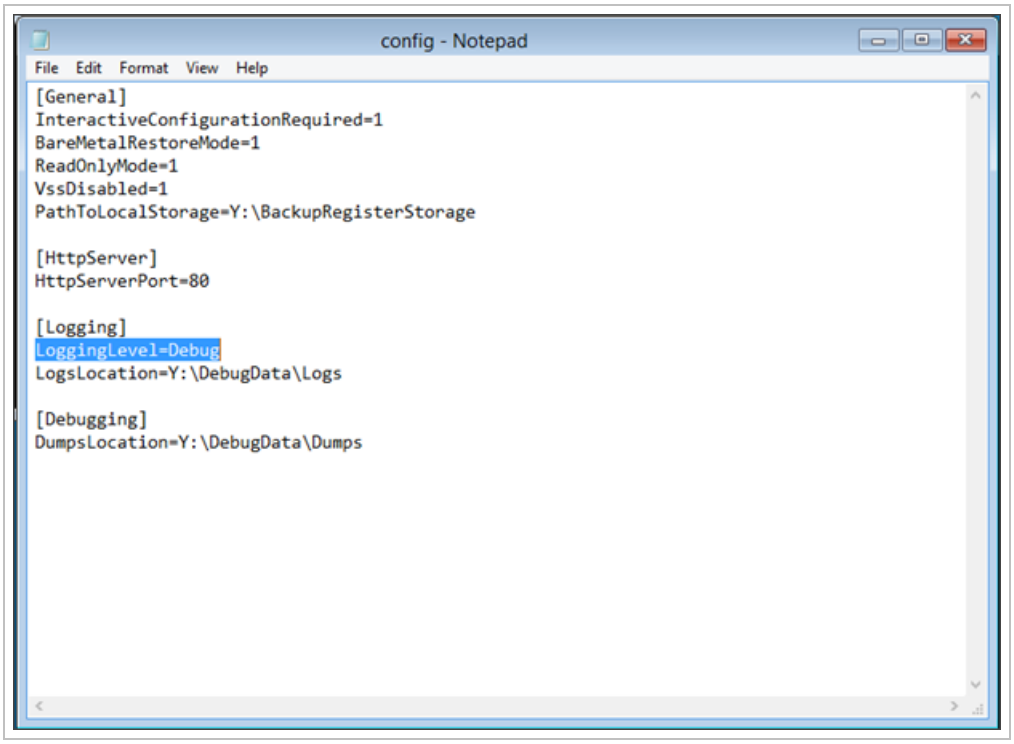
You can enable debug logging while inside the BMR tool by following these steps:

1. In the BMR tool when at the command screen to choose the actions, choose the **Start Command Prompt** option
2. This will bring up a CMD window, in here type:

```
notepad '%programfiles%\Backup Manager\config.ini'
```

3. This will bring up the config.ini file in a notepad box. Add the following two lines to the [Logging] section:

```
LoggingLevel=Debug
LogsLocation=Y:\DebugData\Logs
```



> If `[Logging]` does not exist as its own section, you will have to create this yourself.

4. Save and close the configuration file

Change Drive Letter

If you want to change the drive letter of the LocalSpeedVault plugged in to the Bare Metal Recovery target device this can be done by using the diskpart commands:

1. Enter the CMD window from the BMR tool
2. Type `diskpart` and hit **enter**
3. Type `list disk` and hit **enter**

4. Type `select disk 0` and hit **enter** (for example, the LSV might be another disk)
5. Type `assign letter=R` and hit **enter** (R can be any drive letter not currently in use)
6. Type `exit` and hit **enter**
7. Continue with the Bare Metal Recovery from the interface as normal

Step 4: Recover the source system

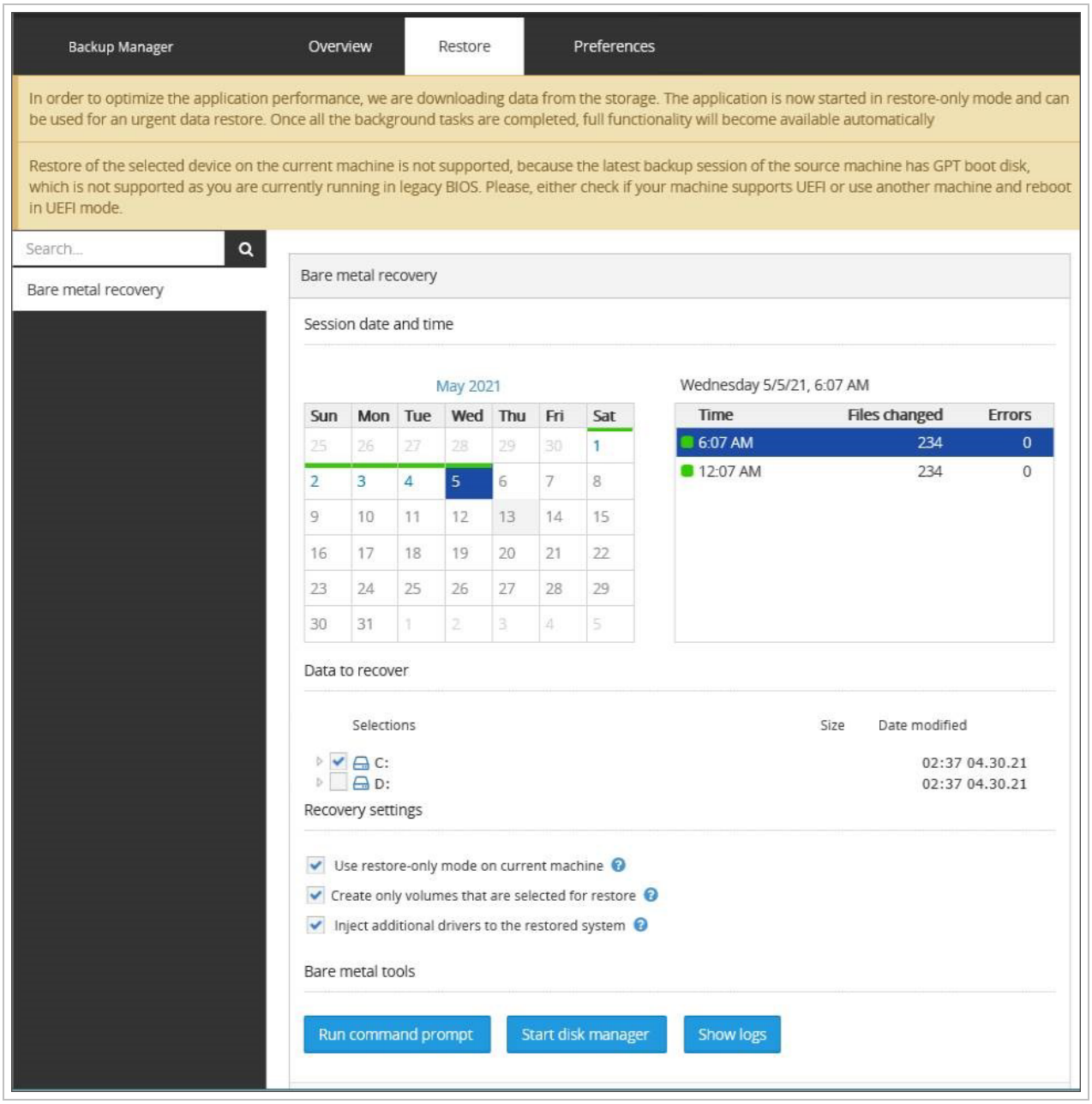
1. After you have configured the boot settings, press 0 on the keyboard (it will start the Backup Manager installation wizard)
2. Select an interface language

3. Enter your backup device name, installation key and encryption key/security code or passphrase
4. When the installation is completed, open the **Restore** tab and configure your recovery preferences

> The data you select for recovery must be sufficient to boot the system.

> Starting from version **18.9**, a new setting has been made available (**Inject additional drivers to the restored system**). It lets you perform recovery with or without additional drivers. The feature works on condition that you added the drivers during bootable media creation or through the boot menu settings on the current machine.

5. Click **Restore** at the bottom to start the recovery



6. When the recovery is completed, eject the USB drive and reboot the computer

> After rebooting the system, some users can get an error message (Windows Error Recovery). This can happen if Windows has detected an unscheduled shutdown. In this case, you need to select "Start Windows Normally". In most cases this is enough to eliminate the error.

What to do if the UEFI mode is not accessible

If the system you are recovering requires you to boot in the UEFI mode and the option is not available from the boot menu or if you get an error message saying that the source disk configuration is not compatible with the target machine firmware, please try selecting the UEFI boot file manually.

1. Look for a firmware option to choose the boot file. Examples: "Boot to file", "Boot to EFI file"
2. Select the file from the USB drive: `\EFI\BOOT\BOOTX64.EFI`

More details can be found in the following Microsoft support article: WinPE: Boot in UEFI or legacy BIOS mode.

Step 5. Recover other data (if applicable)

You can recover the rest of your data according to the general data recovery instruction.

If the Backup Manager was installed on the system drive on the source computer, you will find it available on the target computer. If not, you will need to download it and run the installation.

Virtual disaster recovery guide

The Virtual Disaster Recovery feature lets you create a working mirror of your computer and run it in a virtual environment. The mirror can be kept up-to-date automatically through the Continuous Restore feature.

The feature is currently available on **Windows** devices. Please contact your service provider to add the Virtual Disaster Recovery to your service package (if it is not included yet).

You can perform virtual disaster recovery to the following **targets**:

- VMware VMDK (local)
- VMware ESXi (on a remote server)
- Hyper-V (local)
- Local VHD files (local, no Hyper-V installation required)

> It is highly recommended to use an **isolated network** for tests. Performing virtual disaster recovery to a production environment can result in conflicts (for example, there can be 2 machines with the same IP addresses). Such conflicts lead to errors and data loss.

> Please carefully check the Virtual Disaster Recovery Requirements for the correct recovery type before beginning with the Virtual Disaster Recovery Instructions.

> **Critical Restore?** We're not the judge of when a recovery is especially time critical—you are.
>
> **Critical Restore** is our partner-driven fast escalation process. Just let us know on your initial support call, email, or chat message that a specific recovery is especially time sensitive, and we'll bring all hands on deck immediately to help you get your customer back up and running ASAP.
>
> For more details please see the Critical Restore FAQ's.

Virtual Disaster Recovery Requirements

Before you initiate Virtual Disaster Recovery (VDR), make sure both of the systems involved are supported and properly configured:

- **Source system** – This is the device that has been backed up with Backup Manager and needs to be recovered
- **Host system** – This is the device that the recovery software is installed on, where you want to restore the data to. It can be the same machine as the source system or a different one

You also need to have a note of the backup device's **Encryption key/Security code** or have access to the **Passphrase** before you begin.

Source system requirements

Supported Windows versions

The following Windows versions are supported for Virtual Disaster Recovery:

- Windows 8[1], 8.1, 10, 11 – Pro and Enterprise editions only (due to Microsoft licensing limitations)
- Windows Server 2012[2], 2012 R2, 2016, 2019 and 2022 – Standard and Data-center editions only (due to Microsoft licensing limitations)

Backup selection requirements

Make sure the following data in the source system is backed up:

1. The system state of your computer (the **System State** data source).
2. **The whole system disk** – `C:\` or another disk that has your operating system and that the operating system boots from (the **Files and Folders** data source).
3. Any other data that is important to you. Supported data sources: Files and Folders, MS Exchange, and MS SQL.

> It is possible to back up a system containing **dynamic disks**, though it should be noted that these are converted to basic disks during virtual disaster recovery.

> If a disk uses the **MBR** partition table, the total size of its volumes must not exceed **2TB**.

If in doubt concerning the selection of files, please perform a test restore or contact customer support for assistance.

Optional settings (for better restore speed)

If the data transfer speed through the Internet is not high enough, you can benefit from enabling the LocalSpeedVault in the source system.

Planning to perform recovery from another machine? Then consider placing the **LocalSpeedVault** folder on any of the following:

- A removable storage drive that you will be able to attach to the host machine.
- The host machine (if it is located on the local network).
- Another machine on the local network that is accessible from the host machine.

Host system requirements

---

[1] If the source machine is booted from a GPT disk (UEFI firmware), virtual disaster recovery must be performed from a recent version of Windows: Windows 8.1, Windows 10, Windows Server 2012 R2 or Windows Server 2016.
[2] If the source machine is booted from a GPT disk (UEFI firmware), virtual disaster recovery must be performed from a recent version of Windows: Windows 8.1, Windows 10, Windows Server 2012 R2 or Windows Server 2016.

Supported Windows versions

The following Windows versions are supported for Virtual Disaster Recovery:

- Windows 8[1], 8.1, 10, 11 – Pro and Enterprise editions only (due to Microsoft licensing limitations)
- Windows Server 2012[2], 2012 R2, 2016, 2019 and 2022 – Standard and Data-center editions only (due to Microsoft licensing limitations)

> The host system **must not be older** than the source system. For example, if you want to restore Windows 10, you must install your recovery software on Windows 10 or a newer version.

Device passphrases

To find the device name, passphrase etc. for automatically installed devices, please see Getting passphrases for automatically installed devices.

If you do not know the Encryption Key or Security Code for a regularly installed device, you will need to retrieve this information before progressing. This can be done by converting the device to use passphrase-based encryption. See Convert devices to passphrase-based encryption for full details.

Hyper-V & Local VHD

Cove Data Protection (Cove) has functionality for you to perform virtual disaster recoveries to Hyper-V targets. Hyper-V machines created for virtual disaster recovery purposes contain one or several **virtual disks** (their number equals the number of hard disks you have backed up). These virtual disks have the **VHD** or **VHDX** format. The format is determined by the version of Hyper-V and the system updates installed on your computer. Generally, VHDX disks are created on Hyper-V generation 3.0. VHD disks are created on Hyper-V 2.0.

If you do not have Hyper-V installed on the host machine, consider the "Local VHD file" target instead. It creates a **VHD** file that can be added to a virtual machine later.

Additional Required Software

The host system must have the following software installed:

1. Virtual disaster recovery software (the Backup Manager or the Recovery Console)
2. Hyper-V 2.0 or 3.0. **(Hyper-V Specific - not required for Local VHD file recovery)**

VMWare VMDK & VMWare ESXi

Cove's virtual disaster recovery feature lets you create a VMware machine in a local directory for VMDK and recover your system there.

You will find the following files in the target directory after recovery:

---

[1]If the source machine is booted from a GPT disk (UEFI firmware), virtual disaster recovery must be performed from a recent version of Windows: Windows 8.1, Windows 10, Windows Server 2012 R2 or Windows Server 2016.
[2]If the source machine is booted from a GPT disk (UEFI firmware), virtual disaster recovery must be performed from a recent version of Windows: Windows 8.1, Windows 10, Windows Server 2012 R2 or Windows Server 2016.

1. **VMX** - the primary configuration file, that can be opened with VMware Player/Workstation
2. **VMDK** - a virtual disk file, that stores the contents of the virtual machine's hard disk drive. The number of VMDK disks equals the number of hard drives in the source system

If you want to enable continuous recovery for multiple devices, consider using the **target vSphere/ESXi server** as your virtual disaster recovery host. Make sure you use the **same datacenter and storage** for the host machine and the target machine. This will give you **twofold or threefold speed increase** (confirmed by in-house tests).

Additional Required Software VMWare VMDK

The host machine must have **64-bit** virtual disaster recovery software installed (the Backup Manager or the Recovery Console).

Additional Required Software VMWare ESXi

1. VMware vSphere/VMware. All **paid 64-bit** versions are supported: 6.0, 6.5, 6.7, 7.0 and 8.0

   > Older versions of VMware may continue to work. However, as these have reached **End of Life** and are no longer supported by Microsoft, we can only offer limited support.

2. **64-bit** virtual disaster recovery software (the Backup Manager or the Recovery Console)

> **Free versions** of VMware ESXi hosts are **not supported**. However, we have two workaround options available for these versions:
>
> 1. Create a new virtual machine with required characteristics and perform bare metal recovery there (recommended as a faster option)
> 2. Perform virtual disaster recovery to a VMDK file. Use VMware vCenter Converter to convert the local VMDK file from the workstation format to the appropriate format and to attach it to the ESXi server

> For restore purposes, you **must** ensure the version of VMWare ESXi on the host device is the same or higher as is on the source device.

Once these requirements are met, carefully follow the Virtual Disaster Recovery Instructions to enable VDR for the appropriate target.

Virtual Disaster Recovery Instructions

You can perform virtual disaster recovery using either of these tools:

1. The Backup Manager - lets you recover data from one device to either the same source device or a new one
2. The Recovery Console - lets you recover data from multiple devices simultaneously to a new device

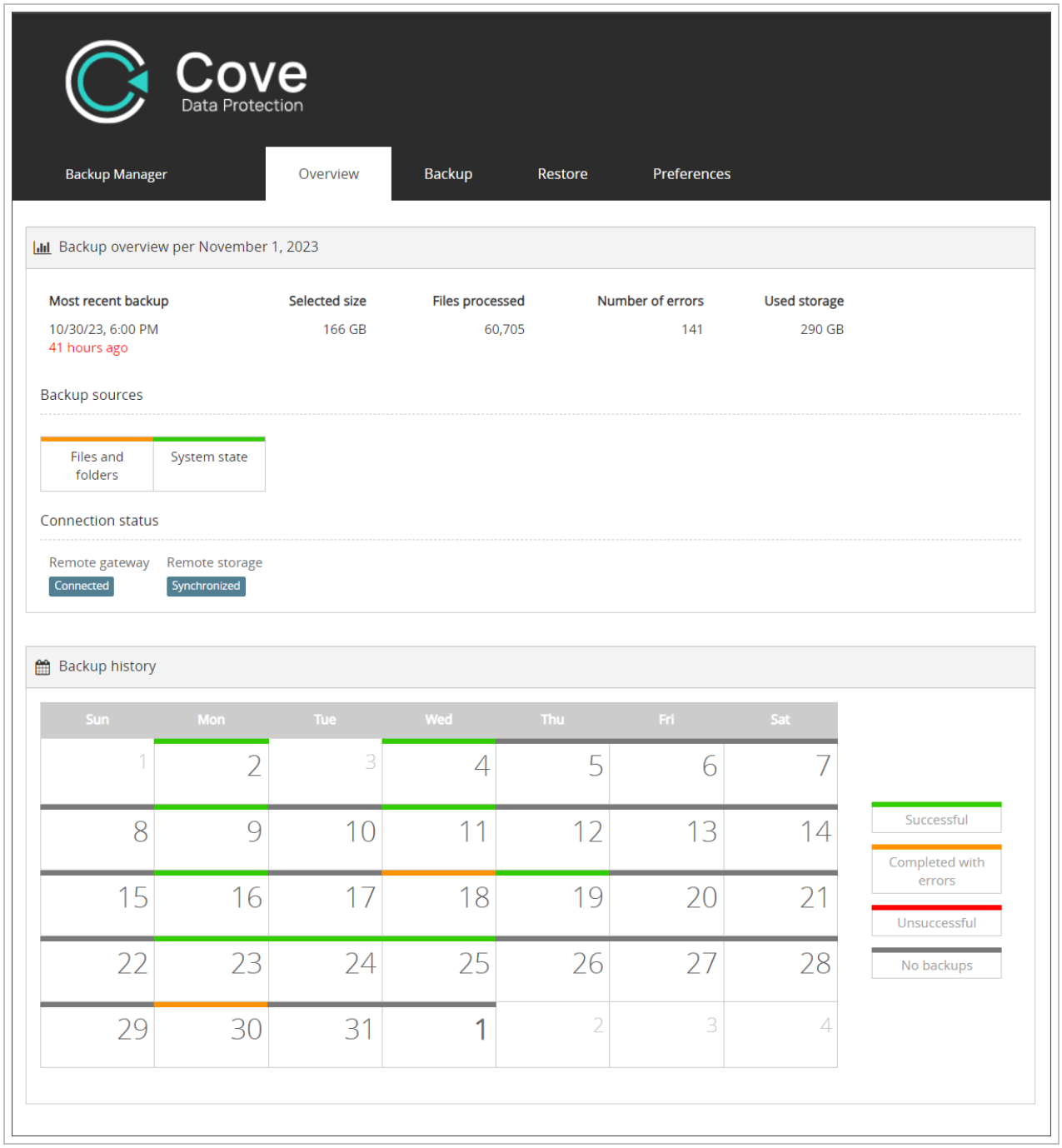
Both of the tools support one-time restores and Continuous Restore.

> Before beginning the Virtual Disaster Recovery, all Virtual Disaster Recovery Requirements **must** be met for the relevant recovery target.

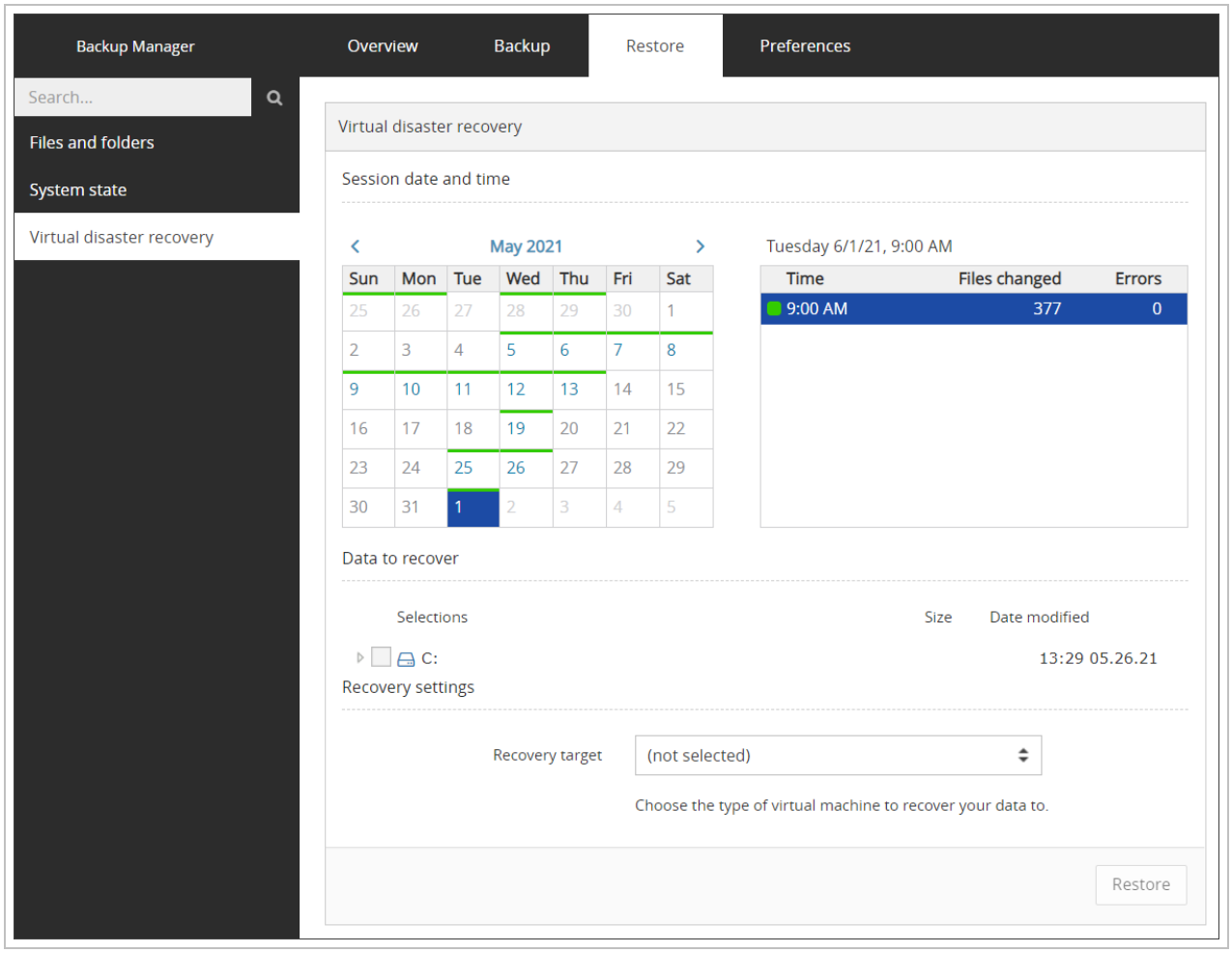
Backup Manager instructions

To perform virtual disaster recovery through the Backup Manager:

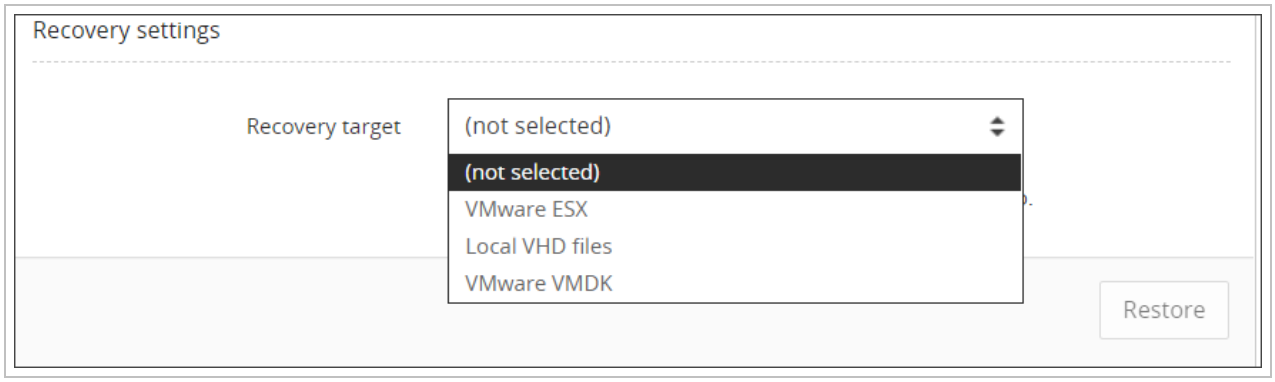
1. Launch the Backup Manager for the device



2. Navigate to the **Restore** tab
3. Click **Virtual Disaster Recovery** from the left-hand sources list



4. Using the calendar, find the session date and time you wish to restore from
5. Select the data to recover
6. In the **Recovery Target** dropdown, select the type of target you want to recover the data to

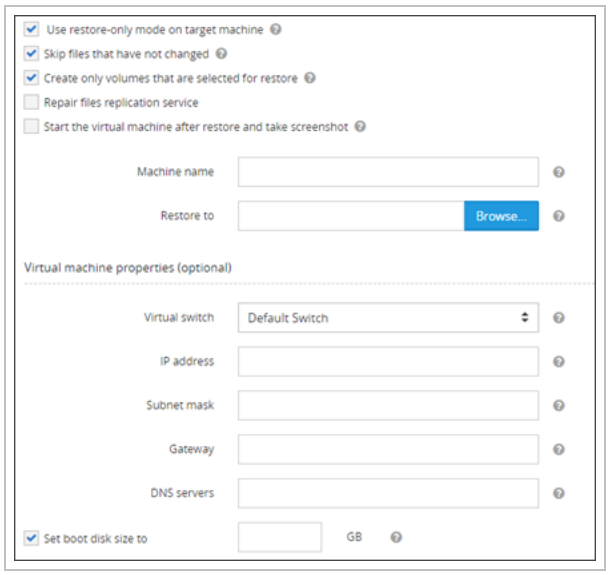


This list is adaptive, so will only show recovery targets that are available on the host device.

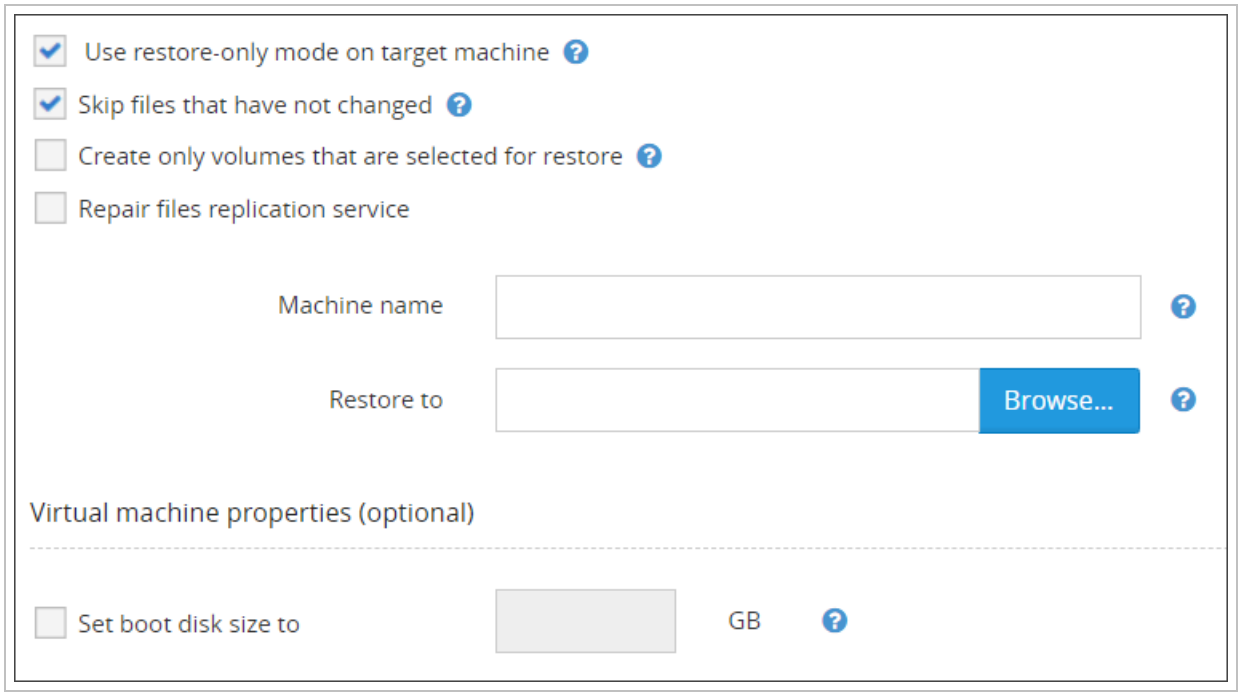
7. Fill out all settings fields for the target used before clicking **OK**

   See the Virtual Disaster Recovery Settings **page** for full details on required and optional settings for each recovery target:

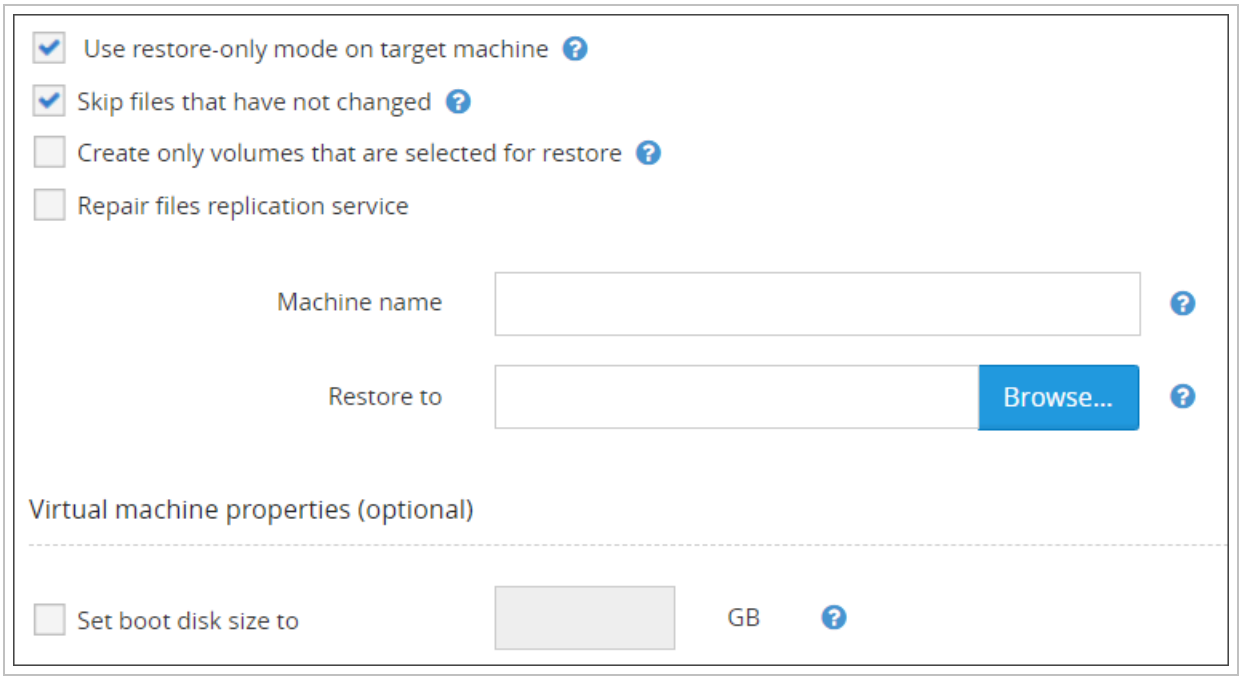
   Hyper-V:



   Local VHD files:



   VMWare VMDK:


Use restore-only mode on target machine
Skip files that have not changed
Create only volumes that are selected for restore
Repair files replication service
Machine name
Restore to
Browse...
Virtual machine properties (optional)
Set boot disk size to
GB

VMWare ESXi:

- [x] Use restore-only mode on target machine
- [x] Skip files that have not changed
- [ ] Create only volumes that are selected for restore
- [ ] Repair files replication service
- [ ] Start the virtual machine after restore and take screenshot

Access to remote ESX server

Server address

Username

Password Connect

Access to virtual machine

Machine name

Data center Select an Option

Host Select an Option

Storage Select an Option

Resource pool Select an Option

Virtual machine properties (optional)

IP address

Subnet mask

Gateway

DNS servers

- [ ] Set boot disk size to GB

8. Click **Restore** to start a recovery process

   Once the Virtual Disaster recovery begins, you will see a banner appear tracking the restore process in the Backup Manager.

> The length of time the recovery takes depends on the size of the system you are restoring, the data transfer speed, and the performance of your computer.

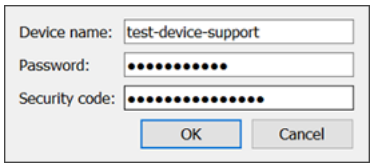
Recovery Console instructions from the most recent session

To perform virtual disaster recovery through the Recovery Console:

1. Start the Recovery Console on the host system
2. If the device already exists, move to step #3. If the device is not listed, you should add it first.

   ### To add a device:

   a. Click **Add**

   b. Fill in the device details:

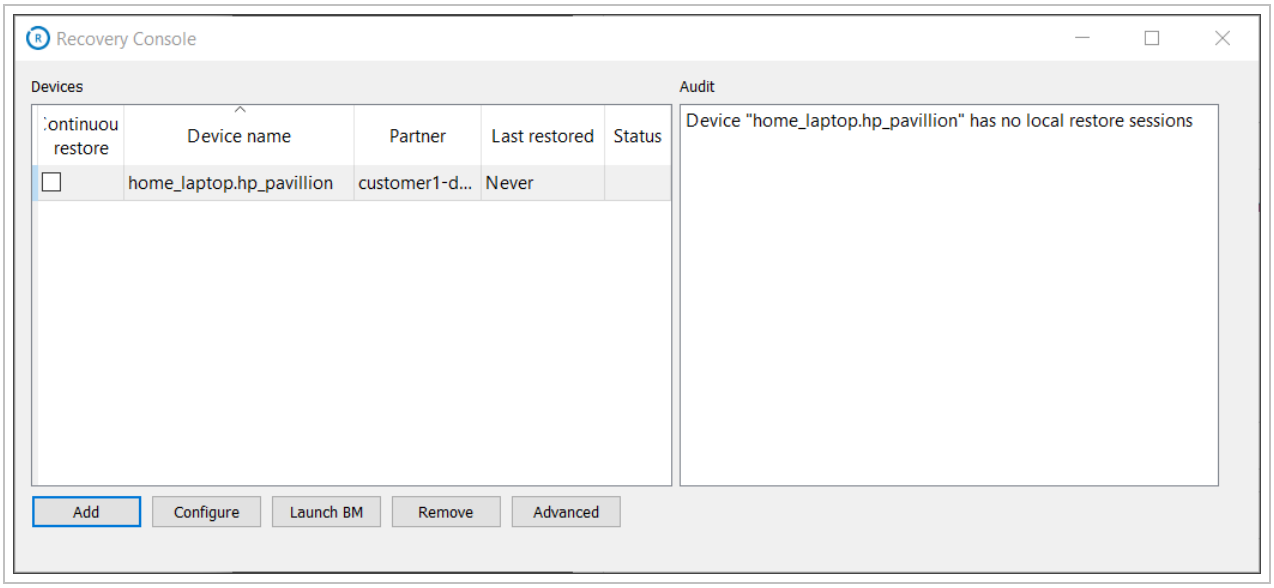
   - **Device name** - The device name as was given when Backup Manager was initially installed. This can be found on the Settings tab of the device in the Management Console.
   - **Password** - The device's Installation Key which can be found on the Settings tab of the device in the Management Console
   - **Security code** - This Is also known as the **Encryption Key** or **Passphrase** if the device was automatically installed or you have converted the device to use passphrase-based encryption.

     Device passphrases

     To find the device name, passphrase etc. for automatically installed devices, please see Getting passphrases for automatically installed devices.

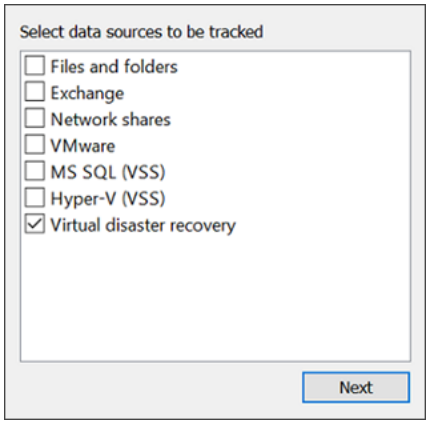
     If you do not know the Encryption Key or Security Code for a regularly installed device, you will need to retrieve this information before progressing. This can be done by converting the device to use passphrase-based encryption. See Convert devices to passphrase-based encryption for full details.

   c. Click **OK**



If the source device is already added but the Virtual Disaster Recovery source is not configured, select the device from the devices panel and then click **Configure**.

3. From the list of data sources, choose **Virtual disaster recovery**



4. From the **Restore target** list, choose the type of virtual machine you want to recover your system to

> The VDR **restore target** list is not adaptive, meaning it will show all recovery targets, even ones that are not available on the host device.

5. Fill out all settings fields for the target used

   See the Virtual Disaster Recovery Settings **page** for full details on required and optional settings for each recovery target. For example:

   Hyper-V:

Settings for device "home_laptop.hp_pavillion"

Virtual disaster recovery

Restore target HyperV

- [x] Use restore-only mode on target machine
- [x] Skip files that have not changed
- [x] Remove obsolete data from target computer
- [ ] Create only volumes that are selected for restore
- [ ] Change the FRS and DFSR services to authoritative
- [ ] Start the virtual machine after restore and take screenshot

Recover the data to a new virtual machine running on MS Hyper-V.

Restore tree

- [x] Virtual disaster recovery
  - [x] C:
  - [x] D:

HyperV role is not available on this machine: inplace HyperV restore is impossible

Access to virtual machine

Machine name

Location Browse

Virtual switch

Virtual machine properties (optional)

Boot disk size (GB)

IP address

Subnet mask

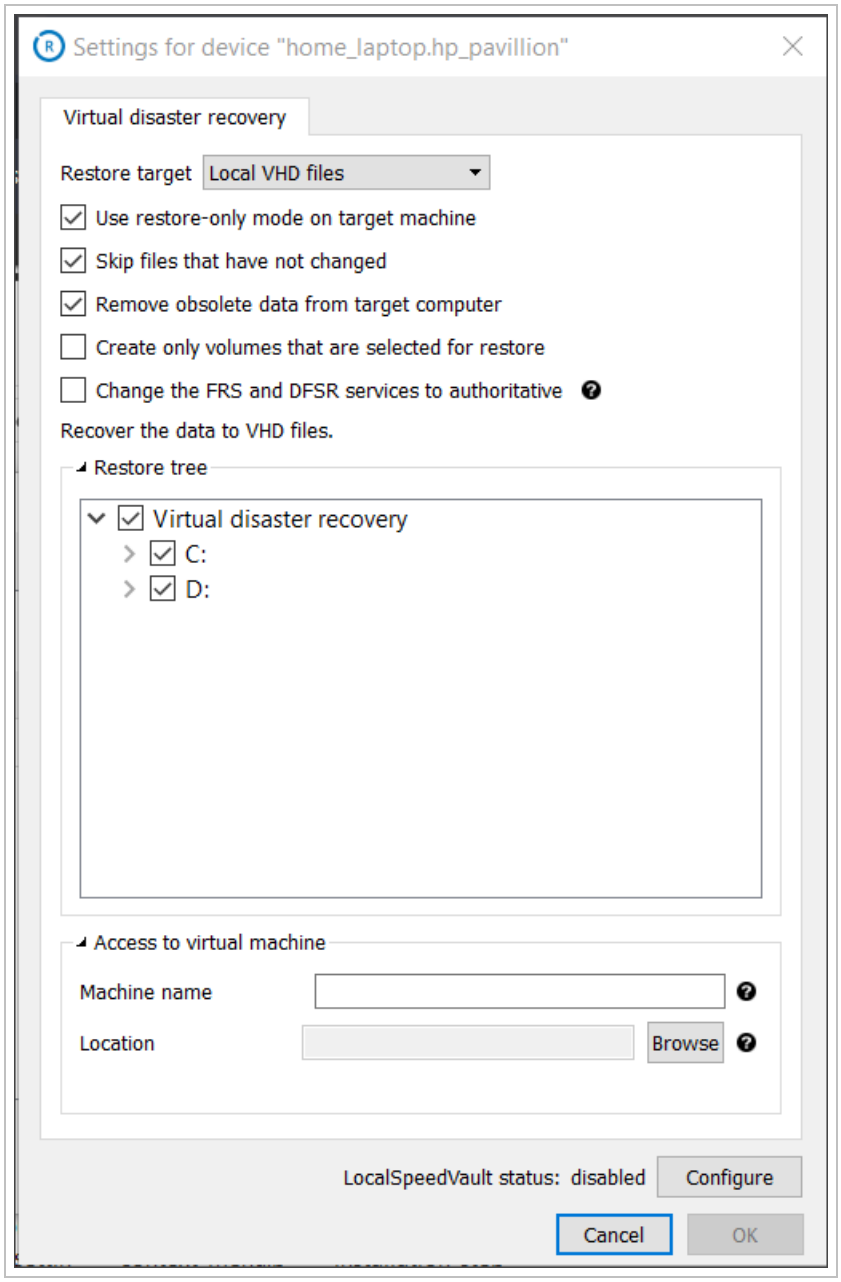
Gateway

DNS server

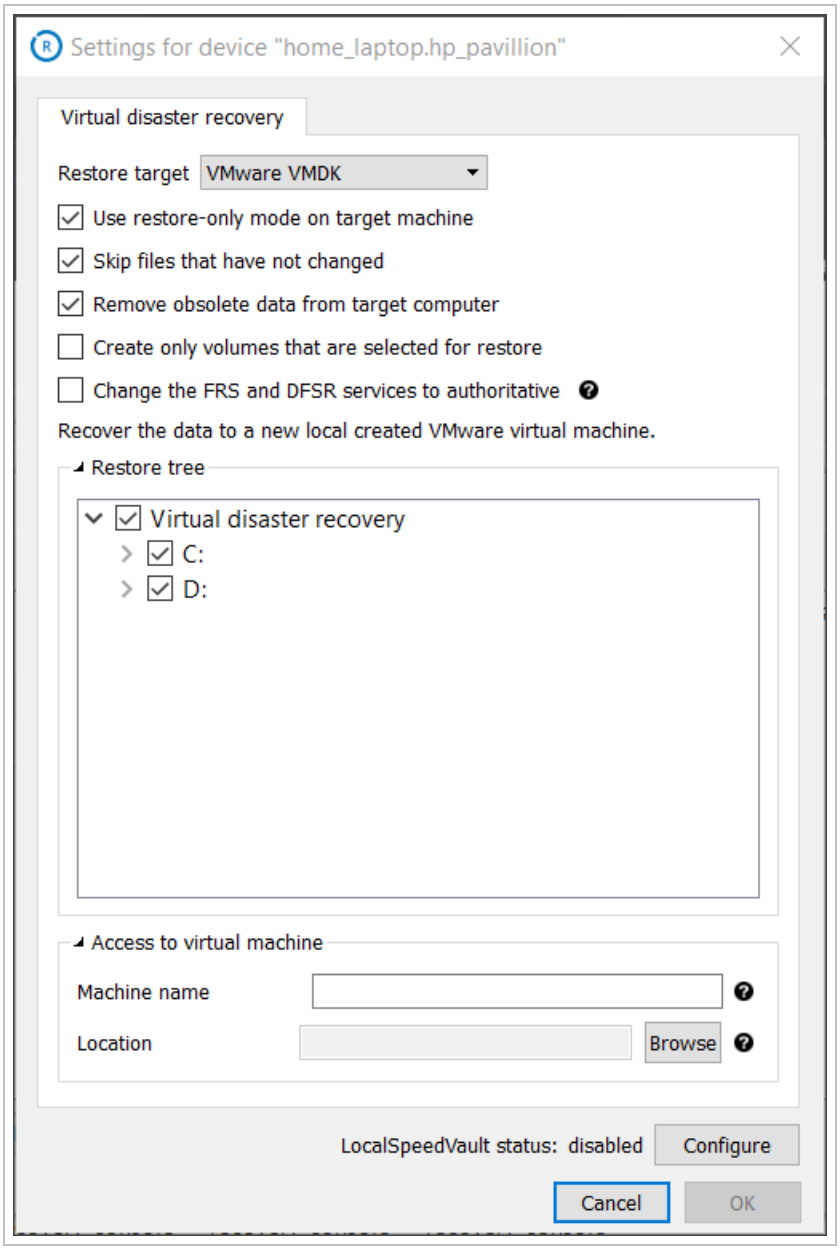
LocalSpeedVault status: disabled Configure

Cancel OK

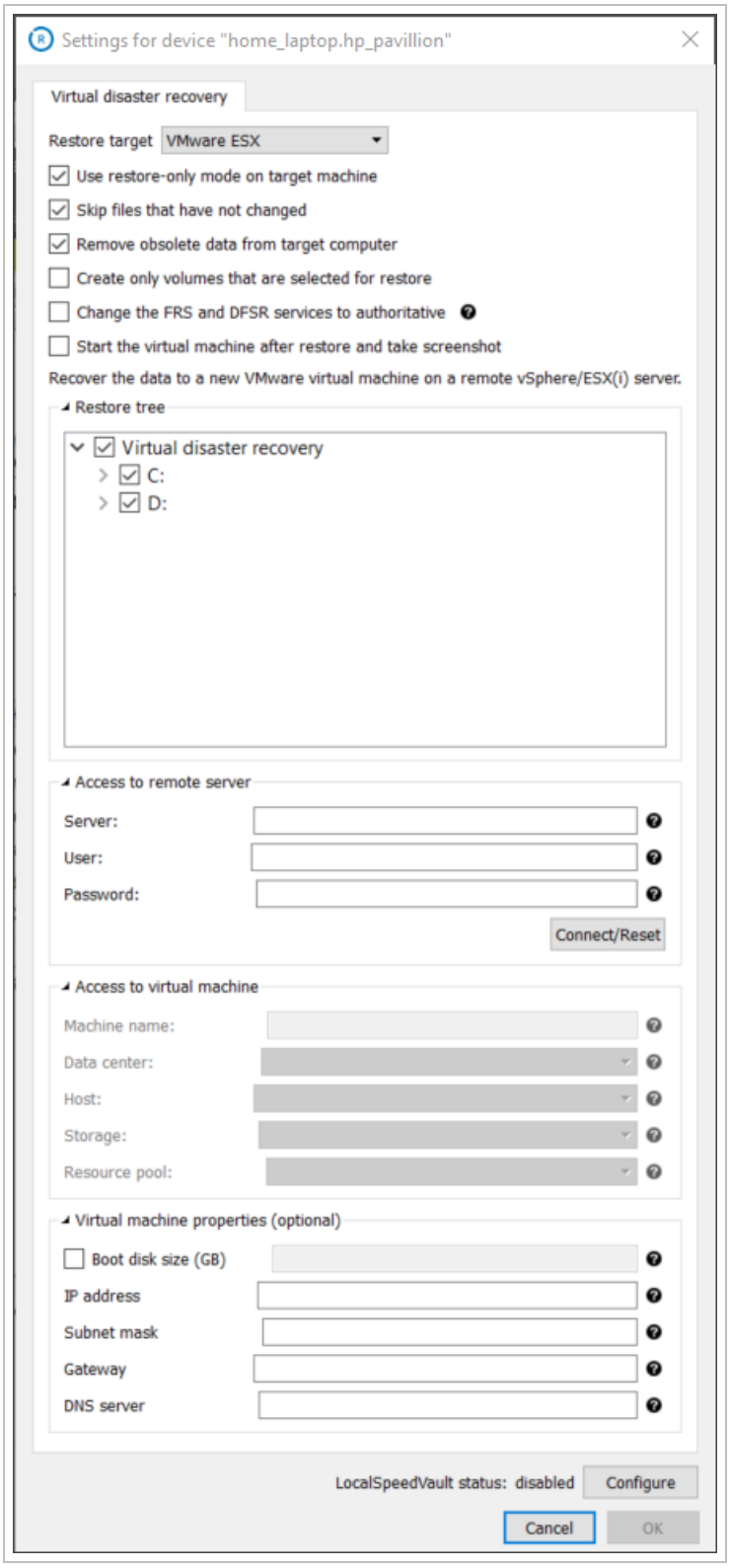
Local VHD files:



VMWare VMDK:


Settings for device "home_laptop.hp_pavillion"
Virtual disaster recovery
Restore target
VMware VMDK
Use restore-only mode on target machine
Skip files that have not changed
Remove obsolete data from target computer
Create only volumes that are selected for restore
Change the FRS and DFSR services to authoritative
Recover the data to a new local created VMware virtual machine.
Restore tree
Virtual disaster recovery
C:
D:
Access to virtual machine
Machine name
Location
Browse
LocalSpeedVault status: disabled
Configure
Cancel
OK

VMWare ESXi:


Settings for device "home_laptop.hp_pavillion"
Virtual disaster recovery
Restore target
VMware ESX
Use restore-only mode on target machine
Skip files that have not changed
Remove obsolete data from target computer
Create only volumes that are selected for restore
Change the FRS and DFSR services to authoritative
Start the virtual machine after restore and take screenshot
Recover the data to a new VMware virtual machine on a remote vSphere/ESX(i) server.
Restore tree
Virtual disaster recovery
C:
D:
Access to remote server
Server:
User:
Password:
Connect/Reset
Access to virtual machine
Machine name:
Data center:
Host:
Storage:
Resource pool:
Virtual machine properties (optional)
Boot disk size (GB)
IP address
Subnet mask
Gateway
DNS server
LocalSpeedVault status: disabled
Configure
Cancel
OK

6. Click **OK**

The Recovery Console will offer you to start data recovery for the device. Click **Yes** to continue or click **No** to add the device without recovering data (you will be able to do it any time later using the **Continuous restore** checkbox).

The length of time the recovery takes depends on the size of the system you are restoring, the data transfer speed, and the performance of your computer.

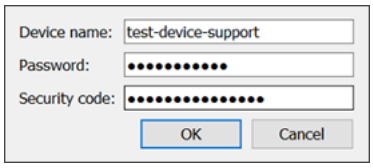
Recovery Console instructions from a specific session date or time

To perform virtual disaster recovery from a specific date or time session through the Recovery Console:

1. Start the Recovery Console on the host system.
2. If the device already exists, move to step #3. If the device is not listed, you should add it first.

   ### To add a device:

   a. Click **Add**

   b. Fill in the device details:

   - **Device name** - The device name as was given when Backup Manager was initially installed. This can be found on the Settings tab of the device in the Management Console.
   - **Password** - The device's Installation Key which can be found on the Settings tab of the device in the Management Console
   - **Security code** - This Is also known as the **Encryption Key** or **Passphrase** if the device was automatically installed or you have converted the device to use passphrase-based encryption.

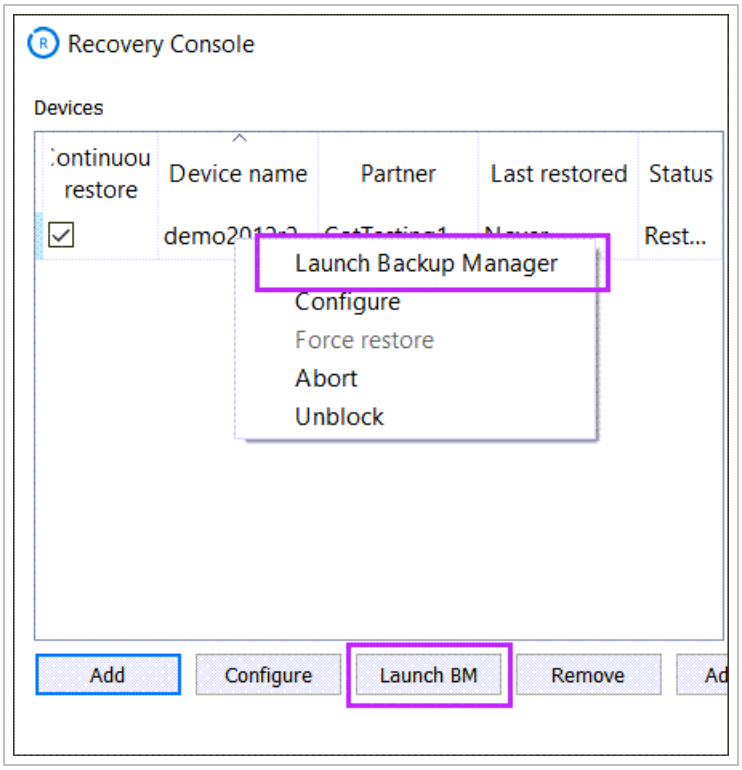
     Device passphrases

     To find the device name, passphrase etc. for automatically installed devices, please see Getting passphrases for automatically installed devices.

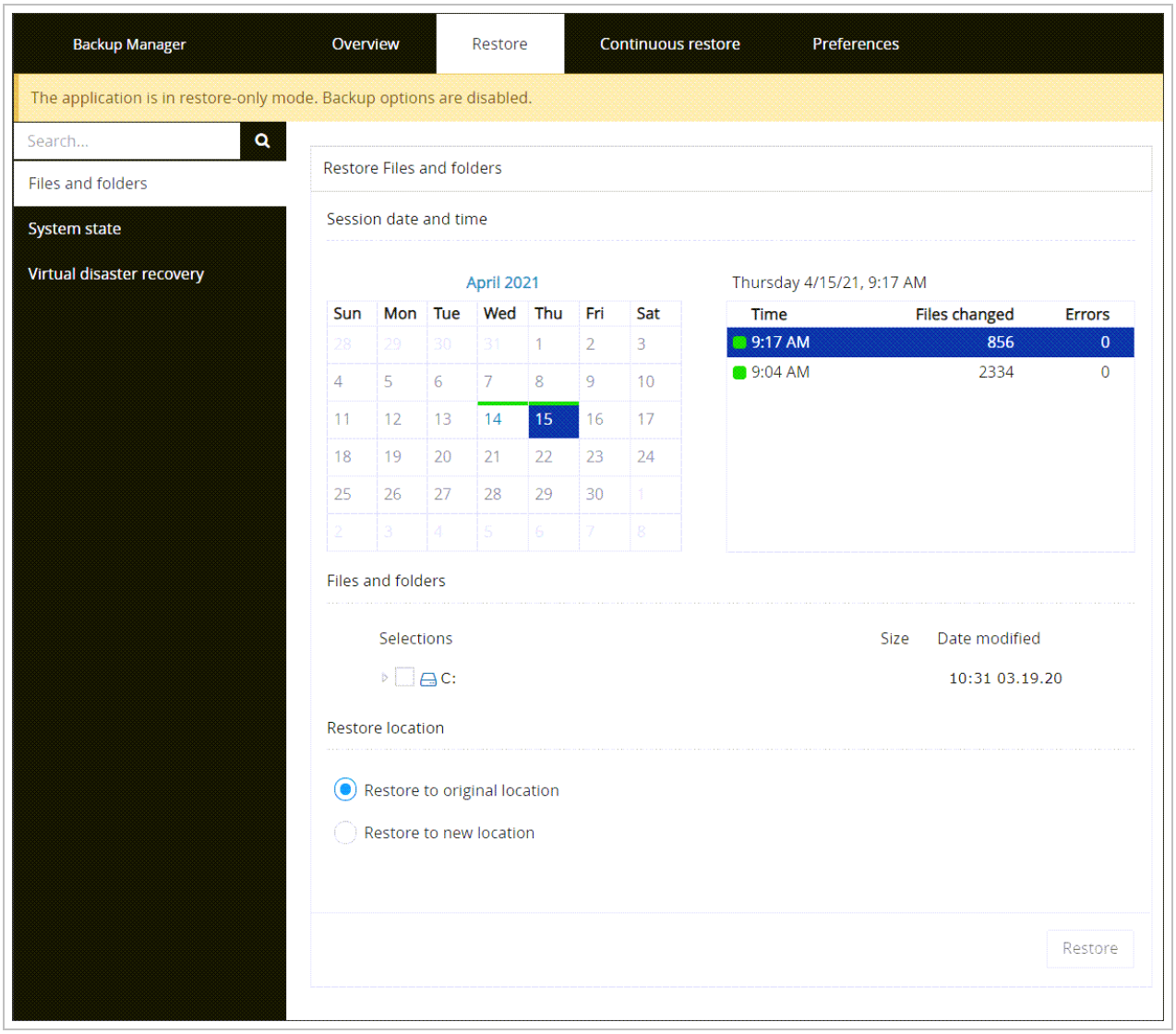
     If you do not know the Encryption Key or Security Code for a regularly installed device, you will need to retrieve this information before progressing. This can be done by converting the device to use passphrase-based encryption. See Convert devices to passphrase-based encryption for full details.

   c. Click **OK**

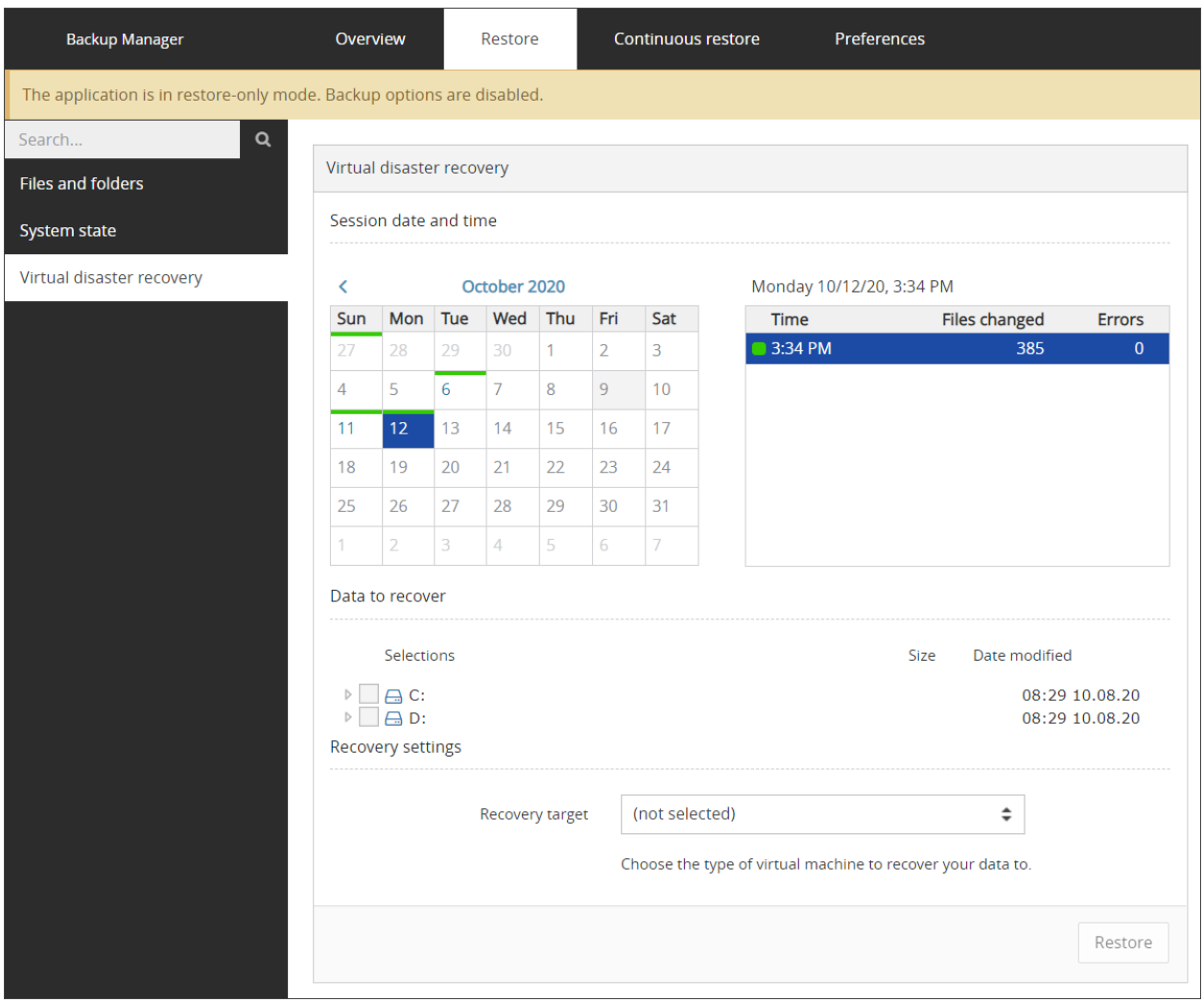
3. Highlight the device you wish to do the Virtual Disaster Recovery for and either click the **Launch BM** button or right-click and select **Launch Backup Manager**



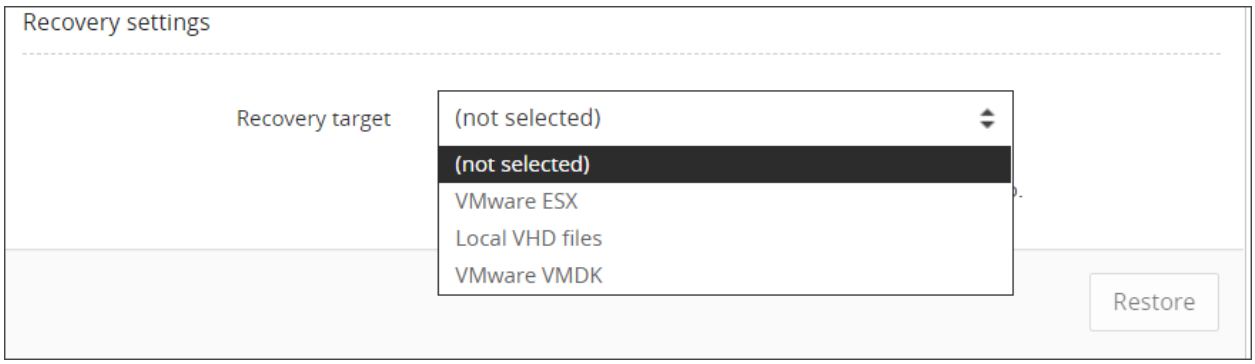
4. The device's Backup Manager will open in your browser in **Restore Only** mode, displaying a banner stating so



5. Navigate to the **Restore** tab
6. Click **Virtual Disaster Recovery** from the left hand sources list



7. Using the calendar, find the session date and time you wish to restore from
8. Select the data to recover
9. In the **Recovery Target** dropdown, select the type of target you want to recover the data to

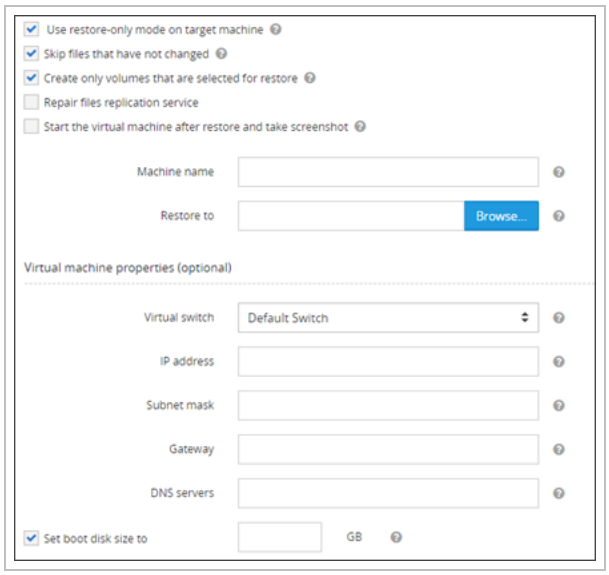


This list is adaptive, so will only show recovery targets that are available on the host device.

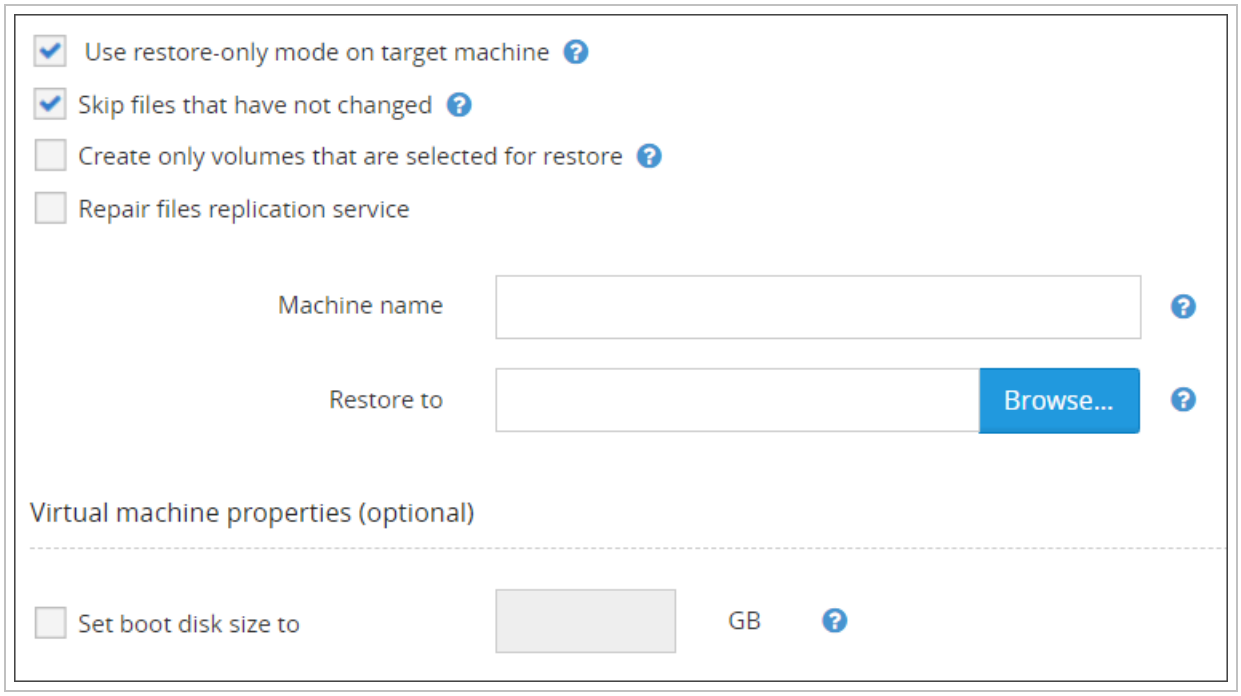
10. Fill out all settings fields for the target used

See the Virtual Disaster Recovery Settings **page** for full details on required and optional settings for each recovery target:

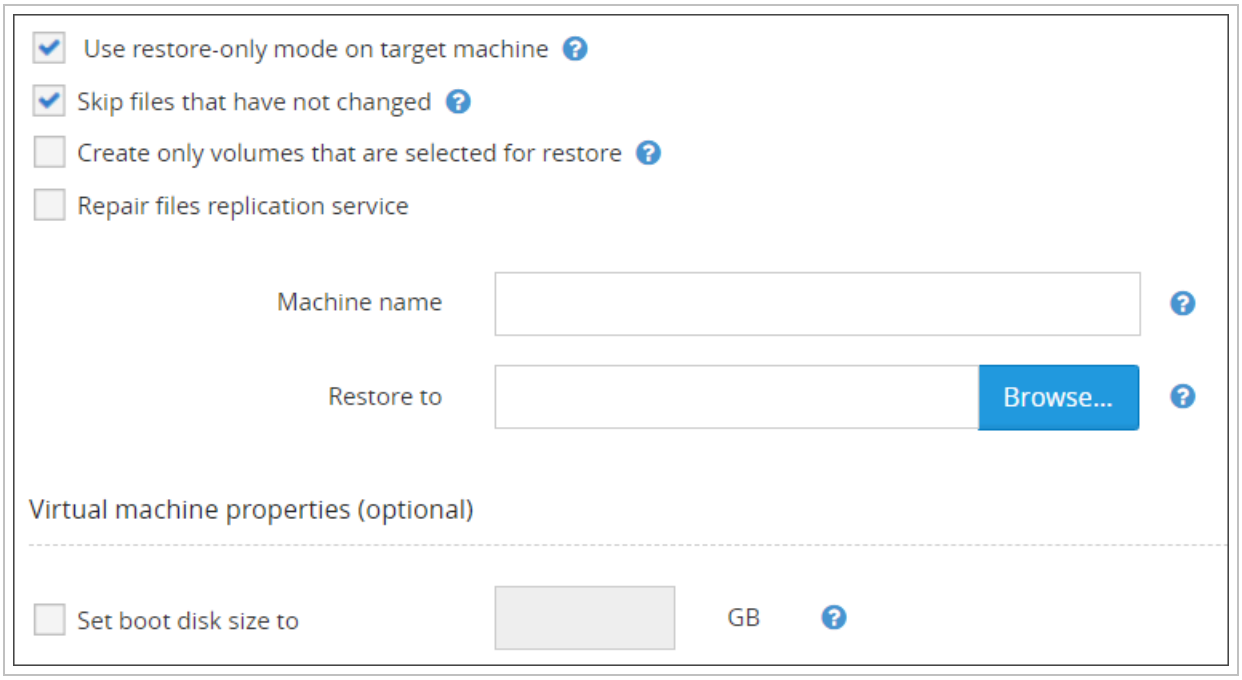
Hyper-V:



Local VHD files:



VMWare VMDK:


Use restore-only mode on target machine
Skip files that have not changed
Create only volumes that are selected for restore
Repair files replication service
Machine name
Restore to
Browse...
Virtual machine properties (optional)
Set boot disk size to
GB

VMWare ESXi:

- [x] Use restore-only mode on target machine
- [x] Skip files that have not changed
- [ ] Create only volumes that are selected for restore
- [ ] Repair files replication service
- [ ] Start the virtual machine after restore and take screenshot

Access to remote ESX server

Server address

Username

Password Connect

Access to virtual machine

Machine name

Data center Select an Option

Host Select an Option

Storage Select an Option

Resource pool Select an Option

Virtual machine properties (optional)

IP address

Subnet mask

Gateway

DNS servers

- [ ] Set boot disk size to GB

11. Click **Restore** to start a recovery process

    Once the Virtual Disaster recovery begins, you will see a banner appear tracking the restore process in the Backup Manager.

> The length of time the recovery takes depends on the size of the system you are restoring, the data transfer speed, and the performance of your computer.

Virtual disaster Recovery for Linux

> Support for Virtual Disaster Recovery on **Linux devices** has ceased.

Virtual Disaster Recovery Settings

Settings for a successful Virtual Disaster Recovery (VDR) will depend on the recovery target used.

Hyper-V, Local VHD, VMWare VMDK

The Hyper-V, Local VDH and VMWare VMDK recovery targets all share the same two required settings:

- **Machine name** - A name that you want to assign to the target virtual machine. If you keep the field blank, it will be automatically populated with the name of your backup device
- **Restore to** - Specify a path to the directory where your new virtual machine will be created

These recovery targets share the following optional settings:

- **Set boot disk size to ...** - Use this setting to customize the size to the system disk created on the virtual machine (by default, the new disk is the same size as the original)

  > If the disk contains several partitions, you cannot reduce the original size by more than the amount of free space on the last partition. For example, if the total size of the disk is 100 GB and the last partition has 10 GB of free space, you can set the value to 90 or more.

- **Use restore-only mode on target machine** - This setting helps prevent unwanted backups from running on the recovered virtual machine
- **Skip files that have not changed** - This setting can be used to optimize data recovery operations and increases recovery speed. It applies to subsequent restore sessions not the initial restore session in which the whole amount of data is transferred
- **Create only volumes that are selected for restore** - When this setting is on, the target virtual machine will contain only those disks that have data selected for recovery. When off, and no data from a disk is selected for recovery, the virtual disk is created without any data

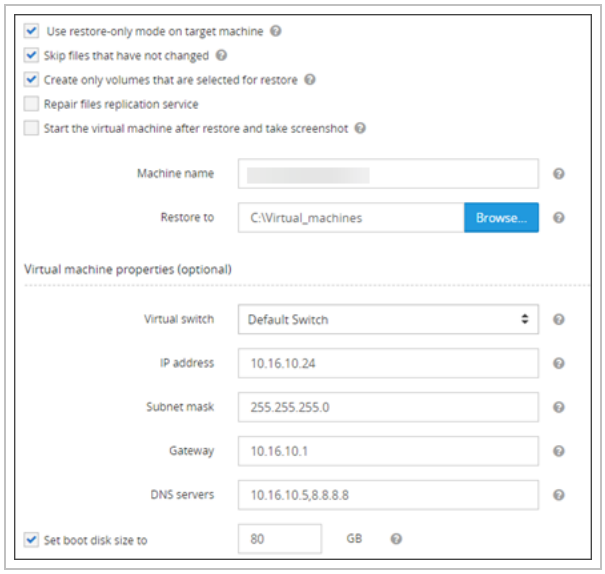
  > The setting is ignored if the disk you have excluded from recovery contains critical data. Such a thing can happen if your recovery selection includes MS Exchange or MS SQL and some files belonging to these data sources are located on the excluded disk. In this case the disk is created and populated with the files required by MS Exchange and MS SQL.

- **Repair files replication service** - If you are restoring Active Directory with multiple domain controllers, you should change the FRS and DFSR services to authoritative in the domain controller that will be started in the first place. Avoid marking several FRS/DFSR services as authoritative in the production environment as it can result in data loss. When the feature is on, the FRS and DFSR services are started on the target VM in the authoritative mode. The NETLOGON and SYSVOL shares become available, so the Active Directory and DNS services become functional again

  More information about FRS/DFSR is available in the Microsoft Knowledge Base. Article IDs: KB2218556, kbinfo KB290762.

Additional Hyper-V Optional Settings

The Hyper-V recovery target has several additional optional settings to allow for more customization:



- **Virtual machine properties** - You can assign **custom properties** to the new virtual machine:
  - **Virtual switch** - choose the Hyper-V network adapter that will be used by your new virtual machine. The selection of available adapters is detected automatically
  - **DNS servers** - assign the list of custom DNS servers (separated by comma)

    Example: `8.8.8.8` or `8.8.8.8,7.7.7.7`
  - **IP address** - assign a custom IP address to the virtual machine
  - **Subnet mask** - assign a custom subnet mask to the virtual machine
  - **Gateway** - assign a custom gateway to the virtual machine

- **Start the virtual machine after restore and take screenshot** - If the option is enabled, the new virtual machine is booted up after recovery and a confirmation screenshot is created. The results of virtual disaster recovery sessions together with screenshots of the booted systems come in email notifications (a special notification rule has to be activated by the service provider or system administrator)

  The screenshots are also available in the Management Console (see the "Virtual Disaster Recovery data session verification details (restore)" column in the **Device Management** module)

Important: Use the feature carefully if there is another virtual machine in the local network offering the same services (for example, the Active Directory) as it can result in a conflict with subsequent data loss.

VMWare ESXi

The VMWare EXSi recovery target has different required and optional settings to the others:

- [x] Use restore-only mode on target machine
- [x] Skip files that have not changed
- [ ] Create only volumes that are selected for restore
- [ ] Repair files replication service
- [ ] Start the virtual machine after restore and take screenshot

Access to remote ESX server

Server address: server-address.here

Username: username1

Password: ••••••••• Connect

These settings will not become available until you connect to the server

Machine name: test-lab-b2

Data center: Select an Option

Host: Select an Option

Storage: Select an Option

Resource pool: Select an Option

Virtual machine properties (optional)

IP address:

Subnet mask:

Gateway:

DNS servers:

- [ ] Set boot disk size to GB

Required settings

There are two sections of the VMWare EXSi setup which require configuration:

1. **Access to remote ESXi server** – Enter your vSphere/ESXi server access credentials to let the recovery software access the server and create a virtual machine there
   - **Server Address** - The address to the vSphere/ESXi server
   - **Username** - The administrator login username
   - **Password** - The administrator login password
2. **Access to virtual machine** – You must assign a name to the new virtual machine. The rest of the settings are retrieved automatically after a connection to the server is established. Where options are available, you will be able to choose a suitable one from a dropdown list

Optional settings

The VMWare ESXi recovery target has the following optional settings which may be configured:

- **Set boot disk size to ...** - Use this setting to customize the size to the system disk created on the virtual machine (by default, the new disk is the same size as the original)

  > If the disk contains several partitions, you cannot reduce the original size by more than the amount of free space on the last partition. For example, if the total size of the disk is 100 GB and the last partition has 10 GB of free space, you can set the value to 90 or more.

- **Use restore-only mode on target machine** - This setting helps prevent unwanted backups from running on the recovered virtual machine
- **Skip files that have not changed** - This setting can be used to optimize data recovery operations and increases recovery speed. It applies to subsequent restore sessions not the initial restore session in which the whole amount of data is transferred
- **Create only volumes that are selected for restore** - When this setting is on, the target virtual machine will contain only those disks that have data selected for recovery. When off, and no data from a disk is selected for recovery, the virtual disk is created without any data

  > The setting is ignored if the disk you have excluded from recovery contains critical data. Such a thing can happen if your recovery selection includes MS Exchange or MS SQL and some files belonging to these data sources are located on the excluded disk. In this case the disk is created and populated with the files required by MS Exchange and MS SQL.

- **Repair files replication service** - If you are restoring Active Directory with multiple domain controllers, you should change the FRS and DFSR services to authoritative in the domain controller that will be started in the first place. Avoid marking several FRS/DFSR services as authoritative in the production environment as it can result in data loss. When the feature is on, the FRS and DFSR services are started on the target VM in the authoritative mode. The NETLOGON and SYSVOL shares become available, so the Active Directory and DNS services become functional again

  > More information about FRS/DFSR is available in the Microsoft Knowledge Base. Article IDs: KB2218556, kbinfo KB290762.

- **Start the virtual machine after restore and take screenshot** - If the option is enabled, the new virtual machine is booted up after recovery and a confirmation screenshot is created. The results of virtual disaster recovery sessions together with screenshots of the booted systems come in email notifications (a special notification rule has to be activated by the service provider or system administrator)

  > The screenshots are also available in the Management Console (see the "Virtual Disaster Recovery data session verification details (restore)" column in the **Device Management** module)

  > Important: Use the feature carefully if there is another virtual machine in the local network offering the same services (for example, the Active Directory) as it can result in a conflict with subsequent data loss.

Continuous Restore for Virtual Disaster Recovery

Virtual Disaster Recoveries can be performed **on request** or set it to the **Continuous Restore** mode where data recovery is synchronous with backups performed in the source system.

Requirements

> The Continuous Restore requires a dedicated computer or virtual machine that must not be used for other purposes (learn more).

Device passphrases

To find the device name, passphrase etc. for automatically installed devices, please see Getting passphrases for automatically installed devices.

If you do not know the Encryption Key or Security Code for a regularly installed device, you will need to retrieve this information before progressing. This can be done by converting the device to use passphrase-based encryption. See Convert devices to passphrase-based encryption for full details.

Enabling the Continuous Restore mode

Continuous Restore can be enabled either in Recovery Console or by installing Backup Manager in restore-only mode. Information on configuring this from Backup Manager can be found here: Continuous restore in Backup Manager.

Recovery Console instructions

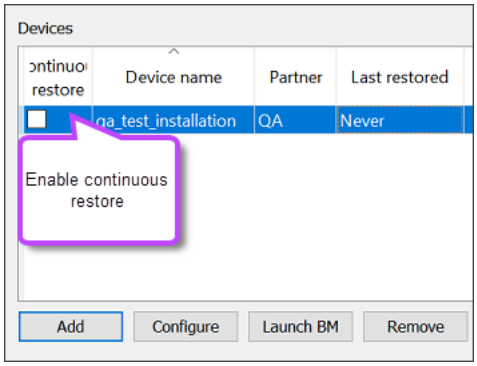
> This can be found from the Downloads page in Management Console, or from the Backup Downloads page on our website.

The Continuous Restore mode[1] is the predefined option in the Recovery Console. You can manage the setting for each device through the **Continuous Restore** checkbox to the left of each device name.

1. Add the device to the Recovery Console following these steps
2. Once the device has been added and configured correctly, tick **Continuous Restore** which can be found to the left of the device name in the Devices panel

---

[1]Repeated data recovery to a computer or virtual machine that is specifically allocated for that purpose. The recovery is synchronous with backups performed in the source system.



3. The Virtual Disaster Recovery will now begin running in Continuous Restore mode. If you need to amend any settings, this can be done by launching Backup Manager for the device and changing settings from **Continuous restore > Virtual disaster recovery**

> If you click 'Launch BM' before configuring continuous restore as above, you will find the content of the tab is greyed out and you cannot make any changes. Enable continuous restore first before launching the Backup Manager client.

Using virtual machines in-between restore sessions

The target virtual machine **is not supposed to be in use** while the Continuous Restore mode is active. If your recovery software detects that the virtual machine was started in-between restore sessions, further restores **are blocked** and a warning message appears. This is done to prevent possible data loss.

Unblocking the Continuous Restore

There are several ways to **unblock the Continuous Restore process:**

1. Click the **Unblock** button in the warning message
2. In Backup Manager, go to **Continuous restore > Virtual disaster recovery** and then click **Restore**. This will initiate a quick delta restore that will overwrite the changes at the target location (if any)
3. In the Recovery Console, right-click the device and choose **Unblock** from the context menu

After this is done, the continuous restore process will be fully functional again.

> If the virtual machine may contain changes that you want to keep, please make a copy of it before you unblock the Continuous Restore mode.

Disabling virtual machine checks

The recovery software checks if the virtual machine has been in use before each virtual disaster recovery session. If you are sure no important data is added to the virtual machine, you can **disable these checks** and have the previous version overwritten without warning messages. To do it, add `VdrRestorePolicyForceOverwrite=1` to the `[General]` section of the configuration file belonging to your recovery software.

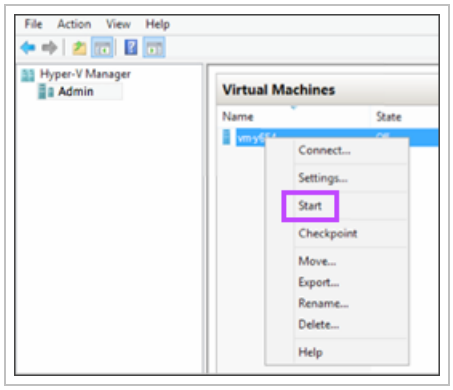
- Backup Manager instructions
- Recovery Console instructions

> The setting applies to **all** backup devices installed on the current computer (one device for the Backup Manager or multiple devices for the Recovery Console).

Hyper-V Post Virtual Disaster Recovery

Once you have completed the Virtual Disaster Recovery Instructions and the recovery process has completed for the Hyper-V Virtual Disaster Recovery, you can boot the virtual machine.

1. Open the Hyper-V Manager
2. Right-click on the new virtual machine (its name will coincide with the name you gave it during configuration, or that of the backup device if no name was given)
3. Choose **Start** from the context menu



VMWare VMDK Post Virtual Disaster Recovery

The **VMWare VMDK files** created by the Virtual Disaster Recovery have the "VMWare workstation 8" format. Such files cannot be copied to the ESXi.

Before these can be used, they must be converted to an appropriate format using a VMWare Converter.

Please see the VMWare documentation for details.

Glossary of Cove Data Protection (Cove) terms

Additional Services

Within this section, you will find information and instructions on using and managing your own storage devices, and information on using JSON-RPC API with Cove Data Protection (Cove). You can also find information about our legacy tool, Cloud Management Console here.

What's inside:

Storage management guide

Cove Data Protection (Cove) has two partnership models to choose from. They are based on storage ownership:

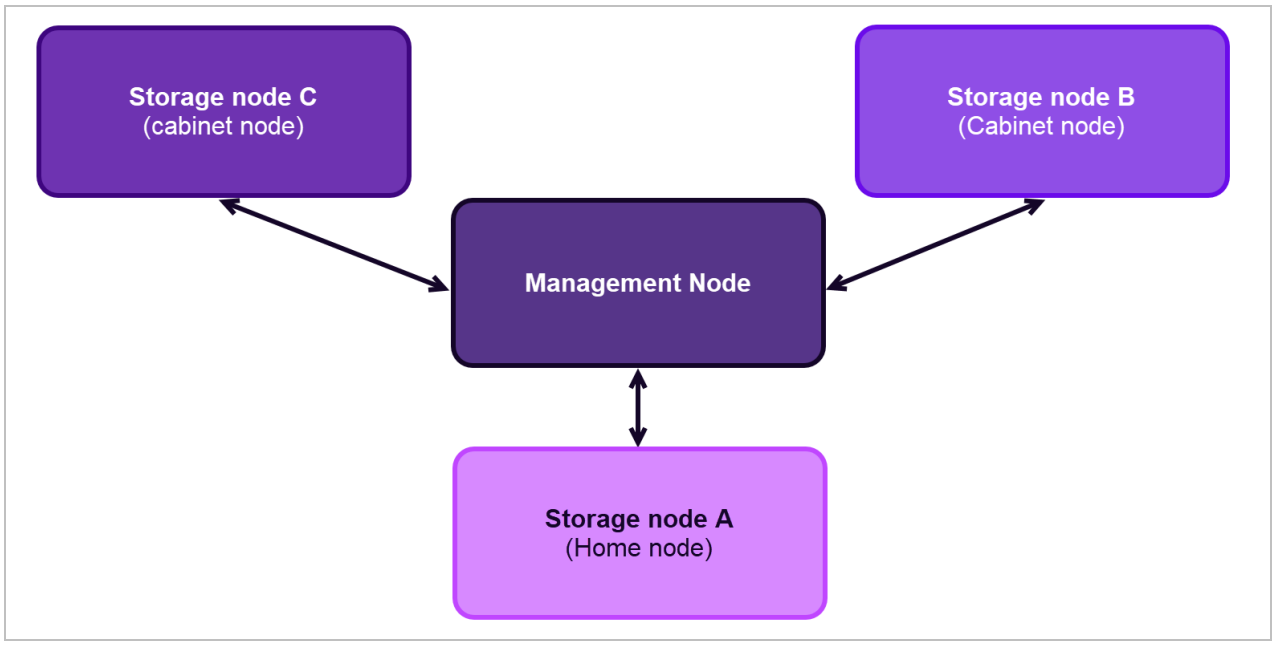
1. **All-inclusive** - We provide storage for customers using this model and it is taken care of by the service provider
2. **Software-only** - Customers who are subscribed on the "software-only" basis manage their own storage

The current guide helps software-only customers maintain their storage.

> We recommend updating all storage node software to version **18.3**. This is necessary to avoid conflicts with devices running backup software version 18.4 or higher. As a result of these conflicts, the statuses of some backup sessions may be displayed incorrectly (e.g. "Undefined" instead of "Skipped").

Cloud structure

The Cloud is organized as a set of **storage servers** and a **management server**. In the software and supporting documentation these servers are referred to as **nodes**.



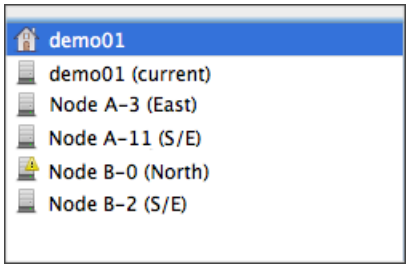
The **management node** is the primary component in the Cloud structure. It distributes data among the storage nodes so that the data is available for recovery at any time. Storage nodes do not communicate with each other directly but do so through the management node. The management node is always maintained by the service provider.

Storage nodes contain backup data from Backup Manager devices. Although storage nodes can differ in their hardware and software characteristics, technically they are all equal and interchangeable. Data from a device may be spread over several storage nodes. Also if a storage node becomes unavailable, another one will take its place.

Functions of a node

A storage node can function in one (or in both) of the following ways in relation to a device:

1. **Home node** - The home node stores the Backup Register (a journal with the list of all files and directories that have been backed up). Another copy of the Backup Register is available on the client machine
2. **Cabinet node** - The cabinet node stores backup data distributed into cabinets for faster transfer. You can learn how cabinets are created on the backup technology page



The same node can function as a home node for some devices and as a cabinet node for others.

States of a node

A storage node can have one of the following states:

- **Online/Operable** - The node is used for storage
- **Offline/Temporary not available** - The node has been disabled for a short period of time (usually several hours). In Backup Manager versions before 16.5 (released in May 2016), the state will be automatically reset within the next 24 hours unless the storage node service has been stopped. If other nodes are available, backup activities continue running to the other available nodes. Data recovery from the node is usually possible in this state
- **Offline/Out of service** - The node has been discontinued/decommissioned and is no longer used for storage. This can be a temporary or a permanent condition. If other nodes are available, backup activities continue running to the other available nodes. Recovery options for **all devices** that have all or some of their data on the node are blocked. For this reason, it is necessary to migrate the node to new hardware before setting its state to **Out of service**

Requirements and recommendations

Supported operating systems

GNU/Linux	FreeBSD	Windows
All versions (kernel 2.6.16+, GLIBC 2.4+ with NPTL)	Minimum v12	▪ Windows 8 / 8.1 ▪ Windows 10

GNU/Linux	FreeBSD	Windows
		▪ Windows 11 ▪ Windows Server 2012 / 2012 R2 (limited[1]) ▪ Windows Server 2016 (limited[2]) ▪ Windows Server 2019 (limited[3]) ▪ Windows Server 2022 (limited[4]) **Recommended:** Windows Server 2012 R2, 2016, 2019 and 2022

Supported file system types

The file system must be **physical storage**, connected as local storage or via an ISCSI target. **Network-based** file systems such as NFS, AFS or SMB are not suitable for storage node installation.

The following file system types are recommended:

- Windows: NTFS
- FreeBSD: ZFS RAIDZ-2
- Linux: ext4 or ZFS

Storage Node Installer version

The storage node software must be **compatible** with the versions of backup devices hosted on it. Due to some major structural changes released at the beginning of 2017, backup devices running Backup Manager 17.0 or greater must have storage node software version 17.0 or greater. At the same time, devices powered by the older versions of the Backup Manager work well both on 16x and 17x storage nodes.

Recommended number of storage nodes

If your company has chosen to use private storage, you need to install **several storage nodes** to get started. If one of them becomes unavailable, its functions will be automatically transferred to another node so backups will continue running and the data will stay available for recovery.

Hardware recommendations

To create a storage node, you need a server with enough esources.

- 2+ TB of free hard disk space (depends on the amount of data intended for backup as well as its retention period);
- 2+ GB of RAM plus 1 extra GB for each additional TB of data.

---

[1]New features such as Docker-based containers, Storage Spaces Direct and Shielded VMs are not.

[2]Only the features compatible with Windows Server 2012 R2 are supported.

[3]Only the features compatible with Windows Server 2012 R2 are supported.

[4]Only the features compatible with Windows Server 2012 R2 are supported.

> If the amount of free space on a storage node goes below the default of **200 GB**, the node status changes to "Full". It becomes impossible to create new devices on this node. All new backup data is redirected to free storage nodes. As older sessions are cleared according to the retention policy, some storage space frees up automatically. When the amount of free space reaches **300 GB** (by default), the node status returns to "Free".

Storage virtualization recommendations

We recommend using the RAID storage virtualization technology.

Clusters

It is possible to use a SAN Cluster as a storage node. It must use ISCSI protocol.

Custom SSL Certificates

It is possible to use custom SSL certificates for software-only partner storage nodes.

1. Create a valid SSL certificate, for example with Comodo or Verisign
2. Create a `server.key` file
   - Put the private key of the new certificate into this file
3. Merge domain certificate with CA bundle into a single `server.crt` file
   - For Windows storage nodes:
     a. Copy `server.crt` and `server.key` to `C:\Program Files\CloudStorageNode\nginx\conf`, replacing existing files
     b. Restart **Cloud Storage Node Monitor** service to apply changes
   - For Linux storage nodes:
     a. Copy `server.crt` and `server.key` to `/opt/iaso-cloud/etc/nginx/ssl`, replacing existing files
     b. restart the services with this command in terminal:

```
sudo /etc/init.d/CloudStorageController restart
```

Generate Certificate Signing Request (CSR) for SSL certificates

Use the below steps to make the needed change:

1. Open command prompt with administrator privileges and run the following commands (changing subj and domain in CN value with your information)

```
cd C:\Program Files\CloudStorageNode
set OPENSSL_CONF=C:\users\remote\Documents\openssl.cnf.txt

openssl.exe req -sha256 -new -newkey rsa:2048 -nodes -subj
"/C=US/ST=NC/L=Durham/O=LogicNowLimited/CN=backup01.company.com" -keyout
"C:\Program Files\CloudStorageNode\nginx\conf\new.server.key" -out
"C:\Program Files\CloudStorageNode\nginx\conf\new.server.csr"
```

   Check and confirm result CSR file with following execute:

```
openssl.exe req -in "C:\Program
Files\CloudStorageNode\nginx\conf\new.server.csr" -noout -text
```

2. Certificate from the CA should have PEM format. If intermediate certificates should be specified in addition to a primary certificate, they should be specified in the same file in the following order: The primary certificate comes first, then the intermediate certificates. Then you get certificate:
   a. Rename `C:\Program Files\CloudStorageNode\nginx\conf\server.key` to `C:\Program Files\CloudStorageNode\nginx\conf\old.server.key`
   b. Rename `C:\Program Files\CloudStorageNode\nginx\conf\new.server.key` to `C:\Program Files\CloudStorageNode\nginx\conf\server.key`
   c. Rename `C:\Program Files\CloudStorageNode\nginx\conf\server.crt` to `C:\Program Files\CloudStorageNode\nginx\conf\old.server.crt`
   d. Put new certificate into the `C:\Program Files\CloudStorageNode\nginx\conf\server.crt`

```
cd C:\Program Files\CloudStorageNode\nginx
```

```
nginx.exe -t
```

   e. Output "nginx: the configuration file C:\Program Files\CloudStorageNode\nginx/conf/nginx.conf syntax is ok" will confirm that new certificate set correctly
3. Restart 'Clout Storage Node Monitor' service

Storage node installation instructions

Please follow instructions relevant to your operating system.

- Install storage node on Linux
- Install storage node on Windows

Storage Node Installers are available in the **Downloads** section of the Management Console. They can also be downloaded from here.

Install storage node on Linux

Storage Node Installers are available in the **Downloads** section of the Management Console. They can also be downloaded from here.

1. Download the **Storage Node Installer** for Linux
2. Open your terminal emulator and set executable rights for the script:

```
root# chmod +x mxb-cloud-sn-linux-x86_64.run
```

3. Launch the script. You can run a **general command** as shown in the example below. In this case you will be asked to provide some settings at the next step (the system will prompt you to enter them one at a time):

```
root# ./mxb-cloud-sn-linux-x86_64.run
```

4. Alternatively, you can **enter these settings** straight away and skip further questions. This is convenient if you have multiple storage nodes to install. This installation method is also more flexible for options as it supports an extra set of parameters. The installation command will look as follows:

```
root# ./mxb-cloud-sn-linux-x86_64.run -- -installation-mode install -cloud-
partner-name 'Smart Telecom' -cloud-partner-user-name root@email.com -cloud-
partner-user-password 029HgatEoauba1 -storage-name 'Primary' -storage-
directory /opt/mxb/storage -storage-node-name 'Smart Telco Node 3' -nginx-
bind-host 192.168.0.222 -nginx-bind-port 443 -external-addresses
'192.168.0.222:443' -web-rcg-bind-host 192.168.0.222 -web-rcg-bind-port 2999
-web-rcg-external-addresses '192.168.0.222:2999'
```

> When setting up the storage node, you must use the email address. You can use the email associated to the root account or you can create a separate user account specifically for use by the Storage node.

> When installing storage nodes, please be aware that you **must use IPv4** as IPv6 is not supported.

5. Submit the remaining installation parameters (if applicable)
6. Review the settings you have submitted. Enter `Y` (Yes) if everything is correct or enter `N` (No) to start over:

```
Please review all the information once again:
==============================================================
Storage directory:          /opt/mxb/storage
--------------------------------------------------------------
Cloud address:              cloudbackup.management:443
Cloud partner name:         Smart Telecom
Cloud user:                 root@email.com
Cloud password:             ********
--------------------------------------------------------------
Storage name:               Primary
Storage node name:          Smart Telco Node 3
--------------------------------------------------------------
```

```
NGINX bind address:         192.168.0.222:443
External addresses:         192.168.0.222:443
RCG bind address:           192.168.0.222:1999
RCG external address:       192.168.0.222:1999
Web RCG bind address:       192.168.0.222:2999
Web RCG external addresses: 192.168.0.222:2999
============================================================
Is everything correct? (Y/n) Y
```

When the installation is complete, the new node will appear among the partner's nodes

To view it in the Cloud Management Console, open the **Manage** menu, and then click **View storage statistics**.

If you need any help with the installation, please contact our support team.

Installation parameters

Required parameters

Parameter	Definition
`-installation-mode`	The action you want to perform: ▪ `install` (install a new storage node or update an existing one) ▪ `upgrade` (upgrade from FTP storage to a cloud storage node)
`-cloud-partner-name`	The name of the partner company you are installing the storage node for (can be copied from your cloud management software)
`-cloud-partner-user-name`	The email address of the user from the partner company who has full access to Customer Management in your cloud management software. The SuperUser role is required.
`-cloud-partner-user-password`	The password associated with `-cloud-partner-user-name`.
`-storage-name`	The name of the storage pool where the new node will be located. Use `Primary` to enable the default storage assigned to the partner company. If you enter a new name, the storage pool will be created automatically.
`-storage-directory`	A path to the directory where backup data will be stored. Use `/opt/mxb/storage` to enable the default directory assigned to the partner or type in your own directory.
`-storage-node-name`	The name you want to assign to the new storage node

Parameter	Definition
`-nginx-bind-host`	The internal IP address of the Nginx server that will be used to upload cabinets to the storage node. Enter `0.0.0.0` if you want the system to choose an available IP address automatically or type in your own IP address.
`-nginx-bind-port`	The port number of the Nginx server. The default port is `443`.
`-external-addresses`	The external IP address and port number of the Nginx server. If the Backup Manager is installed in the same network as the storage node, you can speed up data transfer by entering **several addresses**. Use a comma or a semicolon to separate them, for example `192.168.0.222:443;192.168.0.333:443`. Spaces between values are optional. Avoid using the same external IP address for two or more servers in a local network (it can result in connectivity issues).
`-web-rcg-bind-host`	The internal IP address of the web RCG server that will be used to establish remote connections to the partner's devices. Use `0.0.0.0` to let the system accept connections on all available network interfaces or specify your own host.
`-web-rcg-bind-port`	The internal port number of the web RCG server. `2999` is the default port.
`-web-rcg-external-addresses`	The external IP address and port number of the web RCG server. You can enter several addresses separated by a comma or a semicolon. Spaces between values are optional.

Optional parameters

Parameter	Definition
`-skip-questions`	Lets you skip the final review of the settings submitted. Enter the parameter without any values to enable the feature.
`-no-web-rcg`	Lets you skip entering remote connection settings: `-web-rcg-bind-host`, `-web-rcg-bind-port` and `-web-rcg-external-addresses`. Remote connections to backup clients **will be unavailable** without these settings. The parameter requires Storage Node Installer **16.2** or a greater version.
`-install-path`	A path to the storage node software installation (set to `/opt/mxb` by default)
`-auth-user`	A login name that the Backup Manager will use for basic HTTP authentication when communicating with the new storage node. If no name is set, a default value will be used (`data`).
`-auth-password`	A password that the Backup Manager will use for basic HTTP authentication when communicating with the new storage node. If no value is set, a random password will be generated.

Parameter	Definition
`-no-state-reporting`	Lets you disable storage node disk usage statistics submission to the management node. Enter the parameter without any values to enable the feature.

Remote connection settings for legacy backup clients

If your storage node hosts devices running Backup Manager version 13x, you can configure remote connection settings for these devices.

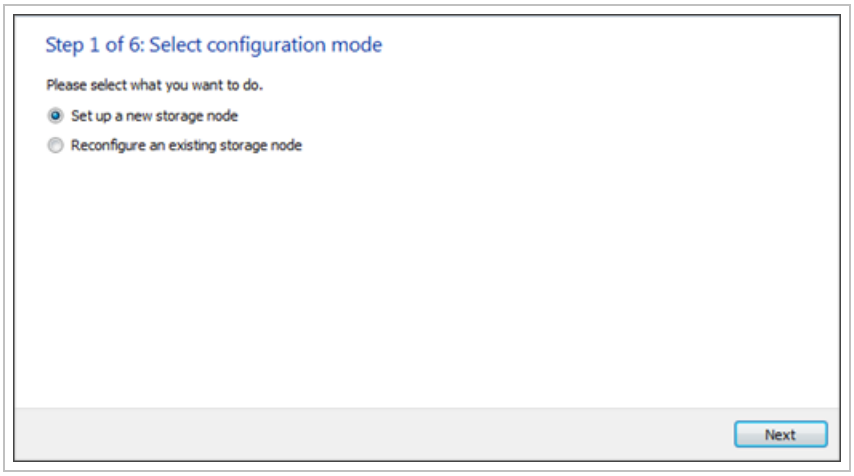
Parameter	Definition
`-rcg-bind-host`	The internal IP address of the RCG server that will be used to establish remote connections to legacy devices. Use `0.0.0.0` if you want the system to accept connections on all available network interfaces or specify your own IP address.
`-rcg-bind-port`	The internal port number of the RCG server. `1999` is the default port.
`-rcg-external-host`	The external IP address of the RCG server. You can use the same IP address that you provided in `-external addresses`.
`-rcg-external-port`	The external port number of the RCG server. `1999` is the default port.
`-no-rcg`	Lets you skip entering remote connection settings for legacy backup clients: `-rcg-bind-host`, `-rcg-bind-port`, `-rcg-external-host`, and `-rcg-external-port`. Remote connections to legacy backup clients **will be unavailable** without these settings. The parameter requires Storage Node Installer **16.2** or a greater version.

Install storage node on Windows

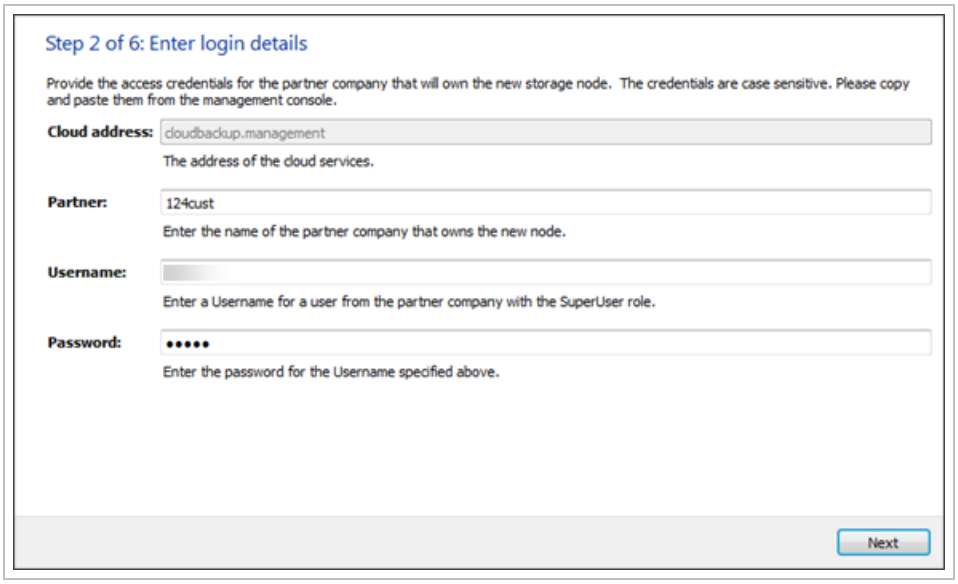
Storage Node Installers are available in the **Downloads** section of the Management Console. They can also be downloaded from here.

Download the Storage Node Installer for Windows and follow a set-up wizard.

1. Choose **Set up a new storage node**

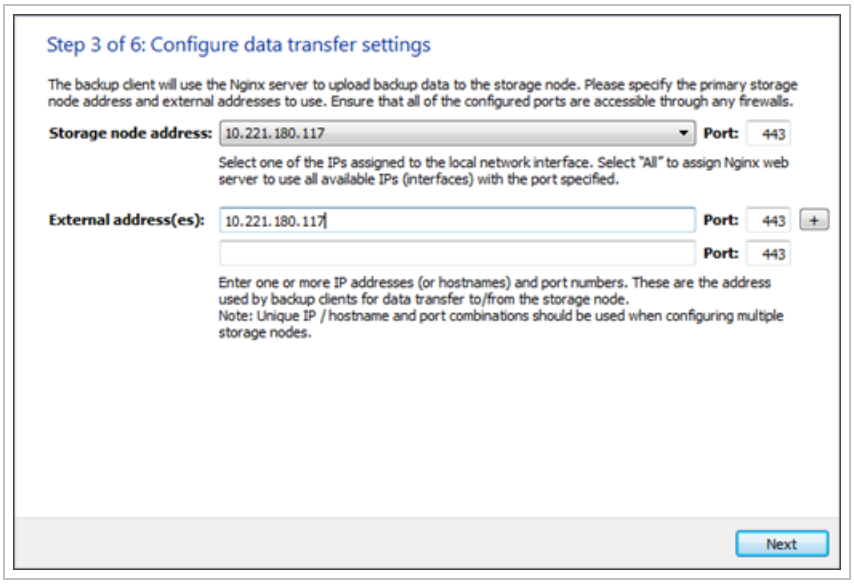


2. Enter your login credentials for access to the cloud, an account with the SuperUser role is required



> When setting up the storage node, you must use the email address in the **Username** field. You can use the email associated to the root account or you can create a separate user account for use by the Storage node.

3. Select the IP address you want to use for the storage node. You can enter the same IP address to the **External address(es)** field. If the external address differs from the primary storage node address, it should forward incoming traffic there (this is achieved with the help of a network adapter)

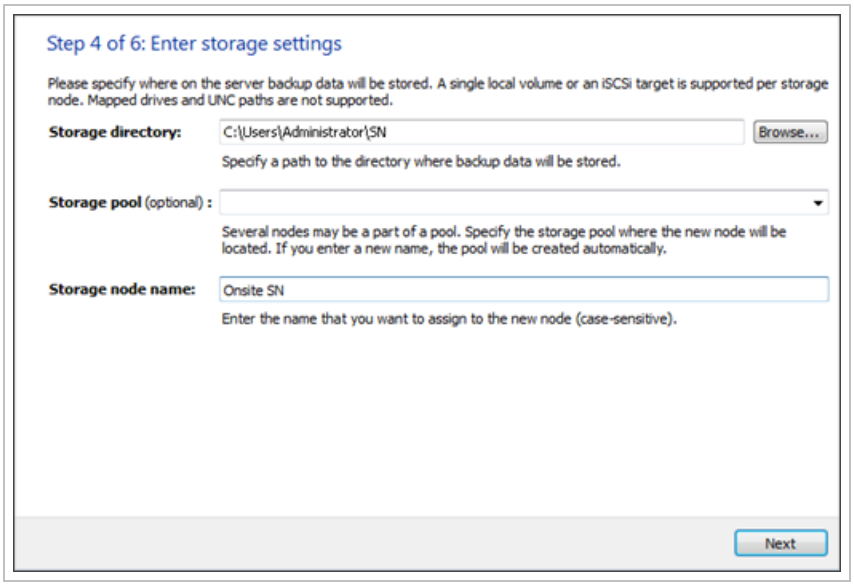


When installing storage nodes, please be aware that you **must use IPv4** as IPv6 is not supported.

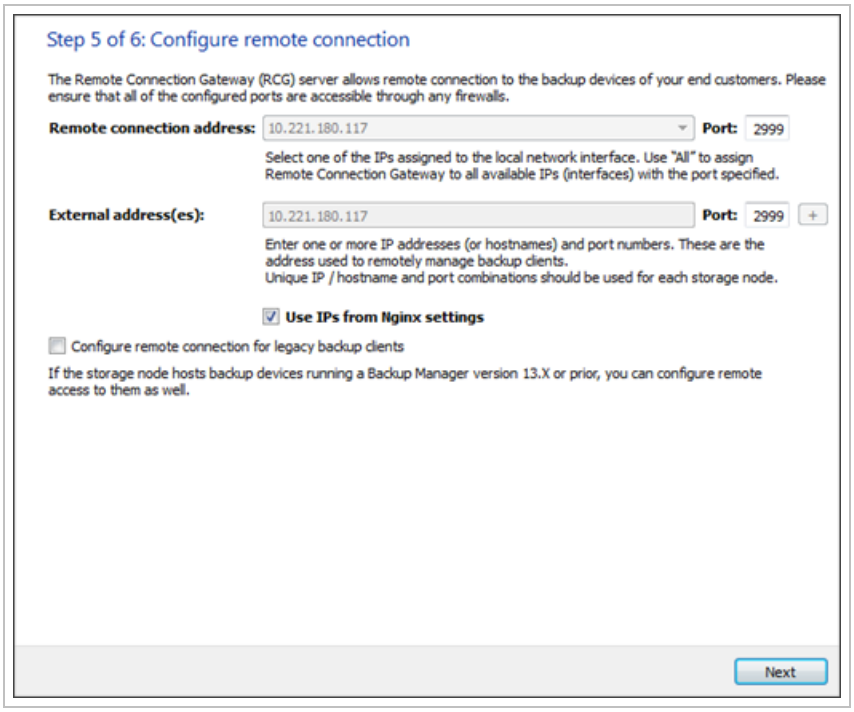
The DNS record can be used in place of the IP address by entering the domain name in the **External Address (es)** field.
In case other external addresses are used, the DNS record should be listed first.

Do not replace the IP addresses for the **Remote connection address**, **External addresses for remote connections**, **Remote connection address for legacy backup clients** and **External address(es) for remote connections to legacy backup clients** fields.

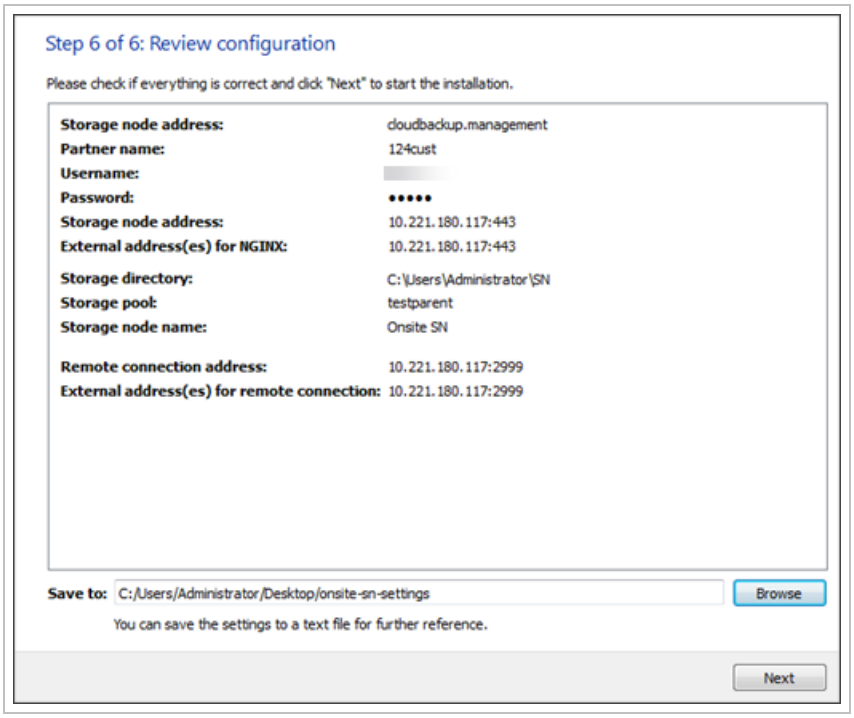
4. Enter information about the new storage location



5. Select the IP address for remote connections to backup devices. You can enter the same address to the **External address(es)** field. If the external address differs from the primary remote connection address, it should forward incoming traffic there (this is achieved with the help of a network adapter)



6. Check the settings you have entered. Use the arrow button at the top to go back to the previous steps and edit the settings. You can save the settings to a text document for further reference **(Save to)**



7. Click **Next** to complete the installation

   After the installation, you can locate the new node among the partner's storage nodes in the Cloud Management Console **(Manage > View storage statistics)**.

> Each storage node requires a unique **IP/port combination**. This applies both to the data transfer settings and remote connection settings.

Settings for storage node installation

Below is the full list of settings that you specify during storage node installation on Windows. For some of the settings older names are provided. They were used in versions prior to 16.2.

Setting	Previous name (if applicable)	Definition
Partner	Partner name	The name of the partner you are installing the storage node for (can be copied from your Cloud management software)
Username	User	The email address of the user from the partner company who has full access to Customer Management in your cloud management software. The SuperUser role is required.
Password		The password associated with the username
Cloud address		The address of the cloud services (detected automatically)
Storage pool	Storage name	The name of the storage pool where the new node will be located. You can choose an existing pool from the list or enter a new name (in that case the pool will be created automatically).
Storage directory		A path to the directory where backup data will be stored
Storage node name		The name you want to assign to the new storage node
Storage node address	Nginx Bind address	The primary IP address and port number of the storage node. It will be used to upload data (namely cabinets and the Backup Register) to the storage node. The recommended port is 443 TCP. If you want the system to use all available IPs (interfaces) with the with the specified port, select **All**.
External addresses for data transfer	External addresses (for Nginx)	The IP address (or hostname) and port number that will be used by Backup Managers for data transfer to and from the storage node. **Advice:** if the Backup Manager is installed in the same network as the storage node, you can speed up data transfer by entering **several addresses**. Avoid using the same external IP address for two or more servers in a local network (it can result in connectivity issues).

Setting	Previous name (if applicable)	Definition
Remote connection address	Web RCG internal address	The primary IP address and port number that will be used to establish remote connections to backup devices. The default port is 2999. If you want the system to use all available IPs (interfaces) with the specified port, select **All**.
External addresses for remote connections	Web RCG external address	The external IP address and port number that will be used to establish remote connections to backup devices.
Remote connection address for legacy backup clients	RCG internal address	The primary remote connection IP address and port number for legacy backup clients running Backup Manager vs. 13x or earlier. The default port number is 1999. If you want the system to use all available IPs (interfaces) with the specified port, select **All**.
External addresses for remote connections to legacy backup clients	RCG external address	The external IP address and port number for remote connections to legacy backup clients running Backup Manager vs. 13x or earlier. The default port is 1999. **Advice:** you can use the same IP address and port number combination that you provided in "External addresses (for Nginx)".

Updating and reconfiguring a storage node

The following topics will guide you through the steps to update and reconfigure a storage node

- Preparatory steps for versions prior to 16.2
- Update and reconfigure a storage node

Preparatory steps for versions prior to 16.2

We recommend using the most **recent version** of the Storage Node Installer for best results. If you want to continue with versions prior to **16.2**, some preparatory steps are necessary:

- Stop the storage node service
- Stop related processes
- Make a backup copy of the current Storage Node Installer installation directory

> In version 16.2 and later of the Storage Node Installer, all necessary processes are stopped automatically. This guarantees that there will not be any conflicts during reconfiguration, so no preparatory steps are needed.

Stop the storage node service

1. Start a terminal emulator or the command line with Admin permissions
2. Stop the storage node service:

   ### Linux instructions

   - For the CloudStorageController: `# /etc/init.d/CloudStorageController stop`
   - For the ProcessController (in legacy versions): `# /etc/init.d/ProcessController stop`

   ### FreeBSD instructions

   - For the CloudStorageController: `# /etc/rc.d/CloudStorageController stop`
   - For the ProcessController (in legacy versions): `# /etc/rc.d/ProcessController stop`

   ### Windows instructions

   - For the CloudStorageController: `net stop CloudStorageController`
   - For the ProcessController (in legacy versions): `net stop ProcessController`
3. Close the terminal or command line

Checking the storage node service name

The name of the storage node service is "CloudStorageController". In versions released in 2013 or earlier, the name of the process is "ProcessController".

If in doubt, you can check which of the names applies to the current storage node installation:

- For the CloudStorageController: `# ps x | grep CloudStorageController | grep -v grep`
- For the ProcessController: `# ps aux | grep ProcessController | grep -v grep`

If the service is running, you will get a response similar to the following:

```
15942 ? Ssl 0:00 /opt/mxb/bin/CloudStorageController serve
```

Stop related processes

Make sure to stop all the processes (listed below) that are associated with the storage node service:

- `nginx`
- `RemoteConnectionGateway`
- `WebRemoteConnectionGateway`
- `StorageNodeAgent`
- `ReportingService`
- `CloudStorageController` or `ProcessController` (in legacy versions)

Making sure the service has been stopped (optional)

To make sure the service has been stopped, run the following command.

Instructions for Linux and FreeBSD

On Linux and FreeBSD, use the `grep` command followed by the name of a process. For example, you can check the status of the `RemoteConnectionGateway` process in the following way:

```
# ps aux | grep RemoteConnectionGateway
```

If the service is stopped, no output will be returned.

Windows instructions

On Windows, you can access the processes through the **Processes** tab of Task Manager. To end a running process, either:

1. Right-click the process and select **End Process**,

   Or
2. Left click the process to highlight and select **End Process** from the bottom right-hand corner of the Task Manager

Update and reconfigure a storage node

To update the storage node software or to reconfigure the current settings, you need to repeat the installation as you would when installing a storage node for the first time, with the **Reconfigure** option enabled.

Storage Node Installers are available in the **Downloads** section of the Management Console. They can also be downloaded from here.

> Storage node reconfiguration **does not influence** active backup sessions (new backup data is distributed among other storage nodes available to your company while the home node is unavailable).

Options

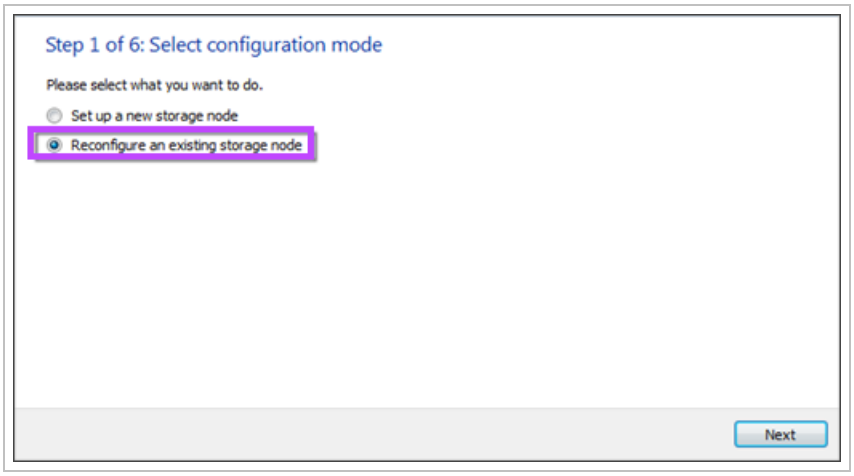
You can change most of the settings during storage node reconfiguration. There are only 2 major properties are not subject to editing during a reconfigure: name and customer. This means it is **not possible** to re-assign an existing node to a different customer or rename the node. In these cases you will need to create a new node and put the current node out of service if it is no longer needed.

The DNS record can be used in place of the IP address by entering the domain name in the External Address(es) field. In case other external addresses are used, the DNS record should be listed first.

> Do not replace the IP addresses for the **Remote connection address**, **External addresses for remote connections**, **Remote connection address for legacy backup clients** and **External address(es) for remote connections to legacy backup clients** fields.

Instructions

1. Download the Storage Node Installer for your operating system from the N-Able Cove Data Protection page
2. Start the Storage Node Installer
   - On Windows, it opens as a set-up wizard. Choose **Reconfigure an existing storage node**



   - On Linux and FreeBSD, use the command line. Set executable rights for the script (`root# chmod +x mxb-cloud-sn-linux-x86_64.run`) and then run the Storage Node Installer (`root# ./mxb-cloud-sn-linux-x86_64.run`). You will be asked what you want to do. Set `-installation-mode` to `install`

```
./mxb-cloud-sn-linu x-x86_64.run
Verifying archive integrity... All good.
Uncompressing Cloud Storage Node installer........

Cloud storage node installation modes:
[1] Setup new or update existing cloud storage node
[2] Upgrade old appliance to a cloud storage node
Enter the number: 1

Cloud partner name: AcmeIT
Cloud user: root@email.com
Cloud password for 'root' user: 123456
Attempting to authenticate at cloud.securebackupandrestore.com:443... ok

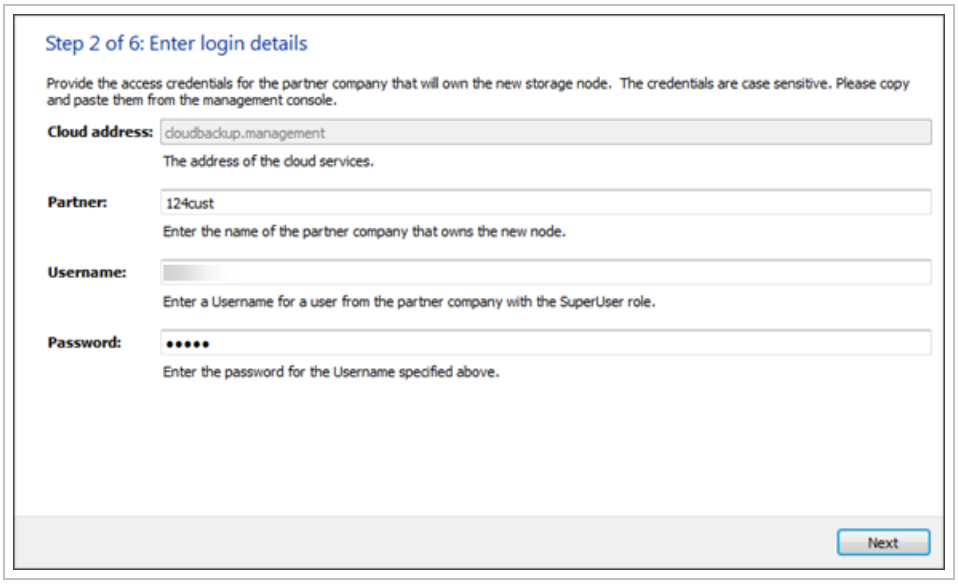
Storage directory [/opt/mxb/storage]:

Storage name [Primary]: linux_001
Storage node name: Linux001
......
```

3. Proceed through the installation steps for the relevant Operating System, updating the settings needed:

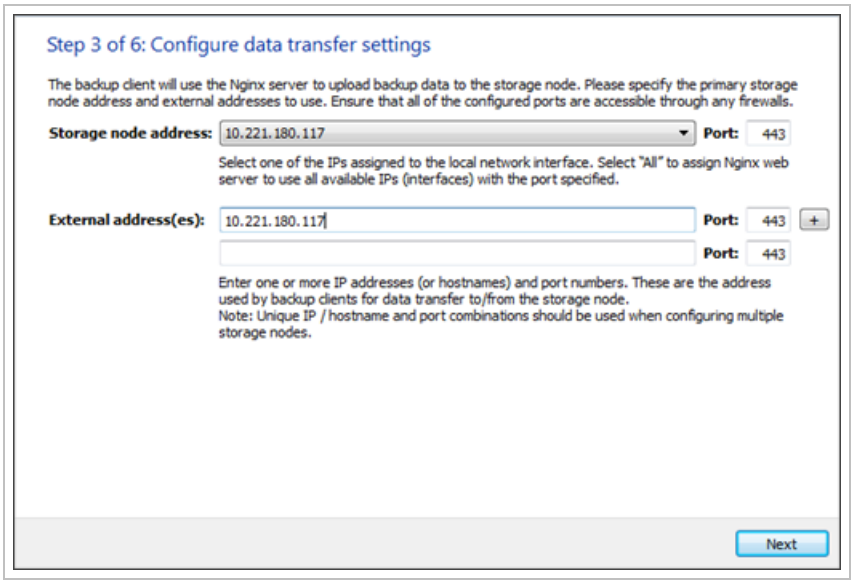
Windows

a. Enter your login credentials for access to the cloud. An account with the SuperUser role is required



> The settings that you can reconfigure can be found in Settings for storage node installation

b. Select the IP address you want to use for the storage node. You can enter the same IP address to the **External address(es)** field. If the external address differs from the primary storage node address, it should forward incoming traffic there (this is achieved with the help of a network adapter)

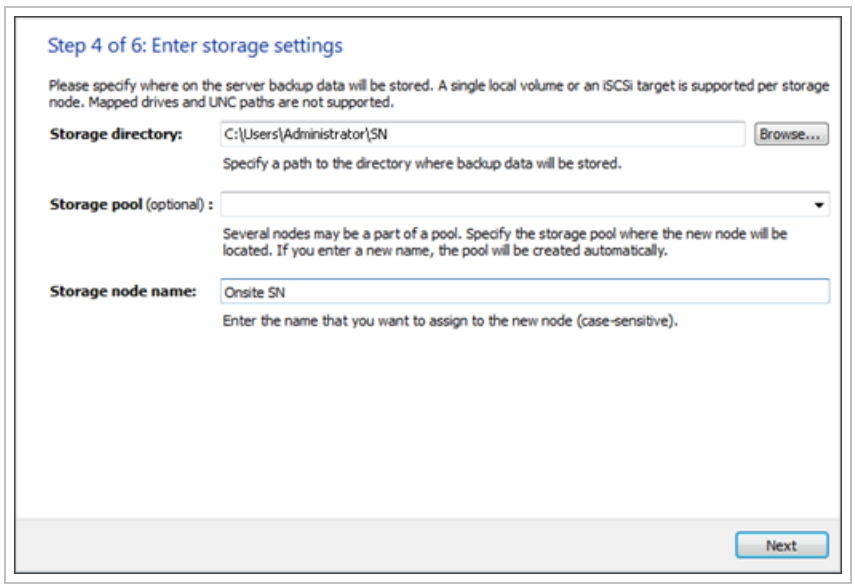


> When installing storage nodes, please be aware that you must use IPv4 as IPv6 is not supported.

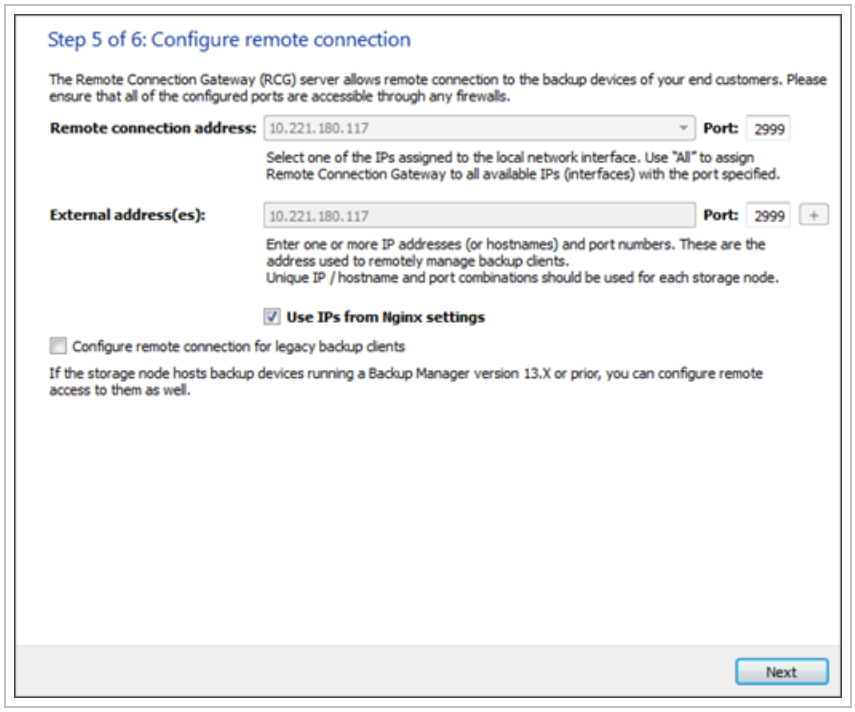
> The DNS record can be used in place of the IP address by entering the domain name in the **External Address(es)** field.
> In case other external addresses are used, the DNS record should be listed first.

> Do not replace the IP addresses for the **Remote connection address**, **External addresses for remote connections**, **Remote connection address for legacy backup clients** and **External address(es) for remote connections to legacy backup clients** fields.

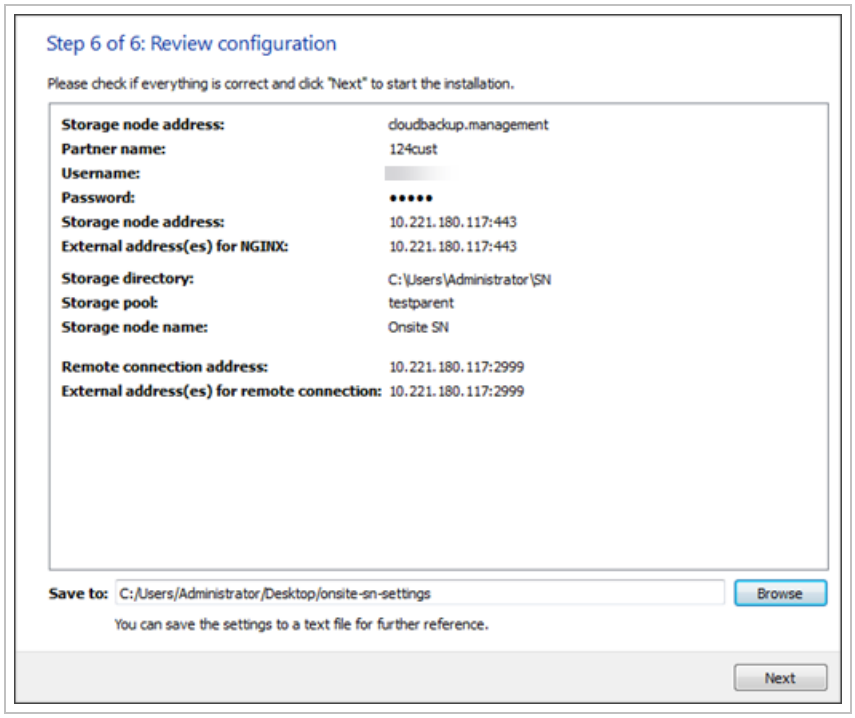
c. Enter information about the new storage location



d. Select the IP address for remote connections to backup devices. You can enter the same address to the **External address(es)** field. If the external address differs from the primary remote connection address, it should forward incoming traffic there (this is achieved with the help of a network adapter)



e. Check the settings you have entered. Use the arrow button at the top to go back to the previous steps and edit the settings. You can save the settings to a text document for further reference **(Save to)**



f. Click **Next** to complete the installation

After the reconfiguration, you can locate the node among the partner's storage nodes in the Cloud Management Console **(Manage > View storage statistics)** with the new configuration.

GNU/Linux

a. Submit the Installation parameters with the necessary changes

b. Review the settings you have submitted. Enter `Y` (Yes) if everything is correct or enter `N` (No) to start over. Here is an example:

```
Please review all the information once again:
============================================================
Storage directory:          /opt/mxb/storage
------------------------------------------------------------
Cloud address:              cloudbackup.management:443
Cloud partner name:         Smart Telecom
Cloud user:                 root@email.com
Cloud password:             ********
------------------------------------------------------------
Storage name:               Primary
Storage node name:          Smart Telco Node 3
------------------------------------------------------------
NGINX bind address:         192.168.0.222:443
External addresses:         192.168.0.222:443
RCG bind address:           192.168.0.222:1999
RCG external address:       192.168.0.222:1999
Web RCG bind address:       192.168.0.222:2999
Web RCG external addresses: 192.168.0.222:2999
============================================================
Is everything correct? (Y/n) Y
```

When the reconfiguration is complete, the node will appear among the partner's nodes with the appropriate changes made.

The new settings will be **applied automatically** within the next couple of hours.

> If you have previously configured Log Size Limiting entries in the storage node config.ini, these will need to be re-added after reconfiguration of the storage node is complete:
> `[Logging]`
> `SingleLogMaxSizeInMB=X`
> `TotalLogsMaxSizeInMB=X`

Relocating a storage node to new hardware

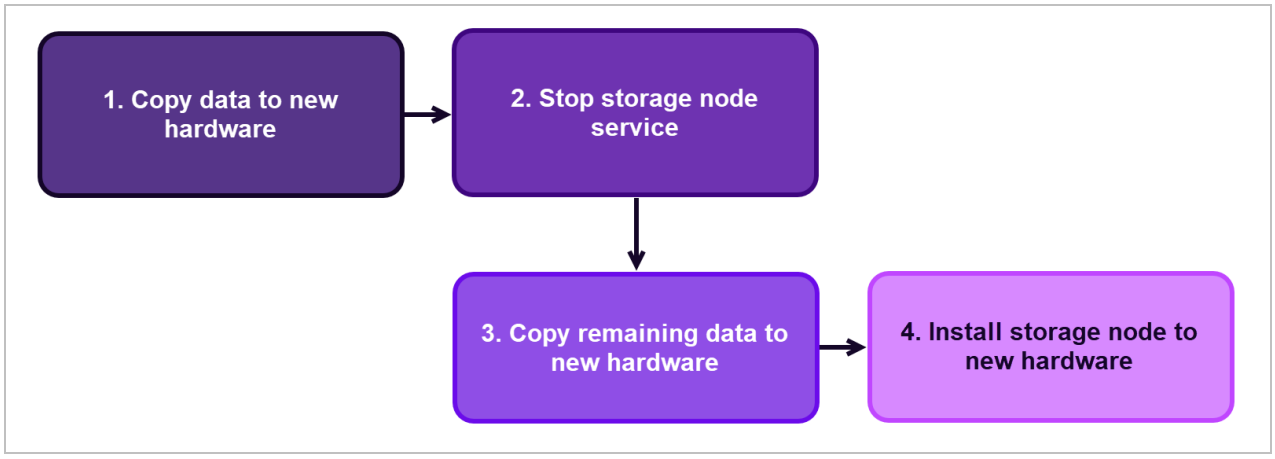
Software-only customers who use their own storage may sometimes need to relocate a storage node to new hardware (for example, when there is a need for more space and better performance).

Requirements

The new hardware must meet the storage node installation requirements. It can run the same operating system as the source hardware or a different one (as long as it is supported).

Instructions

In short, the migration process looks in the following way.



Please follow step-by-step instructions for your operating system.

- Relocate storage node on GNU/Linux
- Relocate storage node on Windows

Relocate storage node on GNU/Linux

Step 1: Copy the data

Start by copying the data from the source machine to the target machine. We recommend using the **rsync** utility to cut the downtime while the node is unavailable. You can install it either on the source machine or on the target machine as in the current example.

1. Start a terminal emulator on the target machine and install rsync (if you do not have it yet)
   - Debian and Ubuntu: `# apt-get install rsync`
   - CentOS, RHEL, and SUSE: `# yum install rsync`
2. Create a directory on the target machine where you want to copy the data - for example `/storage_new`

   ```
   # mkdir /storage_new
   ```

3. Copy the data from the source machine to the target machine. Keep the **storage node service** ("CloudStorageController" or "ProcessController" in the older versions) running to decrease the downtime for the Backup Managers using it. Format the command in the following way:

   ```
   # rsync -av --progress <username@source_machine_IP/source_directory/>
   <target_directory>
   ```

For example:

```
# rsync -av --progress root@192.168.0.123:/storage_orig/ /storage_new/
rsync.exe -av --progress /cygdrive/x/FtpStorage/ /cygdrive/e/FtpStorage
15942 ?        Ssl    0:00 /opt/mxb/bin/CloudStorageController serve
```

Step 2: Stop the storage node service

Start a terminal emulator on the source machine and stop the storage node service (detailed instructions).

The downtime has started.

Step 3: Copy new data

Now it is necessary to copy the **most recent backup data** that might have accumulated on the source storage node after the initial synchronization session. We recommend copying the data with the `--delete` option (it removes temporary files from the target directory).

```
rsync -av --progress --delete root@192.168.0.123:/storage_orig/ /storage_new/
```

Once finished with the final synchronization, the original and target folders will contain exactly the **same data**.

Step 4: Create a user for storage node access

Create a new user and a group named "iasouser" with GUID 2001 on the new storage node.

1. Start the terminal emulator and create a group: `groupadd -g 2001 iasouser`
2. Then create a user in that group: `useradd -u 2001 -g 2001 iasouser`

Step 5: Install storage node software to new hardware

1. Copy the original storage node installation folder from the original machine

   ```
   rsync -av --progress root@192.168.0.123:/opt/mxb /opt/
   ```

2. Download a storage node installation package for your operating system:

   ```
   wget -c https://cdn.cloudbackup.management/maxdownloads/mxb-cloud-sn-linux-
   x86_64.run
   ```

3. Give execute permissions to the file:

   ```
   chmod +x ./mxb-cloud-sn-linux-x86_64.run
   ```

4. Run the Storage Node Installer: `./mxb-cloud-sn-linux-x86_64.run`

5. Select the **Reconfigure** option and complete the installation. You can use a different IP address but it is important that the primary properties **stay unchanged**:
   - Storage node name (`-storage-node-name`)
   - Storage pool name (`-storage-name`)

Result

The migration is completed. All the devices will be automatically connected to the new storage node within the next 30 minutes.

If you want to make sure the storage node has started working on the new hardware, check the Nginx access log for incoming connections. There should be a lot of 201\207 requests there.

```
tail -f /opt/mxb/var/log/nginx/nginx-access.log
```

Another way to verify the migration is through the Cloud Management Console **(Manage > View storage statistics)**.

Relocate storage node on Windows

Step 1: Copy the data

Start by copying the data from the source machine to the target machine. We recommend using Robocopy, a command-line utility that is included into all Windows packages starting from Windows Vista and Windows Server 2008. Robocopy minimizes the downtime while the node is unavailable.

To learn more about the syntax, start the Command Prompt and submit the following command:

```
Robocopy /?
```

You can run Robocopy either on the source machine or on the target machine as in the current example.

1. Create a directory on the target machine where you want to copy the data - for example `\storage_new`:

   ```
   mkdir data\storage_new
   ```

2. Copy the data from the source machine to the target machine

   ```
   robocopy \\source_machine\original_dir \new_dir /E
   ```

Examples

If the source is in the **local network**, format the command in the following way:

```
robocopy \\ 192.168.0.123\storage_orig data\storage_new /E
```

If the source is on a **remote server**, you need to log in to the server, go to the source directory and then do the copying.

```
NET USE \\192.168.0.123\IPC$ /u:root 123456 cd c:storage/ robocopy \\
192.168.0.123\storage_orig data\storage_new /E
```

Step 2: Stop the storage node service

1. Start the Services Console
2. Navigate to **Backup Service Controller**or **Process Controller** service
3. Right-click and select **Stop**
4. Now find the **Cloud Storage Node Monitor** service
5. Right-click and select **Stop**

> The downtime has started

Step 3: Copy new data

Now it is necessary to copy the most recent backup data that might have accumulated on the source storage node after the initial synchronization session. We recommend copying the data with the `/MIR` option (it removes temporary files from the target directory).

```
robocopy \\ 192.168.0.123\storage_orig data\storage_new /MIR
```

When the final synchronization is completed, the original and the target folders will contain exactly the same data.

Step 4: Create a user for storage node access

Create a new user and a group named "iasouser" with GUID 2001 on the new storage node.

1. In the Command Prompt, create a new group:

   ```
   net localgroup 2001 /add
   ```

2. Create a user in that group:

   ```
   net localgroup 2001 iasouser /add
   ```

Step 5: Install storage node software to new hardware

1. Copy the original storage node installation folder from the original machine

   ```
   robocopy \\192.168.0.123\ C:\Program Files\CloudStorageNode \Program
   Files\CloudStorageNode /E
   ```

2. Make sure the storage_node_config.ini has been copied
3. Download the Storage Node Installer for your operating system from the N-Able website

4. Run the Storage Node Installer with the **Reconfigure** option. You can change the settings as necessary (even use a different IP address). But it is important that the primary properties stay unchanged:
   - Storage node name
   - Storage pool

Managing private storage

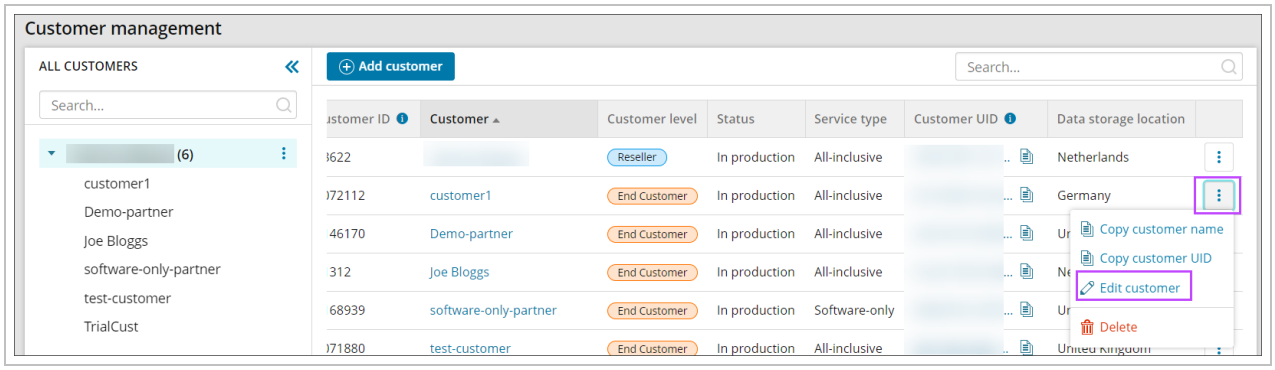
The primary tools for managing private storage, including Storage Reporting to view storage statistics, selecting the partnership model for customers and selecting the storage pool for the device.

Tool	Tasks performed
Storage Node Installer	▪ Installing storage nodes ▪ Reconfiguring storage nodes
Backup & Recovery Console	▪ Getting statistics for storage nodes (used size, total size, reserved size, number of devices) ▪ Selecting a partnership model for customers ▪ Selecting a storage pool for devices
Cloud Management Console (legacy)	▪ Changing storage node states (Online/Offline and Operable/Out of service) ▪ Checking which storage pool a backup device is assigned to
Third-party monitoring systems (Nagios, Zabbix, etc.)	Checking HTTPS port availability and the amount of free space left on a storage node. Learn more.

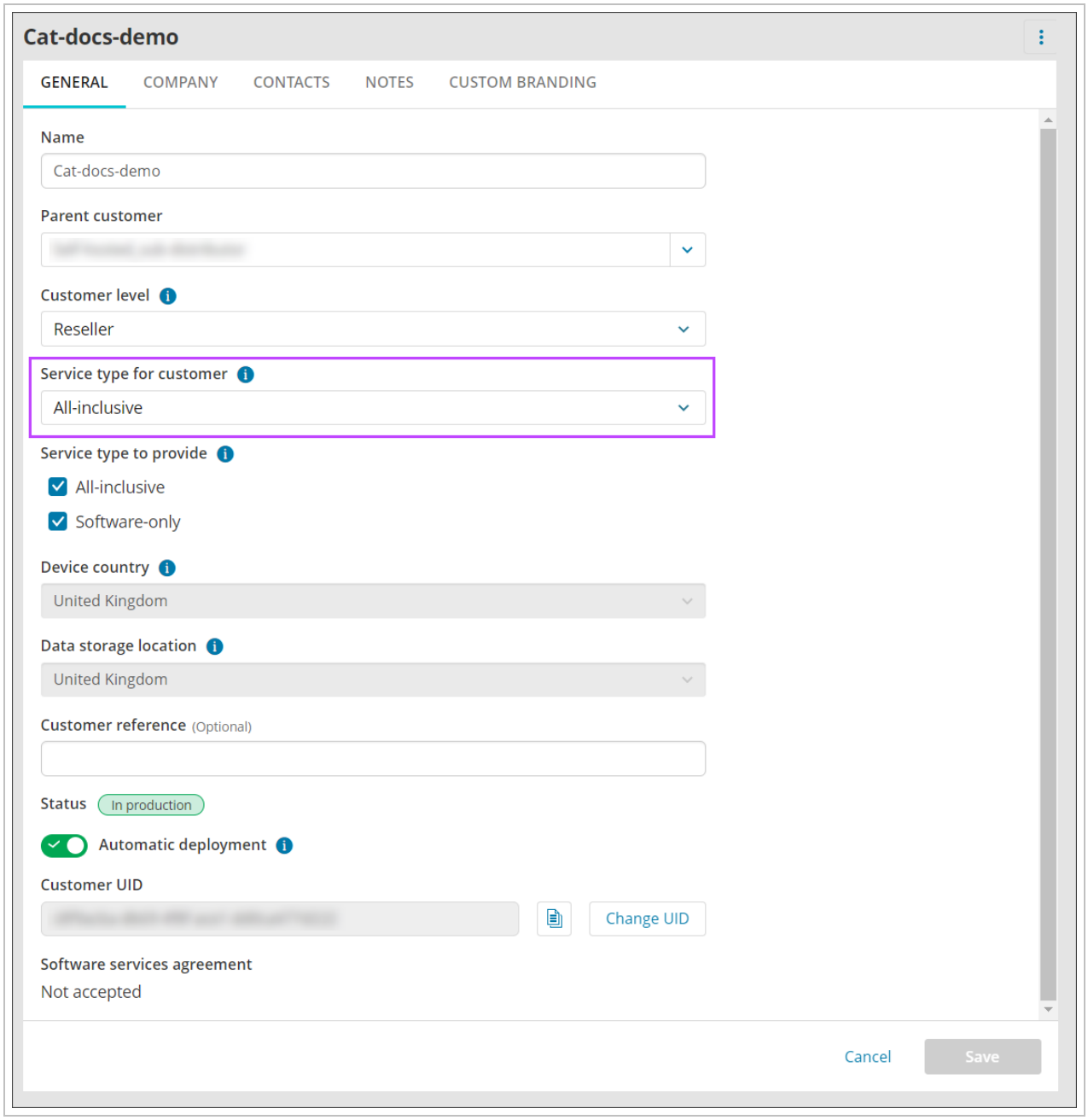
Selecting partnership model for customers

By default, your customers use the same storage that is available to your company. You can set a partnership model for each of your customers individually:

1. Log in to the Management Console under a **SuperUser** account
2. In the Management section of the vertical menu, click **Customers** to open the **Customer Management** window
3. Find the customer from the list
4. Either click the three vertical dots from the Customers list on the left-hand pane or scroll to the right and click the three vertical dots to open the Action menu



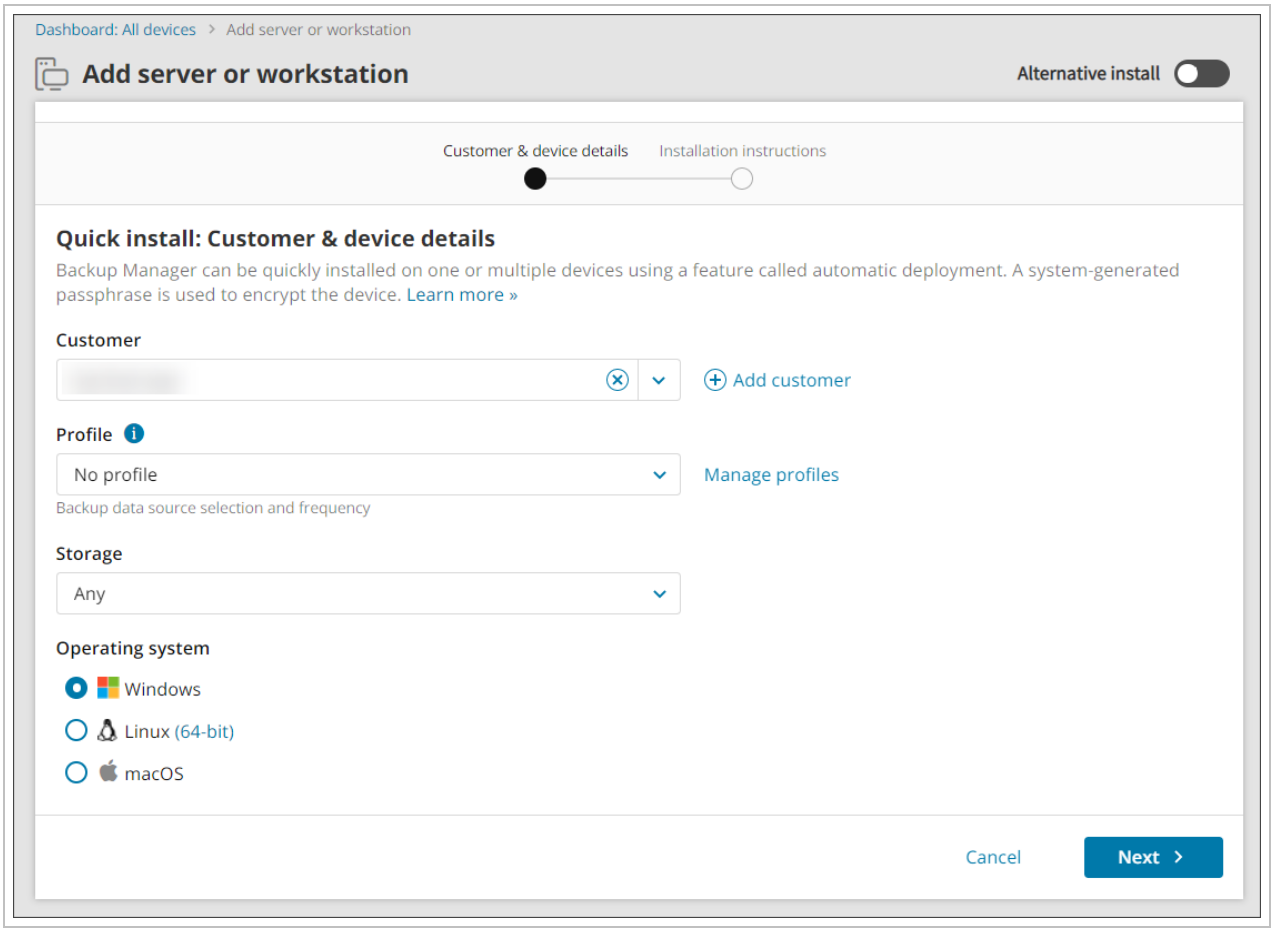
5. Click **Edit customer**
6. Choose an appropriate value from the **Service type** list ("Software-only" or "All-inclusive")



The changes will take effect within the next 30 minutes.

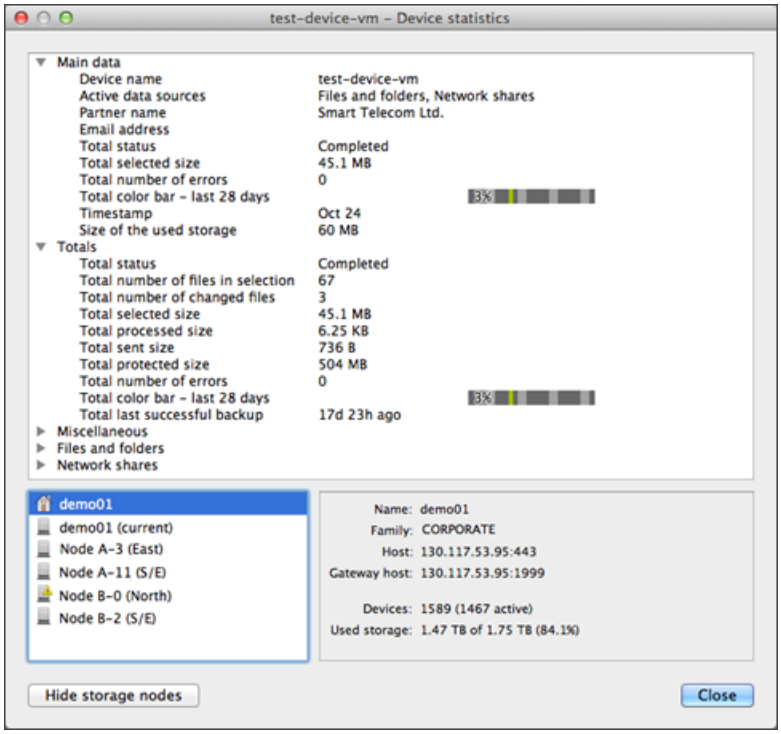
Selecting storage pool for device

When you add a new backup device, you can select a storage pool for it. Choose **Any** if you want the device to use all storage pools available to the customer.



To find out which storage pool an existing device is assigned to, use the Cloud Management Console.

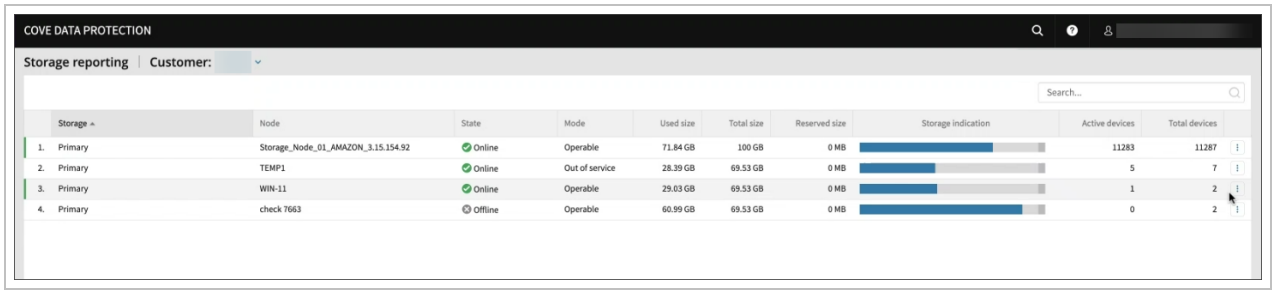
1. Right-click the device and choose **Statistics** from the context menu
2. Click **Show storage nodes**



Storage Reporting

Use the **Storage Reporting** tool Management Console to view the storage reports. This report, shows the following statistics for storage nodes belonging to your company:

- Storage State
- Mode
- Used size
- Total size
- Reserved size
- Number of devices that are uploading data to this node
- Total number of devices that have data stored on this node



> The **Storage reporting** module in the Management Console is available to **software-only customers** only as configured in Customer management in Management Console

View Storage Report

1. Log in to the Management Console under a **SuperUser** account, Administrator account, Manager account or Operator account
2. In the vertical menu, click **Storage reporting**

Storage Indication Breakdown	
Blue	Used storage
Light Grey	Remaining *unused* portion of the total storage space
Dark Grey	Reserved *unused* portion of the total storage space (i.e. cannot be used)

Monitoring private storage

Private storage can be monitored using third-party monitoring systems such as Nagios or Zabbix.

HTTPS port accessibility

To check the HTTPS port accessibility:

Start your monitoring system and format your request in the following way:

```
curl -k <server_address>
```

For example:

```
curl -k https://eu.cloudbackup.management/
```

The response must be `403 Forbidden` and the port must be taken by the Nginx service.

```
<html>
    <head>
       <title>403 Forbidden</title>
    </head>
    <body bgcolor="white">
       <center><h1>403 Forbidden</h1></center>
       <hr><center>nginx/1.8.1</center>
    </body>
</html>
```

Other tasks

Here are some other typical tasks:

- Monitor the amount of **free space** on your storage nodes
- Monitor running storage node **services**. The primary services are as follows: the Cloud Storage Controller, Nginx, Reporting Service and Web Remote Connection Gateway

Each monitoring system has its own templates to accomplish the tasks.

> Data transfer statuses are monitored automatically. As a software-only customer, you are responsible for the **file system integrity** so that the uploaded data stay consistent.

Storage node service

As a storage administrator, you may need to stop or restart the storage node service from time to time.

Checking the storage node service name

The name of the storage node service is "CloudStorageController". In versions released in 2013 or earlier, the name of the process is "ProcessController".

If in doubt, you can check which of the names applies to the current storage node installation:

- For the CloudStorageController: `# ps x | grep CloudStorageController | grep -v grep`
- For the ProcessController: `# ps aux | grep ProcessController | grep -v grep`

If the service is running, you will get a response similar to the following:

```
15942 ? Ssl 0:00 /opt/mxb/bin/CloudStorageController serve
```

Stop the storage node service

1. Start a terminal emulator or the command line with Admin permissions
2. Stop the storage node service:

   #### Linux instructions

   - For the CloudStorageController: `# /etc/init.d/CloudStorageController stop`
   - For the ProcessController (in legacy versions): `# /etc/init.d/ProcessController stop`

   #### FreeBSD instructions

   - For the CloudStorageController: `# /etc/rc.d/CloudStorageController stop`
   - For the ProcessController (in legacy versions): `# /etc/rc.d/ProcessController stop`

   #### Windows instructions

   - For the CloudStorageController: `net stop CloudStorageController`
   - For the ProcessController (in legacy versions): `net stop ProcessController`
3. Close the terminal or command line

Making sure the service has been stopped (optional)

To make sure the service has been stopped, run the following command.

Instructions for Linux and FreeBSD

- For the CloudStorageController: `# ps x | grep CloudStorageController | grep -v grep`
- For the ProcessController (in legacy versions): `# ps aux | grep ProcessController | grep -v grep`

If the service is stopped, no output will be returned.

Windows instructions

On Windows, you can access the services through the Task Manager (the **Services** tab) or through the Services Console.

JSON-RPC API guide for Cove Data Protection (Cove)

JSON-RPC is a light-weight remote procedure call protocol encoded in JSON. It allows for multiple calls to be sent to the Cove Data Protection (Cove) server which may be answered asynchronously.

> We recommend the use of JSON-RPC API **only** if you are familiar with it and are confident in your ability to construct functional calls.

> For information on how to read and use the Cove schema, see the How to use the Backup Manager JSON-RPC API schema page.

There are 2 types of web services in Cove:

1. **Management Service** - provides management functions and statistics for all devices belonging to a certain customer. The key entity in the Management Service protocol is the **customer**
2. **Reporting Service** - provides detailed backup and restore statistics for selected devices. It runs on every storage node

For some methods you may be asked for column vectors or column codes or be provided with these in the call response. Please view the Management Console column codes for API page to see the full list of column vectors and their definitions.

> Be aware that methods and parameters are case sensitive so ensure you use the correct capitalization as documented in the Schema.

> Please note, the **old** legacy notations (found here) will still work for many calls, however, we would strongly recommend you change to use the new notations as soon as possible.

Data format

The services are exposed via a **custom JSON-RPC protocol**. It lists available methods and supported parameters, but it **cannot** be used to generate a client for the service automatically.

JSON-RPC schema for Cove Data Protection (Cove)

Making changes

All changes made using API's can only be made for **one at a time**. If you require changes to be made on several devices, customers, storages, etc. at the same time you would need to follow the below process:

1. Enumerate the list of devices, customers, storages, users, etc. using the appropriate method (`EnumerateAccounts`, `EnumeratePartners`, etc.)
2. Write a script to make the necessary changes in whichever tool you prefer
3. Parse the list output into the script you have written
4. Run your script to make the changes

> For any changes made with the API, we would recommend you re-run the appropriate method to confirm your changes have been successful.

Date and time format

All of the Backup Manager API methods will display date and time as Unix format.

This means that the time is shown as the number of seconds that have passed since 00:00:00 UTC, 1st January 1970. For example:

- Unix timestamp: 1554986978
- Coordinated universal time (UTC): 2019-04-11 12:49:38

You can calculate the time to more readable format by using this conversion table:

Human Readable Time	Seconds
1 minute	60 seconds
1 hour	3600 seconds
1 day	86400 seconds
1 month (30.44 days)	2629743 seconds
1 year (365.24 days)	31556926 seconds

> Some API tools may convert this time for you automatically. Alternately, you can find Unix to Human Readable Time conversion tools by searching online.

Size format

All of the Backup Manager API methods will display sizes in Bytes. You can calculate the sizes to a more readable format by using this conversion table (where n=number of bytes given in the output):

Bytes	Calculation	Size format
1,024 bytes	n/2^10	1 kilobyte (K / Kb)
1,048,576 bytes	n/2^20	1 megabyte (M / Mb)
1,073,741,824 bytes	n/2^30	1 gigabyte (G / Gb)
1,099,511,627,776 bytes	n/2^40	1 terabyte (T / TB)

> Some API tools may convert this size for you automatically. Alternately, you can find Bytes size conversion tools by searching online.

Requirements for HTTP requests

You can run test requests using any command-line tools that support HTTP: curl, SoapUI, Advanced REST Client Chrome plug-in or any other:

- **HTTP method** - POST
- **HTTP header**- `Content-Type: application/json`
- **Endpoint** - `https://api.backup.management/jsonapi`

What's Inside

How to use the Backup Manager JSON-RPC API schema

> The schema for the protocol is currently in **beta**.

The schema lists available methods and supported parameters, but it **cannot** be used to generate a client for the service automatically.

The schema can be found here: JSON-RPC schema for Cove Data Protection (Cove)

You can find information on how to Construct A JSON-RPC API Call in conjunction with our Schema here.

Recommendations

Before getting started, we would recommend you either download a JSON API reader plugin for your preferred web browser or use a browser which automatically reads API's and breaks the schema down into sections for you, as this makes it easier to view.

It is also advisable to have the API platform of your liking installed on your device before beginning.

Schema sections

Using a reader or a browser with a built-in reader allows for a much easier view of the schema so that the page is broken down into smaller sections:

Enums

The **Enums** section displays a list of supported values (enumerators) for parameters where this parameter requires the choice of one or more of a set of **predefined values**.

These lists of supported values can be used with their respective methods to filter information or to work out what an output means.

Example

Below are the values available for `AccountFlags::Enum`:

```
{
    "Name" : "AccountFlags::Enum",
    "Namespace" : "",
    "Struct" : "AccountFlags",
    "Values" : [ "Undefined", "Managed_Obsolete", "Trial", "AutoDeployed", "Count"
]
}
```

This means that for any Method with a Parameter (Params) whose Type is 'AccountFlags::Enum' such as AccountInfo, the selection will be one or multiple of the AccountFlag::Enum Values.

Methods

The **Methods** section shows the names of the methods that can be used, and which parameter names and types can be used with these methods.

> If a type is not `int`, `bool`, `std::time_t`, `std::string` or `std::set<int>`, then the type is either an **enumeration**, or **structure** and will be found by searching for the type in these sections. E.g. `"AccountStatisticsQuery"` with its accepted fields and types, is found in Structs.

Example

The method `EnumerateAccountStatistics` has the following parameters that can be used when calling this method:

```
{
    "IsConstant" : true,
    "Name" : "EnumerateAccountStatistics",
    "Params" : [
       {
           "IsOutput" : false,
```

```
            "IsPointer" : false,
            "Name" : "query",
            "Type" : "AccountStatisticsQuery"
           },
           {
            "IsOutput" : true,
            "IsPointer" : false,
            "Name" : "totalStatistics",
            "Type" : "TotalStatisticsInfo"
           }
    ],
    "ResultType" : "std::unique_ptr<IForwardIterator<AccountStatisticsInfo> >"
},
```

Structs

In the **Structs** section you will see the fields and the accepted field types for parameters that show something other than an ::Enum or one of the these types:

- int
- bool
- std::time_t
- std::size_t
- std::string
- std::set<int>
- std::vector<std::string>

Example

The below example contains all of the parameters that may be used under the `"Query"` parameter named `"AccountStatisticsQuery"`:

```
{
    Fields: [
       {
           "Name" : "PartnerId",
           "Type" : "int"
       },
       {
           "Name" : "Filter",
           "Type" : "std::string"
       },
       {
```

```
            "Name" : "ExcludedPartners",
            "Type" : "std::set<int>"
        },
        {
            "Name" : "SelectionMode",
            "Type" : "AccountStatisticsSelectionMode::Enum"
        },
        {
            "Name" : "Labels",
            "Type" : "std::set<int>"
        },
        {
            "Name" : "StartRecordNumber",
            "Type" : "std::size_t"
        },
        {
            "Name" : "RecordsCount",
            "Type" : "std::size_t"
        },
        {
            "Name" : "OrderBy",
            "Type" : "std::string"
        },
        {
            "Name" : "Columns",
            "Type" : "std::vector<std::string>"
        },
        {
            "Name" : "Totals",
            "Type" : "std::vector<std::string>"
        }
        ],
    "Name" : "AccountStatisticsQuery",
    "Namespace" : ""
},
```

For a list of Column Vectors, please see the Management Console column codes for API page.

Construct A JSON-RPC API Call

To construct a functional call in your API program of choice, you need

1. Ensure the start of the method includes the following, filling in your Visa with one received by running an authorization call:

```
{
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "id":"jsonrpc",
```

2. Search in the schema for the method you need and add this to the call you are creating:

```
    "method" : "EnumerateAccountStatistics",
```

3. Add the parameters and fill these in with the criteria you wish to search for:

```
    "params" : {
       "query" : {
           "PartnerId" : partner-id-number-here,
           "StartRecordNumber" : number-of-records-to-start-displaying-from,
           "RecordsCount" : number-of-records-to-return,
           "Columns" : in-this-format-["xn","xn","xn"]-the-column-short-codes-to-
display
       }
    }
}
```

> If a type is not `int`, `bool`, `std::time_t`, `std::string` or `std::set<int>`, then the type is either an enumeration, or structure and will be found by searching for the type in these sections. E.g. `"AccountStatisticsQuery"` with its accepted fields and types, is found in Structs.

- If it is an enumeration (list) your API parameter should contain one or more of the given types

4. Ensure you have closed the brackets and have commas at the end of lines which are followed by another parameter

The combined example query would look something like this:

```
{
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "id":"jsonrpc",
    "method" : "EnumerateAccountStatistics",
    "params" : {
       "query" : {
           "PartnerId" : 123456,
           "StartRecordNumber" : 0,
           "RecordsCount" : 5,
           "Columns" : ["T3", "G3"]
       }
    }
}
```

For the above query, a sample response would be:

```
{
    "jsonrpc": "2.0",
    "id": "jsonrpc",
    "result": {
       "result": [
           {
               "AccountId": 987654,
               "Flags": [
                   "AutoDeployed"
               ],
               "PartnerId": 123456,
               "Settings": null
           },
           {
               "AccountId": 987654,
               "Flags": [
               "AutoDeployed"
               ],
               "PartnerId": 123456,
               "Settings": [
           {
                       "T3": "248260085992"
                   }
               ]
           },
               "AccountId": 987654,
```

```
                "Flags": null,
                "PartnerId": 123456,
                "Settings": [
                    {
                        "G3": "8094565"
                    }
                    {
                        "T3": "29928402"
                    }
                ]
        ],
        "TotalStatistics": null
    },
    "visa": "{{visa}}"
}
```


Authorization in JSON-RPC API

Any request to the Management Service must be authorized. You can get access credentials from your service provider.

In order for authorization to be permitted, your user account in Management Console must have **API Authentication** enabled. This can be done either at the time of adding the user account, or after, by editing the user in Management Console and enabling **API Authentication**.

Add user

New users will be emailed a link allowing them to create their own password and setup two-factor authentication (2FA).

Customer

Demo-partner

Email

demo.user@invalid.tld

Role

SuperUser

First name (optional)

Demo

Last name (optional)

User

Job title (optional)

CTO

Phone number (optional)

01234 567890

☑ Security officer

The Security Officer role grants permission to request a passphrase. See more »

☑ API authentication

API authentication allows users to authenticate with the API. See more »

Cancel | Save and add another | Save

More information on user types and permissions can be found here.

In a response to your authorization request (`Login`), you will get a **visa**. This is a required parameter for all further requests. The visa stays valid for **15 minutes**.

> Each response contains a new visa. You can use visas from previous calls to keep the **visa chain** uninterrupted. If the interval between service calls exceeds 15 minutes, you will need to repeat the `Login` request and start a new visa chain.

Required parameters

Parameter	Description	Type/Supported values
`partner`	The name of the customer you want to log in under	std::string String
`username`	Your email address for access to the service	std::string String
`password`	Your password for access to the service	std::string String

Sample request

```
{
    "jsonrpc":"2.0",
    "method":"Login",
    "params":{
           "partner":"Smart Telecom Inc.",
           "username":"admin@smart-telecom.net",
           "password":"sec1234!6"
    },
    "id":"1"
}
```

Sample response

```
{
    "id": "1",
    "jsonrpc": "2.0",
    "result": {
       "result": {
               "EmailAddress": "admin@smart-telecom.net",
               "FirstLoginTime": 1464945879,
               "FirstName": "Christine",
               "Flags": [
                   "AllowApiAuthentication"
               ],
               "FullName": "Smith",
               "Id": 50193,
```

```
                "LastLoginTime": 1512383091,
                "Name": "admin@smart-telecom.net",
                "PartnerId": 33491,
                "Password": null,
                "PhoneNumber": "",
                "RoleId": 1,
                "Title": "Reseller",
                "TwoFactorAuthenticationStatus": "Enabled"
        }
    },
    "visa": "{{visa}}"
}
```


Device management methods in JSON-RPC API

To enable backups on a system, a backup device[1] is required.

> A backup device can be installed on several computers: the **primary** computer where data backup takes place and any number of **additional** computers in the restore-only mode.

Below is the list of **primary methods** that let you manage backup devices of a particular customer.

- Adding devices (the `AddAccount` method)
- Getting device information by the device name and password (the `GetAccountInfo` method)
- Getting device information by the device ID (the `GetAccountInfoById` method)
- Getting device information by the device Token (the `GetAccountInfoByToken` method)
- Getting the device ID (the `GetAccountID` method)
- Enumerating Devices in JSON-RPC API (the `EnumerateAccounts` method)
- Enumerating Device Statistics in JSON-RPC API (the `EnumerateAccountStatistics` method)
- Changing the properties of a device (the `ModifyAccount` method)
- Removing devices (the `RemoveAccount` method)

> You can identify other device management methods in the schema by the word `Account` in their names.

Adding backup devices in JSON-RPC API

To add a backup device, use the `AddAccount` method. Devices are added one at a time.

---

[1]A backup device is a piece of hardware (desktop, server or virtual machine) that has Backup Manager software installed to perform routine backup and restore operations. Each device is identified by a unique name, password and encryption key (required for installation and re-installation).

Required parameters

Parameter	Description	Type/Supported values
`accountInfo`	A group of parameters related to the device	`AccountInfo`, (has child parameters of its own see the AccountInfo child parameters table below)

AccountInfo child parameters

Parameter	Description	Type/Supported values
`ID`	An ID to assign to the new device. It must not coincide with the ID of existing devices	`<int>` Integer
`Name`	A name to assign to the new device. It must not coincide with the names of existing devices.	`OptionalNonEmptyString` String
`NameAlias`	An alternative name to assign to the new device. It must not coincide with this devices name or the names of existing devices.	`OptionalNonEmptyString` String
`Password`	A password to assign to the new device.	`OptionalNonEmptyString` String
`Token`	A token that will become the Encryption Key/Security Code for the new device	`OptionalNonEmptyString` String
`Type`	The type of device, based on what data will be backed up	`<AccountType::Enum>` ▪ `Undefined` ▪ `BackupManager` ▪ `Office365` ▪ `GSuite` ▪ `Count`
`PartnerId`	The ID of the customer the device is created for (retrieved through the `GetPartnerInfo` method)	`<int>` Integer
`ProductId`	The ID of the product to assign to the new device. Use the `EnumerateProducts` method to get the list of products available to the customer.	`<int>` Integer
`LocationId`	The location of the device. We recommend using the location of the customer that owns the device (unless you know that the customer has storage in the desired location). This can be found by running the `EnumerateLocations` method and finding the appropriate geographic region.	`<int>` Integer

Parameter	Description	Type/Supported values
`CreationTime`	The time code at which the device was created	`<std::time_t>` Integer in Unix format. For example, 1535673599 stands for August 30, 2018
`ExpirationTime`	The time code at which the device expires	`<std::time_t>` Integer in Unix format. For example, 1535673599 stands for August 30, 2018
`Flags`	An array of flags denoting the type of account	`<AccountFlags::FlagsType>` ▪ `Undefined` ▪ `Managed_Obsolete` ▪ `Trial` ▪ `Count`
`StorageLocationId`	The ID number of the storage location to be used for this new device	`<int>` Integer
`RemovalTime`	The time code at which the device will be removed	`<AbsoluteTime>` Integer as the total number of seconds since the beginning of January 1st 1900
`AccountGroupId`	The ID of the AccountGroup the device is associated to which can be found by running `GetAccountGroup`	`<int>` Integer
`OwnUserId`	The ID of the user running the call	`<int>` Integer
`StorageId`	The ID of the storage pool the device will be assigned to	`<int>` Integer
`ProfileId`	The ID of the profile to assign to the device.	`<int>` Integer
`ContinuityEnabled`	Enable or disable a continuity plan from an array	`ContinuityState::Enum` ▪ `Undefined` ▪ `Disabled` ▪ `RecoveryTesting` ▪ `StandbyImage` ▪ `Count`

Optional parameters

Parameter	Description	Type/Supported values
`homeNodeInfo`	A group of parameters related to the storage node	`StorageNodeInfo`, (has child parameters of its own, see the HomeNodeInfo child parameters table below)

HomeNodeInfo child parameters

Parameter	Description	Type/Supported values
`Id`	The ID number of the home storage node to assign to the device	`<int>` Integer
`ActiveAccounts`	Number of active devices associated to this storage node	`<int>` Integer
`TotalAccounts`	Total number of devices associated to this storage node	`<int>` Integer
`LocationId`	The location of the storage node. We recommend using the location of the customer that owns the node.	`<int>` Integer
`CommonInfo`	Common information regarding the Storage Node	`StorageNodeCommonInfo` (has child parameters of its own, see the StorageNodeCommonInfo child parameters table below)
`StateInfo`	State information regarding the Storage Node	`StorageNodeStateInfo` (has child parameters of its own, see the StorageNodeStateInfo child parameters table below)
`ModeInfo`	Mode information regarding the Storage Node	`StorageNodeModeInfo` (has child parameters of its own, see the StorageNodeModeInfo child parameters table below)

StorageNodeCommonInfo child parameters

Parameter	Description	Type/Supported values
`StorageID`	The ID number of the storage	`<int>` Integer
`Name`	The name of the storage node	`OptionalNonEmptyString` String
`Family`	The family of the storage node	`OptionalNonEmptyString` String
`User`	The username the storage node belongs to	`OptionalNonEmptyString` String
`Password`	The password of the storage node	`OptionalNonEmptyString` String
`Host`	The hostname of the	`OptionalNonEmptyString` String

Parameter	Description	Type/Supported values
	storage	
`Path`	The path to the storage node	`<std::string>`
`GatewayHost`	The gateway host of the storage node	`<std::string>`
`HttpGatwayHost`	The HTTP gateway host of the storage node	`<std::string>`
`CertificateInfo`	Certificate information for the storage node	`StorageNodeCertificateInfo` (has child parameters of its own, see the StorageNodeCertificateInfo child parameters table below)

StorageNodeCertificateInfo child parameters

Parameter	Description	Type/Supported values
`Certificate`	The certificate for the storage node	`<std::string>`
`StartDate`	The start date of the certificate	`<std::time_t>` Integer in Unix format. For example, 1535673599 stands for August 30, 2018
`EndDate`	The expiry date of the certificate	`<std::time_t>` Integer in Unix format. For example, 1535673599 stands for August 30, 2018
`CertificatePin`	The certificate pin	`<std::string>`

StorageNodeStateInfo child parameters

Parameter	Description	Type/Supported values
`State`	The state of the storage node	`storagenodestatetype::flagstype` ▪ `Undefined` ▪ `Online` ▪ `Full` ▪ `Migrated` ▪ `Decommissioned` ▪ `Count`
`UsedStorage`	The used storage on the storage node	`<std::int64_t>` Integer (in mebibytes)

Parameter	Description	Type/Supported values
`TotalStorage`	The total storage available on the storage node	`<std::int64_t>` Integer (in mebibytes)
`PrivilegedStorage`	The privileged storage on the storage node	`<std::int64_t>` Integer (in mebibytes)

StorageNodeModeInfo child parameters

Parameter	Description	Type/Supported values
`Mode`	The mode of the storage node	`storagenodemode::Enum` ▪ `Undefined` ▪ `Operable` ▪ `OutOfService` ▪ `Count`
`Message`	A note relative to the storage node mode	`<std::string>`

Sample request

The below example covers creating a very basic device with the minimum information. Once created in the Management Console, this device can be edited as needed, or changes can be made using the ModifyAccount method.

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "AddAccount",
    "jsonrpc": "2.0",
    "params": {
       "accountInfo": {
               "Name": "test-device",
               "PartnerId": 33495,
               "ProductId": 1,
               "LocationId": 1
       }
    }
}
```

Sample response

```
{
    "id":"jsonrpc",
```

```
    "jsonrpc":"2.0",
    "result":{
       "result":{
               "Id":72910,
               "Name":"test-device",
               "Password":"24e3ec5461ed",
               "Token":"068a53c1-a64b-45c8-a87e-0000XX0000X0Xx0"
       }
    },
    "visa":"{{visa}}"
}
```

Getting device info by name in JSON-RPC API

To get information about a backup device using its name and password, use the `GetAccountInfo` method.

Required parameters

Parameter	Description	Supported values
`name`	The name of the backup device to get information for	`<std::string>`
`password`	The password for access to the backup device	`<std::string>`

Optional parameters

Parameter	Description	Supported values
`homeNodeInfo`	A group of parameters related to the storage node	`StorageNodeInfo`, (has child parameters of its own, see the HomeNodeInfo child parameters table below)

HomeNodeInfo child parameters

Parameter	Description	Type/Supported values
`Id`	The ID number of the home storage node to assign to the device	`<int>` Integer
`ActiveAccounts`	Number of active devices associated to this storage node	`<int>` Integer
`TotalAccounts`	Total number of devices associated to this storage node	`<int>` Integer
`LocationId`	The location of the storage node. We recommend using the location of the customer that owns the node.	`<int>` Integer

Parameter	Description	Type/Supported values
`CommonInfo`	Common information regarding the Storage Node	`StorageNodeCommonInfo` (has child parameters of its own, see the StorageNodeCommonInfo child parameters table below)
`StateInfo`	State information regarding the Storage Node	`StorageNodeStateInfo` (has child parameters of its own, see the StorageNodeStateInfo child parameters table below)
`ModeInfo`	Mode information regarding the Storage Node	`StorageNodeModeInfo` (has child parameters of its own, see the StorageNodeModeInfo child parameters table below)

StorageNodeCommonInfo child parameters

Parameter	Description	Type/Supported values
`StorageID`	The ID number of the storage	`<int>` Integer
`Name`	The name of the storage node	`OptionalNonEmptyString` String
`Family`	The family of the storage node	`OptionalNonEmptyString` String
`User`	The username the storage node belongs to	`OptionalNonEmptyString` String
`Password`	The password of the storage node	`OptionalNonEmptyString` String
`Host`	The hostname of the storage	`OptionalNonEmptyString` String
`Path`	The path to the storage node	`<std::string>`
`GatewayHost`	The gateway host of the storage node	`<std::string>`
`HttpGatwayHost`	The HTTP gateway host of the storage node	`<std::string>`
`CertificateInfo`	Certificate information for the storage node	`StorageNodeCertificateInfo` (has child parameters of its own, see the StorageNodeCertificateInfo child parameters table below)

StorageNodeCertificateInfo child parameters

Parameter	Description	Type/Supported values
`Certificate`	The certificate for the storage node	`<std::string>`
`StartDate`	The start date of the certificate	`<std::time_t>` Integer in Unix format. For example, 1535673599 stands for August 30, 2018
`EndDate`	The expiry date of the certificate	`<std::time_t>` Integer in Unix format. For example, 1535673599 stands for August 30, 2018
`CertificatePin`	The certificate pin	`<std::string>`

StorageNodeStateInfo child parameters

Parameter	Description	Type/Supported values
`State`	The state of the storage node	`storagenodestatetype::flagstype` ▪ `Undefined` ▪ `Online` ▪ `Full` ▪ `Migrated` ▪ `Decommissioned` ▪ `Count`
`UsedStorage`	The used storage on the storage node	`<std::int64_t>` Integer (in mebibytes)
`TotalStorage`	The total storage available on the storage node	`<std::int64_t>` Integer (in mebibytes)
`PrivilegedStorage`	The privileged storage on the storage node	`<std::int64_t>` Integer (in mebibytes)

StorageNodeModeInfo child parameters

Parameter	Description	Type/Supported values
`Mode`	The mode of the storage node	`storagenodemode::Enum` ▪ `Undefined` ▪ `Operable` ▪ `OutOfService` ▪ `Count`
`Message`	A note relative to the storage node mode	`<std::string>`

Sample request

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "visa": "{{visa}}",
    "method": "GetAccountInfo",
    "params": {
           "name": "test-device",
           "password": "uadafjha36r"
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "homeNodeInfo": {
           "ActiveAccounts": 1084,
           "CommonInfo": {
               "CertificateInfo": {
                   "ValidationMethod": "OsTrustStore"
               },
               "Family": "WEBMOD",
               "GatewayHost": "",
               "Host": "hostname:port",
               "HttpGatewayHost": "hostname:port",
               "Name": "storageName",
               "Password": "*****",
               "Path": "",
               "StorageId": 1234567,
               "User": "*****"
           },
           "Id": 2345678,
           "LocationId": 1,
           "ModeInfo": {
               "Mode": "Operable"
           },
           "StateInfo": {
               "PrivilegedStorage": 0,
               "State": [
                   "Online"
```

```
                ],
                "TotalStorage": 269320579,
                "UpdateTimestamp": 1666347496,
                "UsedStorage": 210196248
            },
            "TotalAccounts": 165
        },
        "result": {
            "CreationTime": 1517402049,
            "ExpirationTime": 1535673599,
            "Id": 72896,
            "LocationId": 1,
            "Name": "test-device",
            "NameAlias": null,
            "OverrideVirtual": "Default",
            "PartnerId": 33495,
            "Password": "673487fcvg1",
            "ProductId": 28382,
            "RemovalTime": 0,
            "StorageId": 0,
            "StorageLocationId": 1,
            "Token": "3068a53c1-a64b-45c8-a87e-0000XX0000X0Xx0",
            "Type": "BackupManager"
        }
    },
    "visa": "{{visa}}"
}
```


Getting device info by ID in JSON-RPC API

To get information about a backup device by its ID, use the `GetAccountInfoById` method.

Required parameters

Parameter	Description	Supported values
`accountId`	The ID of the backup device to get information for. This information can be found when running the `GetAccountInfo` call which uses the account name.	`<int>` Integer

Optional parameters

Parameter	Description	Supported values
`homeNodeInfo`	A group of parameters related to the storage node	`StorageNodeInfo`, (has child parameters of its own, see the HomeNodeInfo child parameters table below)

HomeNodeInfo child parameters

Parameter	Description	Type/Supported values
`Id`	The ID number of the home storage node to assign to the device	`<int>` Integer
`ActiveAccounts`	Number of active devices associated to this storage node	`<int>` Integer
`TotalAccounts`	Total number of devices associated to this storage node	`<int>` Integer
`LocationId`	The location of the storage node. We recommend using the location of the customer that owns the node.	`<int>` Integer
`CommonInfo`	Common information regarding the Storage Node	`StorageNodeCommonInfo` (has child parameters of its own, see the StorageNodeCommonInfo child parameters table below)
`StateInfo`	State information regarding the Storage Node	`StorageNodeStateInfo` (has child parameters of its own, see the StorageNodeStateInfo child parameters table below)
`ModeInfo`	Mode information regarding the Storage Node	`StorageNodeModeInfo` (has child parameters of its own, see the StorageNodeModeInfo child parameters table below)

StorageNodeCommonInfo child parameters

Parameter	Description	Type/Supported values
`StorageID`	The ID number of the storage	`<int>` Integer
`Name`	The name of the storage node	`OptionalNonEmptyString` String
`Family`	The family of the storage node	`OptionalNonEmptyString` String
`User`	The username the	`OptionalNonEmptyString` String

Parameter	Description	Type/Supported values
	storage node belongs to	
`Password`	The password of the storage node	`OptionalNonEmptyString` String
`Host`	The hostname of the storage	`OptionalNonEmptyString` String
`Path`	The path to the storage node	`<std::string>`
`GatewayHost`	The gateway host of the storage node	`<std::string>`
`HttpGatwayHost`	The HTTP gateway host of the storage node	`<std::string>`
`CertificateInfo`	Certificate information for the storage node	`StorageNodeCertificateInfo` (has child parameters of its own, see the StorageNodeCertificateInfo child parameters table below)

StorageNodeCertificateInfo child parameters

Parameter	Description	Type/Supported values
`Certificate`	The certificate for the storage node	`<std::string>`
`StartDate`	The start date of the certificate	`<std::time_t>` Integer in Unix format. For example, 1535673599 stands for August 30, 2018
`EndDate`	The expiry date of the certificate	`<std::time_t>` Integer in Unix format. For example, 1535673599 stands for August 30, 2018
`CertificatePin`	The certificate pin	`<std::string>`

StorageNodeStateInfo child parameters

Parameter	Description	Type/Supported values
`State`	The state of the storage node	`storagenodestatetype::flagstype` ▪ `Undefined` ▪ `Online` ▪ `Full`

Parameter	Description	Type/Supported values
		▪ Migrated ▪ Decommissioned ▪ Count
UsedStorage	The used storage on the storage node	<std::int64_t> Integer (in mebibytes)
TotalStorage	The total storage available on the storage node	<std::int64_t> Integer (in mebibytes)
PrivilegedStorage	The privileged storage on the storage node	<std::int64_t> Integer (in mebibytes)

StorageNodeModeInfo child parameters

Parameter	Description	Type/Supported values
Mode	The mode of the storage node	storagenodemode::Enum ▪ Undefined ▪ Operable ▪ OutOfService ▪ Count
Message	A note relative to the storage node mode	<std::string>

Sample request

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "visa": "{{visa}}",
    "method": "GetAccountInfoById",
    "params": {
       "accountId": 72896
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
```

```
    "result": {
       "homeNodeInfo": {
           "ActiveAccounts": 1084,
           "CommonInfo": {
               "CertificateInfo": {
                   "ValidationMethod": "OsTrustStore"
               },
               "Family": "WEBMOD",
               "GatewayHost": "",
               "Host": "hostname:port",
               "HttpGatewayHost": "hostname:port",
               "Name": "storageName",
               "Password": "*****",
               "Path": "",
               "StorageId": 1234567,
               "User": "*****"
           },
           "Id": 2345678,
           "LocationId": 1,
           "ModeInfo": {
               "Mode": "Operable"
           },
           "StateInfo": {
               "PrivilegedStorage": 0,
               "State": [
                   "Online"
               ],
               "TotalStorage": 269320579,
               "UpdateTimestamp": 1666347496,
               "UsedStorage": 210196248
           },
           "TotalAccounts": 165
       },
       "result": {
           "CreationTime": 1517402049,
           "ExpirationTime": 1535673599,
           "Id": 72896,
           "LocationId": 1,
           "Name": "test-device",
           "NameAlias": null,
           "OverrideVirtual": "Default",
           "PartnerId": 33495,
           "Password": "673487fcvg1",
           "ProductId": 28382,
```

```
            "RemovalTime": 0,
            "StorageId": 0,
            "StorageLocationId": 1,
            "Token": "068a53c1-a64b-45c8-a87e-0000XX0000X0Xx0",
            "Type": "BackupManager"
        }
    },
    "visa": "{{visa}}"
}
```

Getting device info by Token in JSON-RPC API

To get information about a backup device by its token, use the `GetAccountInfoByToken` method.

Required parameters

Parameter	Description	Supported values
`token`	The token of the backup device to get information for	`<std::string>`

Optional parameters

Parameter	Description	Supported values
`AccontStorageInfo`	A group of parameters related to the device's storage	`AccountStorageInfo`, (has child parameters of its own, see the AccountStorageInfo child parameters table below)

AccountStorageInfo child parameters

Parameter	Description	Type/Supported values
`CabinetAccountNodeId`	The ID number of the cabinet account node to assign to the device	`<int>` Integer
`HomeAccountNodeId`	The ID number of the home account node to assign to the device	`<int>` Integer
`CabinetStorageNodeId`	The ID number of the cabinet storage node to assign to the device	`<int>` Integer
`HomeStorageNodeId`	The ID number of the home storage node to assign to the device	`<int>` Integer

Sample request

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "visa": "{{visa}}",
    "method": "GetAccountInfoByToken",
    "params": {
       "token": "068a53c1-a64b-45c8-a87e-0000XX0000X0Xx0"
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "accountStorageInfo": {
           "CabinetAccountNodeId": 1234567,
           "CabinetStorageNodeId": 2345678,
           "HomeAccountNodeId": 3456789,
           "HomeStorageNodeId": 4567890        },
       "result": {
           "CreationTime": 1530535000,
           "ExpirationTime": 1790640000,
           "Id": 654321,
           "LocationId": 1,
           "Name": "device1",
           "NameAlias": null,
           "OverrideVirtual": "Default",
           "PartnerId": 13579,
           "Password": "XXXXXXXXXX",
           "ProductId": 28345,
           "RemovalTime": 0,
           "StorageId": 0,
           "StorageLocationId": 1,
           "Token": "068a53c1-a64b-45c8-a87e-0000XX0000X0Xx0",
           "Type": "BackupManager"
       }
    },
    "visa": "{{visa}}"
}
```

Getting device ID in JSON-RPC API

To get a backup device's ID number, use the `GetAccountId` method.

Required parameters

Parameter	Description	Supported values
`accountName`	The name of the backup device to get the ID for	`<std::string>`
`accountPassword`	The password for access to the backup device	`<std::string>`

Sample request

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "visa": "{{visa}}",
    "method": "GetAccountId",
    "params": {
       "accountName": "device1",
       "accountPassword": "XXXXXXX"
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": 543210
    },
    "visa": "{{visa}}"
}
```

Enumerating Devices in JSON-RPC API

You can get the list of devices of your own company and your customers using the `EnumerateAccounts` method.

Required parameters

Parameter	Description	Supported values
partnerId	The ID of the customer whose devices you wish to list (retrieved through the GetPartnerInfo method)	<int> Integer

Sample request

```
{
    "id":"jsonrpc",
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "method" : "EnumerateAccounts",
    "params" : {
           "partnerId" : 123456
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
    "result": [
       {
           "CreationTime": 1543482480,
           "ExpirationTime": 2147483647,
           "Id": 135792,
           "LocationId": 1,
           "Name": "Testpc1",
           "NameAlias": null,
           "PartnerId": 123456,
           "Password": "111222c11011",
           "ProductId": 56789,
           "RemovalTime": 0,
           "StorageLocationId": 1,
           "Token": "9814bf0b-3a13-54jd-j972-0000XX0000X0Xx0",
           "Type": "BackupManager"
       },

       {
```

```
            "CreationTime": 1547372143,
            "ExpirationTime": 2147483647,
            "Id": 246801,
            "LocationId": 1,
            "Name": "Pctestingenviron1",
            "NameAlias": null,
            "PartnerId": 123456,
            "Password": "11ab22c33d44",
            "ProductId": 56789,
            "RemovalTime": 0,
            "StorageLocationId": 1,
            "Token": "530mw397-85dq-47hh-01d5-0000XX0000X0Xx0",
            "Type": "BackupManager"
        }
    ]
    },
    "visa": "{{visa}}"
}
```


Enumerating Device Statistics in JSON-RPC API

You can get the statistics of devices of your own company and your customers using the `EnumerateAccountStatistics` method.

A common use of this method is to output a list of storage space used on the cloud per device. You can get this information by using the `Columns` parameter and using the column `I14`.

> Please be aware that there are no methods which can perform complex calculations, however the `Totals` parameter can do basic calculations using column codes. If you need to do complex calculations, you will have to take the given sizes (in Bytes) and do these manually.

Required parameters

Parameter	Description	Supported values
`query`	A group of parameters related to the device statistics	`AccountStatisticsQuery` (has child parameters of its own, see the AccountStatisticsQuery child parameters table below)

AccountStatisticsQuery child parameters

Parameter	Description	Supported values
`PartnerId`	The ID of the customer the device is created for (retrieved through the `GetPartnerInfo` method)	`<int>` Integer

Parameter	Description	Supported values
`Filter`	Apply a search parameter using regularExpression	`<std::string>`
`ExcludedPartners`	A list of partner ID's to exclude from the search	`IdSet`
`SelectionMode`	An array of selection modes	`AccountStatisticsSelectionMode::Enum` ▪ `Undefined` ▪ `Merged` ▪ `PerInstallation` ▪ `Count`
`Labels`	Any labels to display	`<int>`
`StartRecordNumber`	Which device number to start the output from	`<std::size_t>` Integer (in mebibytes)
`RecordsCount`	How many devices to display	`<std::size_t>` Integer (in mebibytes)
`OrderBy`	How to order the displayed list of results	`<std::string>`
`Columns`	Which column vectors you wish to display in the response	`ColumnVector` (see API Column Codes for all options)
`Totals`	An array of totals represented as strings, will return totalStatistics. For Example: `["SUM (I14)","COUNT (I59==2)"],` This will return totalStatistics with the sum of used storage for the selected partner and filter and also a count of Cloud2Cloud devices	`TotalVector` ▪ `SUM` ▪ `COUNT` ▪ `MAX` ▪ `MIN`

Sample request

```
{
    "jsonrpc":"2.0",
    "id":"jsonrpc",
    "visa": "{{visa}}",
    "method" : "EnumerateAccountStatistics",
    "params" : {
```

```
        "query" : {
                "PartnerId" : 123456,
                "Filter": "ANY =~ 'Device*'",
                "SelectionMode": "Merged",
                "StartRecordNumber": 0,
                "RecordsCount": 3,
                "Columns": ["I1", "I14", "I18", "Do9F00", "D01F07"]
        }
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
        "result": [
            {
                "AccountId": 654321,
                "Flags": [
                    "AutoDeployed"
                ],
                "PartnerId": 123456,
                "Settings": [
                    {
                        "I1": "computerName"
                    },
                    {
                        "I14": "0"
                    },
                    {
                        "I78": "D01D02"
                    }
                ]
            },
            {
                "AccountId": 765432,
                "Flags": null,
                "PartnerId": 456789,
                "Settings": [
                    {
                        "D01F07": "28349567768726"
                    },
```

```
                    {
                        "D09F00": "1"
                    },
                    {
                        "I1": "computerName2"
                    },
                    {
                        "I14": "586755749630"
                    },
                    {
                        "I78": "D01D02"
                    }
                ]
            },
            {
                "AccountId": 876543,
                "Flags": null,
                "PartnerId": 456789,
                "Settings": [
                    {
                        "D09F00": "5"
                    },
                    {
                        "I1": "computerName3"
                    },
                    {
                        "I14": "23630480"
                    },
                    {
                        "I78": "D19D20D05"
                    }
                ]
            }
        ],
        "totalStatistics": null
    },
    "visa": "{{visa}}"
}
```


Changing device properties in JSON-RPC API

To modify a backup device, use the `ModifyAccount` method. You can change the following properties:

- Re-assign the device to another customer
- Change the amount of storage allocated to the device

- Set an expiration time for the device
- Change the location of the device
- Re-assign the device to another storage pool

> Device names and passwords cannot be changed.

Required parameters

Parameter	Description	Type/Supported values
`accountInfo`	A group of parameters related to the device	`AccountInfo`, (has child parameters of its own see the AccountInfo child parameters table below)

AccountInfo child parameters

Parameter	Description	Type/Supported values
`ID`	An ID to assign to the new device. It must not coincide with the ID of existing devices	`<int>` Integer
`Name`	A name to assign to the new device. It must not coincide with the names of existing devices.	`OptionalNonEmptyString` String
`NameAlias`	An alternative name to assign to the new device. It must not coincide with this devices name or the names of existing devices.	`OptionalNonEmptyString` String
`Password`	A password to assign to the new device.	`OptionalNonEmptyString` String
`Token`	A token that will become the Encryption Key/Security Code for the new device	`OptionalNonEmptyString` String
`Type`	The type of device, based on what data will be backed up	`<AccountType::Enum>` ▪ `Undefined` ▪ `BackupManager` ▪ `Office365` ▪ `GSuite` ▪ `Count`
`PartnerId`	The ID of the customer the device is created for (retrieved through the `GetPartnerInfo` method)	`<int>` Integer
`ProductId`	The ID of the product to assign to the new device. Use the `EnumerateProducts` method to get the list of products available to the customer.	`<int>` Integer

Parameter	Description	Type/Supported values
`LocationId`	The location of the device. We recommend using the location of the customer that owns the device (unless you know that the customer has storage in the desired location). This can be found by running the `EnumerateLocations` method and finding the appropriate geographic region.	`<int>` Integer
`CreationTime`	The time code at which the device was created	`<std::time_t>` Integer in Unix format. For example, 1535673599 stands for August 30, 2018
`ExpirationTime`	The time code at which the device expires	`<std::time_t>` Integer in Unix format. For example, 1535673599 stands for August 30, 2018
`Flags`	An array of flags denoting the type of account	`<AccountFlags::FlagsType>` ▪ `Undefined` ▪ `Managed_Obsolete` ▪ `Trial` ▪ `Count`
`StorageLocationId`	The ID number of the storage location to be used for this new device	`<int>` Integer
`RemovalTime`	The time code at which the device will be removed	`<AbsoluteTime>` Integer as the total number of seconds since the beginning of January 1st 1900
`AccountGroupId`	The ID of the AccountGroup the device is associated to which can be found by running `GetAccountGroup`	`<int>` Integer
`OwnUserId`	The ID of the user running the call	`<int>` Integer
`StorageId`	The ID of the storage pool the device will be assigned to	`<int>` Integer
`ProfileId`	The ID of the profile to assign to the device.	`<int>` Integer
`ContinuityEnabled`	Enable or disable a continuity plan from an array	`ContinuityState::Enum` ▪ `Undefined` ▪ `Disabled` ▪ `RecoveryTesting` ▪ `StandbyImage` ▪ `Count`

Optional parameters

Parameter	Description	Supported values
`forceRemoveCustomColumnValuesInOldScope`	Do you wish to force remove custom column values for the device	`bool` Boolean ▪ `True` ▪ `False`

Sample request

In the below example, we are going to re-assign a device to another customer. To do so, submit the ID of the new customer together with the device name.

All other changes can be made by providing the new setting, information or value for the required parameter.

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "ModifyAccount",
    "jsonrpc": "2.0",
    "params": {
       "accountInfo": {
           "PartnerId": 33493,
           "Name": "test-device",
           "NameAlias": "Test-Device-Alias"
       }
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": null,
    "visa": "{{visa}}"
}
```

Removing devices in JSON-RPC API

To remove a backup device, use the `RemoveAccount` method.

Devices are removed together with **all data** that has been backed up for them. There is no way to restore the data after the device has been deleted from the system.

Required parameters

Parameter	Description	Supported values
`accountId`	The ID of the backup device to remove	`<int>` Integer

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "RemoveAccount",
    "jsonrpc": "2.0",
    "params": {
       "accountId": 72899
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": null,
    "visa": "{{visa}}"
}
```

Customer management methods in JSON-RPC API

A **customer** is a company (or a group within a company) that consumes or distributes backup services and are known as Partners within the JSON-RPC API methods. Customers are organized in a hierarchy with Distributor at the top level.

Customers own **backup devices**. Each customer is identified by a unique name or ID.

Below is the list of **primary methods** that let you manage customers.

- Adding a new customer (the `AddPartner` method)
- Getting a list of customers for a company (the `EnumeratePartners` method)

- Getting a list of customer properties (the `EnumeratePartnerProperties` method)
- Getting a list of child customers (the `EnumerateChildPartners` method)
- Getting customer information by name (the `GetPartnerInfo` method)
- Getting customer information by ID (the `GetPartnerInfoById` method)
- Getting customer information by UID (the `GetPartnerInfoByUid` method)
- Getting customer information history (the `GetPartnerInfoHistory` method)
- Getting customer state (the `GetPartnerState` method)
- Getting a customer tree (the `GetPartnerTree` method)
- Regenerate the customer UID (the `RegeneratePartnerUid` method)
- Changing the properties of a customer (the `ModifyPartner` method)
- Removing a customer (the `RemovePartner` method)

> You can identify other customer management methods in the schema by the word `Partner` in their names.

Adding customers in JSON-RPC API

To add customers, use the `AddPartner` method. Customers are added one at a time.

Required parameters

Parameter	Description	Supported values
`partnerInfo`	A group of parameters related to the partner	`PartnerInfo`, (has child parameters of its own see the PartnerInfo child parameters table below)
`createDefaultAccount`	The type of account to be created	`bool` Boolean ▪ `True` ▪ `False`

PartnerInfo child parameters

Parameter	Description	Supported values
`ID`	The ID of the Customer	`<int>` Integer
`ParentId`	The ID of the parent customer	`<int>` Integer
`Name`	The name to assign to the customer	`OptionalNonEmptyString` String
`Level`	The level of the customer in the hierarchy tree	`<PartnerPrivilege::Enum>` ▪ `Undefined`

Parameter	Description	Supported values
	(must be lower than the level of the parent customer)	▪ `Distributor` ▪ `SubDistributor` ▪ `Reseller` ▪ `EndCustomer`
`ChildServiceTypes`	The type of service the customer company can provide to its own customers	`<PartnerServiceType::FlagsType>` ▪ `Undefined` ▪ `AllInclusive` ▪ `SoftwareOnly`
`ServiceType`	The type of service provided to the customer	`<PartnerServiceType::Enum>` ▪ `Undefined` ▪ `AllInclusive` ▪ `SoftwareOnly`
`State`	The current state of the customer	`<PartnerState::Enum>` ▪ `Undefined` ▪ `InProduction` ▪ `InTrial`
`DeviceCountry`	The country the device is in	`<std::string>`
`LocationId`	The location that the customer is assigned to (it is used to set a default storage pool for the customer's devices). Normally, the location is identified automatically by the country in which a customer is located (the `Country` parameter), but you can specify it	`<int>` Integer You can get the list of available locations using the `EnumerateLocations` method

Parameter	Description	Supported values
	yourself as well.	
`Flags`	Properties the customer has configured	`<PartnerFlag::FlagsType>` ▪ `Undefined` ▪ `HasCustomBranding` ▪ `HasCustomUpdatePackages` ▪ `UnsubscribedFromTrialNotifications` ▪ `CanInvoiceOthers` ▪ `Count`
`Company`	A group of parameters related to the company	`PartnerCompanyInfo` (has child parameters of its own see the PartnerCompanyInfo child parameters table below)
`TrialRegistrationTime`	The timestamp that the trial was registered for the Customer	`<std::time_t>` Integer in Unix format. For example, 1535673599 stands for August 30, 2018
`TrialExpirationTime`	The timestamp of when the trial will expire for the Customer	`<std::time_t>` Integer in Unix format. For example, 1535673599 stands for August 30, 2018
`AdvancedPartnerProperties`	Advanced information relating to the Partner	`AdvancedPartnerPropertiesInfo` (has child parameters of its own see the AdvancedPartnerPropertiesInfo child parameters table below)

PartnerCompanyInfo Child Parameters

Parameter	Description	Supported values
`PostAddress`	The postal address for the Customer's company	`PostAddressInfo` (has child parameters of its own see the PostAddress child parameters table below)
`PhoneNumber`	The phone number for the Customer's company	`<std::String>` String
`FaxNumber`	The fax number for the Customer's company	`<std::String>` String
`WebsiteAddress`	The website address in full for the Customer's company	`<std::String>` String
`LegalCompanyName`	The legal name of the Customer's	`<std::String>` String

Parameter	Description	Supported values
	company	
`ChamberOfCommerceNumber`	The chamber of commerce number for the Customer's company	`<std::String>` String
`VatNumber`	The VAT number for the Customer's company	`<std::String>` String
`BankAccountNumber`	The bank account number for the Customer's company	`<std::String>` String
`BillingContactPersonId`	The ID for the person to contatc with regards to billing for the Customer's company	`<std::String>` String

PostAddressInfo Child parameters

Parameter	Description	Supported values
`Country`	The country in which the customer is located. Based on the country, each customer is assigned to a location (see the `LocationId` parameter). Several neighboring countries may belong to the same location. The location is used to set a default **storage pool** for devices belonging to the customer.	`<std::String>` String Country code in ISO Alpha-2 format (recommended) or official country/area name in English. If the parameter is not submitted, the location of the parent customer is used.
`State`	The state in which the customer is located	`<std::String>` String
`District`	The district in which the customer is located	`<std::String>` String
`City`	The city in which the customer is located	`<std::String>` String
`ZipCode`	The ZipCode in which the customer is located	`<std::String>` String
`Address`	The street address at which the customer is located	`<std::String>` String

AdvancedPartnerPropertiesInfo Child Parameters

Parameter	Description	Supported Values
`RegionId`	The ID number for the region the customer is in	`<int>` Integer

Parameter	Description	Supported Values
`ResponsibleUserId`	The ID for the responsible user	`<int>` Integer

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "AddPartner",
    "jsonrpc": "2.0",
    "params": {
       "partnerInfo": {
           "ParentId": 12345,
           "Name": "Zeus & Sons",
           "Level": "EndCustomer",
           "ServiceType": "AllInclusive",
           "ChildServiceTypes": [
               "AllInclusive"
           ],
           "Country": "Greece"
           }
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": 55806
    },
    "visa": "{{visa}}"
}
```

Enumerating customers in JSON-RPC API

To get the list of customers for your own company or your customers, use the `EnumeratePartners` method.

Required parameters

Parameter	Description	Supported values
`parentPartnerId`	The ID of the parent customer	`<int>` Integer

Optional parameters

Parameter	Description	Supported values
`fetchRecursively`	The range of customers to retrieve	`bool` Boolean ▪ `true` (returns the full list of customers) ▪ `false` (returns only 1 level of customers)
`fields`	Lets you specify the type of information you need	`PartnerFields` Numbers of fields separated by a comma in square brackets: ▪ `0` - Name ▪ `1` - Level ▪ `3` - ChildServiceTypes ▪ `4` - ServiceType ▪ `5` - State ▪ `8` - LocationId ▪ `9` - Flags ▪ `10` - Company info ▪ `18` - ExternalCode, MailFrom ▪ `20` - CreationTime

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "EnumeratePartners",
    "jsonrpc": "2.0",
    "params": {
           "parentPartnerId": 12345,
           "fields": [0, 1, 3, 4, 5, 8],
           "fetchRecursively": true
    }
}
```

Sample response


```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result":       [
           {
               "ChildServiceTypes":
               [
                   "AllInclusive",
                   "SoftwareOnly"
               ],
                   "Company": {"PostAddress": null},
                   "ExternalPartnerProperties": null,
                   "Id": 45678,
                   "Level": "SubDistributor",
                   "LocationId": 1,
                   "Name": "WindowsDevices",
                   "ParentId": 12345,
                   "ServiceType": "AllInclusive",
                   "State": "InTrial"
           },
           {
               "ChildServiceTypes":
               [
                   "AllInclusive",
                   "SoftwareOnly"
               ],
                   "Company": {"PostAddress": null},
                   "ExternalPartnerProperties": null,
                   "Id": 34567,
                   "Level": "SubDistributor",
                   "LocationId": 1,
                   "Name": "LinuxDevices",
                   "ParentId": 12345,
                   "ServiceType": "AllInclusive",
                   "State": "Registered"
           },
           {
                   "ChildServiceTypes": null,
                   "Company": {"PostAddress": null},
                   "ExternalPartnerProperties": null,
                   "Id": 23456,
                   "Level": "EndCustomer",
```

```
                    "LocationId": 1,
                    "Name": "Zeus & Sons",
                    "ParentId": 12345,
                    "ServiceType": "AllInclusive",
                    "State": "Registered"
            }
            ]
    },
    "visa": "{{visa}}"
}
```

Enumerating customer properties in JSON-RPC API

To get the list of properties for your own company or your customer's, use the `EnumeratePartnerProperties` method.

Required parameters

Parameter	Description	Supported values
`partnerId`	The ID of the customer	`<int>` Integer

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "EnumeratePartnerProperties",
    "jsonrpc": "2.0",
    "params": {
           "partnerId": 12345
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": [
           {
               "Id": 23,
               "Name": "AllowNonLoopbackAccess"
```

```
            },
            {
                "Id": 1,
                "Name": "AllowedAutoUpdatePolicies"
            },
            {
                "Id": 3,
                "Name": "AutomaticPaymentStatus"
            },
            {
                "Id": 5,
                "Name": "CreditCardInfo"
            },
            {
                "Id": 7,
                "Name": "DefaultUserEmail"
            },
            {
                "Id": 6,
                "Name": "DoubleCheckAvailable"
            },
            {
                "Id": 8,
                "Name": "EulaAccepted"
            },
            {
                "Id": 9,
                "Name": "GoogleAnalyticsId"
            },
            {
                "Id": 10,
                "Name": "Id3"
            },
            {
                "Id": 11,
                "Name": "Id4"
            },
            {
                "Id": 12,
                "Name": "Id5"
            },
            {
                "Id": 13,
                "Name": "Id6"
```

```
            },
            {
                "Id": 14,
                "Name": "LiveChatAvailable"
            },
            {
                "Id": 24,
                "Name": "O365_EAP_Partner"
            },
            {
                "Id": 15,
                "Name": "OriginIPAddress"
            },
            {
                "Id": 16,
                "Name": "OriginKeywordId"
            },
            {
                "Id": 17,
                "Name": "OriginUserAgent"
            },
            {
                "Id": 4,
                "Name": "PartnerBillingType"
            },
            {
                "Id": 21,
                "Name": "PartnerStateChangePolicy"
            },
            {
                "Id": 18,
                "Name": "RegistrationSource"
            },
            {
                "Id": 19,
                "Name": "RegistrationURL"
            },
            {
                "Id": 20,
                "Name": "StorageNodeLiability"
            },
            {
                "Id": 22,
                "Name": "TrackingToken"
```

```
            },
            {
                "Id": 2,
                "Name": "VisiblePartnerEntityName"
            }
        ]
    },
    "visa": "{{visa}}"
}
```

Enumerating child customers in JSON-RPC API

To get the list of child customers for your own company or your customers, use the `EnumerateChildPartners` method.

Required parameters

Parameter	Description	Supported values
`partnerId`	The ID of the customer	`<int>` Integer
`range`	Provide a display range of how many child customers to display	`<std::size_t>`
`partnerFilter`	Provide additional criteria to filter the list of child customers by	`PartnerTreeFilter`, (has child parameters of its own see the PartnerTreeFilter table below)

PartnerTreeFilter Child Parameters

Parameter	Description	Supported values
`States`	An array to chose from of the state of the customer	`PartnerState::Enum` ▪ `Undefined` ▪ `Registered` ▪ `InProduction` ▪ `Rejected` ▪ `InTrial` ▪ `NotActive` ▪ `WaitingForProduction` ▪ `Expired` ▪ `Count`
`NamePattern`	Filter child customer names by specific text	`<std::string>`
`Levels`	An array of customer levels	`PartnerLevel::Enum`

Parameter	Description	Supported values
		▪ Undefined ▪ Root ▪ SubRoot ▪ Distributor ▪ SubDistributor ▪ Reseller ▪ EndCustomer ▪ Site ▪ Count
SortOrder	An array of ways of sorting the results	PartnerTreeSortOrder::Enum ▪ Undefined ▪ ById ▪ ByName ▪ ByLevelAndName ▪ ByCreationTime ▪ Count

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "EnumerateChildPartners",
    "jsonrpc": "2.0",
    "params": {
           "partnerId": 12345
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": {
           "ActualChildCount": 7,
           "Children": null,
```

```
        "Info": {
            "AdvancedPartnerProperties": {
                "RegionId": 8
                },
            "ChildServiceTypes": [
                "AllInclusive",
                "SoftwareOnly"
            ],
            "Company": {
                "BankAccountNumber": "0",
                "BillingContactPersonId": 019283,
                "ChamberOfCommerceNumber": "",
                "FaxNumber": "",
                "LegalCompanyName": "Zeus & Sons",
                "PhoneNumber": "",
                "PostAddress": {
                    "Address": "x",
                    "City": "x",
                    "Country": "NL",
                    "District": "",
                    "State": "",
                    "ZipCode": ""
            },
            "VatNumber": "AB123 456789",
            "WebsiteAddress": ""
        },
        "CreationTime": 1879064897,
        "ExternalCode": "",
        "ExternalPartnerProperties": {
            "GreatPlainsId": 09876,
            "Properties": [
                [
                    "AutomaticPaymentStatus",
                    "0"
                ]
            ]
        },
        "Flags": [
            "HasCustomBranding"
        ],
        "Guid": "123a4567-8901-2bcd-ef34-56g7h89i0123",
        "Id": 1,
        "Level": "Root",
        "LocationId": 1,
```

```
            "MailFrom": "backup@n-able.com",
            "Name": "IASO",
            "ParentId": 0,
            "PrivateFlags": null,
            "RegistrationOrigin": "Undefined",
            "ServiceType": "AllInclusive",
            "State": "InProduction",
            "TrialExpirationTime": 0,
            "TrialRegistrationTime": 0,
            "Uid": "z09yxw87-6v5u-4ts3-rq2p-o10nm987l6k5j4"
            }
        }
    },
    "visa": "{{visa}}"
}
```

Getting Customer Information By Name in JSON-RPC API

To get information on a customer, use the `GetPartnerInfo` method.

Required parameters

Parameter	Purpose	Supported values
`name`	The name of the customer to get details for	`<std::String>` String

Sample request

```
{
    "id": "jsonrpc",
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "method":"GetPartnerInfo",
    "params":{
            "name":"Zeus & Sons"
    }
}
```

Sample response

```
{
    "id":"jsonrpc",
    "jsonrpc":"2.0",
```

```
    "result":{
       "result":{
               "AdvancedPartnerProperties":null,
               "ChildServiceTypes": null,
               "Company":{
                       "BankAccountNumber":"",
                       "BillingContactPersonId":0,
                       "ChamberOfCommerceNumber":"111FF1000",
                       "FaxNumber":"+121340000",
                       "LegalCompanyName":"Zeus & Sons",
                       "PhoneNumber":"+234567890000",
                       "PostAddress":{
                               "Address":"1 Godly Road",
                               "City":"Olympus",
                               "Country":"Greece",
                               "ZipCode":"ABC123"
                       },
                       "VatNumber":"CY99999999L",
                       "WebsiteAddress":"www.zeus-and-sons.com"
               },
               "CreationTime":1464945793,
               "ExternalCode":"",
               "Flags":null,
               "Id":12345,
               "Level":"Distributor",
               "LocationId":1,
               "MailFrom":"",
               "MailingOption":"Undefined",
               "Name":"Zeus & Sons",
               "ParentId":23456,
               "PrivateFlags":null,
               "RegistrationOrigin":"Domestic",
               "State":"InTrial",
               "TrialExpirationTime":1467537793,
               "TrialRegistrationTime":1464945793,
               "Uid":"abcdef-1234-5678-ghij-lmn901e162e9",
               "UpdatePackagesMaxAllowedVersion":""
       }
    },
    "visa":"{{visa}}"
}
```


Getting Customer Information By ID in JSON-RPC API

To get information on a customer using the customer's ID, use the `GetPartnerInfoById` method.

Required parameters

Parameter	Description	Supported values
`partnerId`	The ID of the customer the device is created for (retrieved through the `GetPartnerInfo` method)	`<int>` Integer

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "GetPartnerInfoById",
    "jsonrpc": "2.0",
    "params": {
       "partnerId": 12345
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": {
               "AdvancedPartnerProperties": {
                       "RegionId": 0,
                       "ResponsibleUserId": 0
               },
               "ChildServiceTypes": [
                       "AllInclusive",
                       "SoftwareOnly"
               ],
               "Company": {
                       "BankAccountNumber": "",
                       "BillingContactPersonId": 0,
                       "ChamberOfCommerceNumber": "111FF1000",
                       "FaxNumber": "+121340000",
                       "LegalCompanyName": "Zeus & Sons",
                       "PhoneNumber": "+234567890000",
                       "PostAddress": {
                               "Address": "1 Godly Road",
```

```
                                "City": "Olympus",
                                "Country": "Greece",
                                "ZipCode": "ABC123"
                        },
                        "VatNumber": "CY99999999L",
                        "WebsiteAddress": "www.zeus-and-sons.com"
                },
                "CreationTime": 1464945793,
                "ExternalCode": "",
                "Flags": null,
                "Id": 12345,
                "Level": "Distributor",
                "LocationId": 1,
                "MailFrom": "",
                "MailingOption": "Undefined",
                "Name": "Zeus & Sons",
                "ParentId": 23456,
                "PrivateFlags": null,
                "Privilege": "Regular",
                "RegistrationOrigin": "Domestic",
                "ServiceType": "AllInclusive",
                "State": "InTrial",
                "TrialExpirationTime": 1467537793,
                "TrialRegistrationTime": 1464945793,
                "Uid": "abcdef-1234-5678-ghij-lmn901e162e9",
                "UpdatePackagesMaxAllowedVersion": ""
        }
    },
    "visa": "{{visa}}"
}
```


Getting Customer Information by UID in JSON-RPC API

To get information on a customer using the customer's UID, use the `GetPartnerInfoByUid` method.

Required parameters

Parameter	Description	Supported values
`partnerUid`	The UID of the customer the device is created for (retrieved through the `GetPartnerInfo` method)	`<std::string>`

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "GetPartnerInfoByUid",
    "jsonrpc": "2.0",
    "params": {
       "partnerUid": "abcdef-1234-5678-ghij-lmn901e162e9"
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": {
               "AdvancedPartnerProperties": {
                       "RegionId": 0,
                       "ResponsibleUserId": 0
               },
               "ChildServiceTypes": [
                       "AllInclusive",
                       "SoftwareOnly"
               ],
               "Company": {
                       "BankAccountNumber": "",
                       "BillingContactPersonId": 0,
                       "ChamberOfCommerceNumber": "111FF1000",
                       "FaxNumber": "+121340000",
                       "LegalCompanyName": "Zeus & Sons",
                       "PhoneNumber": "+234567890000",
                       "PostAddress": {
                               "Address": "1 Godly Road",
                               "City": "Olympus",
                               "Country": "Greece",
                               "ZipCode": "ABC123"
                       },
                       "VatNumber": "CY99999999L",
                       "WebsiteAddress": "www.zeus-and-sons.com"
               },
               "CreationTime": 1464945793,
```

```
                "ExternalCode": "",
                "Flags": null,
                "Guid": "a12b3c4d-567e-8f90-gh12-i345j678k90l",
                "Id": 12345,
                "Level": "Distributor",
                "LocationId": 1,
                "MailFrom": "",
                "MailingOption": "Undefined",
                "Name": "Zeus & Sons",
                "ParentId": 23456,
                "PrivateFlags": null,
                "Privilege": "Regular",
                "RegistrationOrigin": "Domestic",
                "ServiceType": "AllInclusive",
                "State": "InTrial",
                "TrialExpirationTime": 1467537793,
                "TrialRegistrationTime": 1464945793,
                "Uid": "abcdef-1234-5678-ghij-lmn901e162e9"
        }
    },
    "visa": "{{visa}}"
}
```


Getting Customer Information History in JSON-RPC API

To get information on a customer's history using the customer's ID, use the `GetPartnerInfoHistory` method.

Required parameters

Parameter	Description	Supported values
`partnerId`	The ID of the customer the device is created for (retrieved through the `GetPartnerInfo` method)	`<std::string>`

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "GetPartnerInfoHistory",
    "jsonrpc": "2.0",
    "params": {
       "partnerId": 123456
```

```
    }
}
```

Sample response


```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": [
           [
               {
                   "Company": {
                       "PostAddress": null
                       },
                   "ExternalPartnerProperties": null,
                   "Id": 123456,
                   "Level": "Reseller",
                   "Name": null,
                   "ParentId": 123456
               },
               {
                   "Timestamp": 1530019465
               }
           ],
           [
               {
                   "Company": {
                       "PostAddress": null
                   },
                   "ExternalPartnerProperties": null,
                   "Id": 123456,
                   "Level": "Reseller",
                   "Name": null,
                   "ParentId": 234567
               },
               {
                   "Timestamp": 1674213687
               }
           ],
           [
               {
                   "Company": {
                       "PostAddress": null
```

```
                    },
                    "ExternalPartnerProperties": null,
                    "Id": 123456,
                    "Level": "Reseller",
                    "Name": null,
                    "ParentId": 234567
                },
                {
                    "Timestamp": 1674213688
                }
            ]
        ]
    },
    "visa": "{{visa}}"
}
```


Getting Customer State in JSON-RPC API

To get the current State of a customer using the customer's ID, use the `GetPartnerState` method.

Required parameters

Parameter	Description	Supported values
`partnerId`	The ID of the customer the device is created for (retrieved through the `GetPartnerInfo` method)	`<std::string>`

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "GetPartnerState",
    "jsonrpc": "2.0",
    "params": {
       "partnerId": 123456
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": "InProduction"
    },
    "visa": "{{visa}}"
}
```

Getting Customer Tree in JSON-RPC API

To get a list of a customer's child partners using the customer's ID, use the `GetPartnerTree` method.

Required parameters

Parameter	Description	Supported values
`partnerId`	The ID of the customer the device is created for (retrieved through the `GetPartnerInfo` method)	`<std::string>`

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "GetPartnerTree",
    "jsonrpc": "2.0",
    "params": {
       "partnerId": 123456
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": {
       "ActualChildCount": 4,
```

```
            "Children": [
                {
                    "ActualChildCount": 0,
                    "Children": null,
                    "Info": {
                        "Company": {
                            "PostAddress": null
                        },
                        "ExternalPartnerProperties": null,
                        "Id": 345678,
                        "Level": "EndCustomer",
                        "Name": null,
                        "ParentId": 123456
                    }
                },
                {
                    "ActualChildCount": 1,
                    "Children": null,
                    "Info": {
                        "Company": {
                            "PostAddress": null
                            },
                        "ExternalPartnerProperties": null,
                        "Id": 456789,
                        "Level": "EndCustomer",
                        "Name": null,
                        "ParentId": 273266
                    }
                },
                {
                    "ActualChildCount": 0,
                    "Children": null,
                    "Info": {
                        "Company": {
                            "PostAddress": null
                            },
                        "ExternalPartnerProperties": null,
                        "Id": 567890,
                        "Level": "EndCustomer",
                        "Name": null,
                        "ParentId": 123456
                    }
                },
                {
```

```
                    "ActualChildCount": 0,
                    "Children": null,
                    "Info": {
                        "Company": {
                            "PostAddress": null
                            },
                        "ExternalPartnerProperties": null,
                        "Id": 678901,
                        "Level": "EndCustomer",
                        "Name": null,
                        "ParentId": 123456
                    }
                }
            ],
            "Info": {
                "Company": {
                    "PostAddress": null
                },
                "ExternalPartnerProperties": null,
                "Id": 123456,
                "Level": "Reseller",
                "Name": null,
                "ParentId": 012345
            }
        }
    },
    "visa": "{{visa}}"
}
```


Regenerate a Customer UID on JSON-RPC API

To regenerate a customer's UID using the customer's ID, use the `RegeneratePartnerUid` method.

Required parameters

Parameter	Description	Supported values
`partnerId`	The ID of the customer the device is created for (retrieved through the `GetPartnerInfo` method)	`<std::string>`

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "GetPartnerInfoHistory",
    "jsonrpc": "2.0",
    "params": {
       "partnerId": 123456
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": "123456a7-bc8d-9e01-f2gh-000xxxxx0xx0000xx000"
    },
    "visa": "{{visa}}"
}
```

Changing customer properties in JSON-RPC API

To change the properties of an existing customer, use the `ModifyPartner` method.You can change the following properties:

- Re-assign the customer to another customer
- Change the service types provided to the customer
- Set flags to the customer
- Change the address of the customer
- Change a trial customer to in production

> Customer ID's cannot be changed.

Required parameters

Parameter	Description	Supported values
`partnerInfo`	A group of parameters related to the partner	`PartnerInfo` (has child parameters of its own see the PartnerInfo child parameters table below)

PartnerInfo child parameters

Parameter	Description	Supported values
`ID`	The ID of the Customer	`<int>` Integer
`ParentId`	The ID of the parent customer	`<int>` Integer
`Name`	The name to assign to the customer	`OptionalNonEmptyString` String
`Level`	The level of the customer in the hierarchy tree (must be lower than the level of the parent customer)	`<PartnerPrivilege::Enum>` ▪ `Undefined` ▪ `Distributor` ▪ `SubDistributor` ▪ `Reseller` ▪ `EndCustomer`
`ChildServiceTypes`	The type of service the customer company can provide to its own customers	`<PartnerServiceType::FlagsType>` ▪ `Undefined` ▪ `AllInclusive` ▪ `SoftwareOnly`
`ServiceType`	The type of service provided to the customer	`<PartnerServiceType::Enum>` ▪ `Undefined` ▪ `AllInclusive` ▪ `SoftwareOnly`
`State`	The current state of the customer	`<PartnerState::Enum>` ▪ `Undefined` ▪ `InProduction` ▪ `InTrial`
`DeviceCountry`	The country the device is in	`<std::string>`
`LocationId`	The location that the customer is assigned to (it is used to set a default storage pool for the customer's devices).	`<int>` Integer You can get the list of available locations using the `EnumerateLocations` method

Parameter	Description	Supported values
	Normally, the location is identified automatically by the country in which a customer is located (the `Country` parameter), but you can specify it yourself as well.	
`Flags`	Properties the customer has configured	`<PartnerFlag::FlagsType>` ▪ `Undefined` ▪ `HasCustomBranding` ▪ `HasCustomUpdatePackages` ▪ `UnsubscribedFromTrialNotifications` ▪ `CanInvoiceOthers` ▪ `Count`
`Company`	A group of parameters related to the company	`PartnerCompanyInfo` (has child parameters of its own see the PartnerCompanyInfo child parameters table below)
`TrialRegistrationTime`	The timestamp that the trial was registered for the Customer	`<std::time_t>` Integer in Unix format. For example, 1535673599 stands for August 30, 2018
`TrialExpirationTime`	The timestamp of when the trial will expire for the Customer	`<std::time_t>` Integer in Unix format. For example, 1535673599 stands for August 30, 2018
`AdvancedPartnerProperties`	Advanced information relating to the Partner	`AdvancedPartnerPropertiesInfo` (has child parameters of its own see the AdvancedPartnerPropertiesInfo child parameters table below)

PartnerCompanyInfo Child Parameters

Parameter	Description	Supported values
`PostAddress`	The postal address for the Customer's company	`PostAddressInfo` (has child parameters of its own see the PostAddress child

Parameter	Description	Supported values
		parameters table below)
`PhoneNumber`	The phone number for the Customer's company	`<std::String>` String
`FaxNumber`	The fax number for the Customer's company	`<std::String>` String
`WebsiteAddress`	The website address in full for the Customer's company	`<std::String>` String
`LegalCompanyName`	The legal name of the Customer's company	`<std::String>` String
`ChamberOfCommerceNumber`	The chamber of commerce number for the Customer's company	`<std::String>` String
`VatNumber`	The VAT number for the Customer's company	`<std::String>` String
`BankAccountNumber`	The bank account number for the Customer's company	`<std::String>` String
`BillingContactPersonId`	The ID for the person to contatc with regards to billing for the Customer's company	`<std::String>` String

PostAddressInfo Child parameters

Parameter	Description	Supported values
`Country`	The country in which the customer is located. Based on the country, each customer is assigned to a location (see the `LocationId` parameter). Several neighboring countries may belong to the same location. The location is used to set a default **storage pool** for devices belonging to the customer.	`<std::String>` String Country code in ISO Alpha-2 format (recommended) or official country/area name in English. If the parameter is not submitted, the location of the parent customer is used.
`State`	The state in which the customer is located	`<std::String>` String
`District`	The district in which the customer is located	`<std::String>` String

Parameter	Description	Supported values
`City`	The city in which the customer is located	`<std::String>` String
`ZipCode`	The ZipCode in which the customer is located	`<std::String>` String
`Address`	The street address at which the customer is located	`<std::String>` String

AdvancedPartnerPropertiesInfo Child Parameters

Parameter	Description	Supported Values
`RegionId`	The ID number for the region the customer is in	`<int>` Integer
`ResponsibleUserId`	The ID for the responsible user	`<int>` Integer

Optional parameters

Parameter	Description	Supported values
`forceRemoveCustomColumnValuesInOldScope`	Do you wish to force remove custom column values for the device	`bool` Boolean ▪ `True` ▪ `False`

Sample request

It is possible to change as much about a customer or as little as you like. Provide the `partnerID` to select the customer whose information you need to change, then all other parameters entered will be changed to the information sent in the method.

The below example shows the change of name from "Zeus & Sons" to "Zeus And Sons" and limiting the available service types this Customer can provide to it's customers to `AllInclusive` only.

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "ModifyPartner",
    "jsonrpc": "2.0",
    "params": {
       "partnerInfo": {
               "Id": 12345,
               "Name": "Zeus And Sons",
               "ChildServiceTypes": ["AllInclusive"]
```

```
        }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": null,
    "visa": "{{visa}}"
}
```

Removing Customers in JSON-RPC API

To remove a customer, use the `RemovePartner` parameter.

> ✖ Once a customer is removed, this cannot be undone. There is no way to undo the deletion of a customer.

> ! You can remove only those customer that do not have any devices.

Required parameters

Parameter	Description	Supported values
`partnerId`	The ID of the Customer to remove	`<int>` Integer

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "RemovePartner",
    "jsonrpc": "2.0",
    "params": {
       "partnerId": 12345
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
```

```
    "jsonrpc": "2.0",
    "result": null,
    "visa": "{{visa}}"
}
```

Storage management methods in JSON-RPC API

> This is only available for **Software Only** customers. If you use our storage nodes, this section is not relevant.

To manage storage for Backup devices, see below for the list of **primary methods** that let you manage storage and storage nodes of a particular customer.

> Storage can be installed on several computers and once this device is used for storage, it may **not** be used for any other purpose.

- Getting storage information in JSON-RPC API (the `GetSorageInfo` method)
- Getting storage node information in JSON-RPC API (the `GetStorageNodeInfo` method)
- Getting a list of storage nodes in JSON-RPC API (the `EnumerateStorageNodes` method)
- Getting a list of storage nodes (by account ID) (the `EnumerateStorageNodesByAccountId` method)
- Getting a list of storage statistics in JSON-RPC API (the `EnumerateStorageStatistics` method)
- Getting a list of storages in JSON-RPC API (the `EnumerateStorages` method)

> You can identify other storage management methods in the schema by the word `Storage` in their names.

Getting storage information in JSON-RPC API

You can get the information on storage using the `GetStorageInfo` method.

Required parameters

Parameter	Description	Supported values
`storageId`	The ID of the storage pool you wish to get information for	`<int>` Integer

Sample request

```
{
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "id":"jsonrpc",
    "method" : "GetStorageInfo",
       "params" : {
           "storageId" : 100
```

```
        }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": {
           "Id": 100,
           "LocationId": 1,
           "Name": "Storage01",
           "NodeEmptierTrigger": "",
           "NodeFullTrigger": "",
           "PartnerId": 123456
       }
    },
    "visa": "{{visa}}"
}
```

Getting storage node information in JSON-RPC API

You can get the information on storage nodes using the `GetStorageNodeInfo` method.

Required parameters

Parameter	Description	Supported values
`storageNodeId`	The ID of the storage node to get information for	`<int>` Integer

Sample request

```
{
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "id":"jsonrpc",
    "method" : "GetStorageNodeInfo",
    "params" : {
           "storageNodeId": 100
    }
}
```

Sample response


```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": {
           "ActiveAccounts": 0,
           "CommonInfo": {
           "CertificateInfo": {
               "Certificate": "",
               "CertificatePin": "",
               "EndDate": 0,
               "StartDate": 0
       },
           "Family": "WEBDAVS",
           "GatewayHost": "100.0.0.0",
           "Host": "100.0.0.0:443",
           "HttpGatewayHost": "100.0.0.0:2999",
           "Name": "node_5",
           "Password": "*****",
           "Path": "",
           "StorageId": 200,
           "User": "*****"
       },
       "Id": 100,
       "LocationId": 13,
       "ModeInfo": {
           "Message": "",
           "Mode": "Operable"
       },
       "StateInfo": {
           "PrivilegedStorage": 0,
           "State": [
               "Online",
               "Full"
           ],
           "TotalStorage": 14544046,
           "UsedStorage": 14544046
       },
       "TotalAccounts": 0
       }
    },
    "visa": "{{visa}}"
}
```

Getting a list of storage nodes in JSON-RPC API

You can get a list of details on a storage node using the `EnumerateStorageNodes` method.

Required parameters

Parameter	Description	Supported values
`storageId`	The ID of the storage node	`<int>` Integer

Sample request

```
{
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "id":"jsonrpc",
    "method" : "EnumerateStorageNodes",
    "params" : {
           "storageId": 100
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": [
           {
               "ActiveAccounts": 0,
               "CommonInfo": {
                   "CertificateInfo": {
                       "Certificate": "",
                       "CertificatePin": "",
                       "EndDate": 0,
                       "StartDate": 0
                   },
                   "Family": "FTPS",
                   "GatewayHost": "",
                   "Host": "100.0.0.0,iaso",
                   "HttpGatewayHost": "",
                   "Name": "node_1",
                   "Password": "*****",
```

```
                    "Path": "",
                    "StorageId": 100,
                    "User": "*****"
                },
                "Id": 251,
                "LocationId": 1,
                "ModeInfo": {
                    "Message": "",
                    "Mode": "Operable"
                },
                "StateInfo": {
                    "PrivilegedStorage": 0,
                    "State": [
                        "Online",
                        "Migrated"
                    ],
                    "TotalStorage": 0,
                    "UsedStorage": 0
                },
                "TotalAccounts": 0
            }
        ]
    },
    "visa": "{{visa}}"
}
```


Getting a list of storage nodes (by account ID) in JSON-RPC API

You can get the information of storage nodes used by a device using the `EnumerateStorageNodesByAccountId` method.

Required parameters

Parameter	Description	Supported values
`accounts`	The ID of the account (device)	`<int>` Integer

Sample request

```
{
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "id":"jsonrpc",
    "method" : "EnumerateStorageNodesByAccountId",
```

```
    "params" : {
           "accounts": 135791
    }
}
```

Sample response


```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": [
           {
               "AccountId": 135791,
               "CurrentStorageNodeId": 0987654,
               "StorageNodes": [
                   {
                       "ActiveAccounts": 694,
                       "CommonInfo": {
                           "CertificateInfo": {
                               "ValidationMethod": "OsTrustStore"
                           },
                           "Family": "FAMILY",
                           "GatewayHost": "",
                           "Host": "hostname:port",
                           "HttpGatewayHost": "hostname:port",
                           "Name": "nl.ams.17.01",
                           "Password": "*****",
                           "Path": "",
                           "StorageId": 1001001,
                           "User": "*****"
                       },
                       "Id": 6789012,
                       "LocationId": 1,
                       "ModeInfo": {
                           "Mode": "Operable"
                       },
                       "StateInfo": {
                           "PrivilegedStorage": 0,
                           "State": [
                               "Online"
                           ],
                           "TotalStorage": 269080761,
                           "UpdateTimestamp": 1693215848,
```

```
                            "UsedStorage": 230868142
                        },
                        "TotalAccounts": 4436
                    },
                    {
                        "ActiveAccounts": 1201,
                        "CommonInfo": {
                            "CertificateInfo": {
                                "ValidationMethod": "OsTrustStore"
                            },
                            "Family": "FAMILY",
                            "GatewayHost": "",
                            "Host": "hostnane:port",
                            "HttpGatewayHost": "hostname:port",
                            "Name": "nl.ams.19.14",
                            "Password": "*****",
                            "Path": "",
                            "StorageId": 1001001,
                            "User": "*****"
                        },
                        "Id": 7890123,
                        "LocationId": 1,
                        "ModeInfo": {
                            "Mode": "Operable"
                        },
                        "StateInfo": {
                            "PrivilegedStorage": 0,
                            "State": [
                                "Online"
                            ],
                            "TotalStorage": 393082055,
                            "UpdateTimestamp": 1693219985,
                            "UsedStorage": 205150708
                        },
                        "TotalAccounts": 5963
                    }
                ]
            }
        ]
    },
    "visa": "{{visa}}"
}
```


Getting a list of storage statistics in JSON-RPC API

You can get a list of storage statistics using the `EnumerateStorageStatistics` method.

Required parameters

Parameter	Description	Supported values
`partnerId`	The ID of the customer to list the storages for (retrieved through the `GetPartnerInfo` method as the "Id" result)	`<int>` Integer

Sample request

```
{
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "id":"jsonrpc",
    "method" : "EnumerateStorageStatistics",
    "params" : {
           "partnerId": 123456
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": [
           {
               "LocationId": 1,
               "OnlineStorageNodeCount": 0,
               "TotalOnlineStorageInMb": 0,
               "TotalStorageInMb": 0,
               "TotalStorageNodeCount": 0,
               "UsedOnlineStorageInMb": 0,
               "UsedStorageInMb": 0
           }
       ]
    },
    "visa": "{{visa}}"
}
```

Getting a list of storages in JSON-RPC API

You can get a list of storages using the `EnumerateStorages` method.

Required parameters

Parameter	Description	Supported values
`partnerId`	The ID of the customer to list the storages for (retrieved through the `GetPartnerInfo` method)	`<int>` Integer

Sample request

```
{
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "id":"jsonrpc",
    "method" : "EnumerateStorages",
    "params" : {
           "partnerId": 123456
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": [
           {
               "Id": 100,
               "LocationId": 1,
               "Name": "Storage01",
               "NodeEmptierTrigger": "",
               "NodeFullTrigger": "",
               "PartnerId": 123456
           }
       ]
    },
    "visa": "{{visa}}"
}
```

User management methods in JSON-RPC API

A **user** is a login for a person on the console to allow that person to navigate the Management Console dashboard or to use JSON-RPC API's themselves.

Below is the list of **primary methods** that let you manage users.

- Adding a new user (the `AddUser` method)
- Getting a list of users for a company (the `EnumerateUsers` method)
- Getting user information (the `GetUserInfo` method)
- Getting user information (by User ID) (the `GetUserInfoById` method)
- Getting a list of user roles (the `EnumerateUserRoles` method)
- Changing the properties of a user (the `ModifyUser` method)
- Removing a user (the `RemoveUser` method)

> You can identify other user management methods in the schema by the word `User` in their names.

Adding users in JSON-RPC API

To add users, use the `AddUser` method. Users are added one at a time.

Required parameters

Parameter	Description	Supported values
`userInfo`	A group of parameters related to the user	`UserInfo` (has child parameters of its own see the UserInfo child parameters table below)

UserInfo child parameters

Parameter	Description	Supported values
`ID`	The ID number of the user	`<int>` Integer
`PartnerId`	The ID of the customer the user is created for (retrieved through the `GetPartnerInfo` method)	`<int>` Integer
`Name` (required)	A login name for the user (must be the same as the `EmailAddress`)	`OptionalNonEmptyString`
`Password`	Set a password for the new user	`OptionalNonEmptyString`
`RoleId`	The ID of the role the user will be given (retrieved through the `enumerateUserRoles` method)	`<int>` Integer Choose Int that correlates to the role below: - `1` - SuperUser - `2` - Administrator - `3` - Manager

Parameter	Description	Supported values
		▪ 4 - Operator ▪ 5 - Supporter ▪ 6 - Reporter ▪ 7 - Notifier
ContactPersonId	The ID of the contact person that this new user will be associated with	<int> Integer
TwoFactorAuthenticationStatus	An array of 2FA state's to give to the new user	TwoFactorAuthenticationState::Enum ▪ Undefined ▪ Disabled ▪ Enabled ▪ Count
EmailAddress	The email address of the user (must be the same as the Name given)	<std::String>
Flags	Flag the user with certain feature access	UserFlag::FlagsType ▪ Undefined ▪ TeamViewer ▪ AuthorizedSigner ▪ Administrative ▪ Technical ▪ Sales ▪ Billing ▪ Count
FirstLoginTime	The time-stamp of the first time the user has logged in successfully	<std::time_t> Integer in Unix format. For example, 1535673599 stands for August 30, 2018
LastLoginTime	The time-stamp of the last time the user has logged in successfully	<std::time_t> Integer in Unix format. For example, 1535673599 stands for August 30, 2018
FirstName	The first name of the user	<std::String>
FullName	The surname of the user	<std::String>
Title	A title given to the user of	<std::String>

Parameter	Description	Supported values
	the user	
PhoneNumber	The phone number of the user	<std::String>

Sample request

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "visa": "{{visa}}",
    "method": "AddUser",
    "params": {
           "userInfo": {
               "Name" : "backup.test@mail.com",
               "PartnerId" : 123456,
               "Password" : "AbC123DeF!",
               "RoleId" : 1,
               "EmailAddress" : "backup.test@mail.com",
               "FirstName" : "Backup",
               "FullName" : "Test",
               "Title": "Manager"
           }
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": 876543
    },
    "visa": "{{visa}}"
}
```

Enumerating users in JSON-RPC API

You can get the list of users of your own company and your customers using the `EnumerateUsers` method.

Required parameters

Parameter	Description	Supported values
`partnerIds`	The ID of the customer the users are created for (retrieved through the `GetPartnerInfo` method)	`<int>` Integer in array format e.g. `[partnerIds1,partnerIds2]`

Sample request

```
{
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "id":"jsonrpc",
    "method" : "EnumerateUsers",
    "params" : {
           "partnerIds" : [123456]
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": [
           {
               "EmailAddress": "user1@demodomain.com",
               "FirstLoginTime": 1530020135,
               "FirstName": "User1",
               "Flags": [
                   "SecurityOfficer",
                   "AllowApiAuthentication"
               ],
               "FullName": "Demo",
               "Id": 765432,
               "LastLoginTime": 1573030172,
               "Name": "user1@demodomain.com",
               "PartnerId": 123456,
               "Password": null,
               "PhoneNumber": "",
               "RoleId": 1,
               "Title": "End-User",
               "TwoFactorAuthenticationStatus": "Disabled"
```

```
            },
            {
                "EmailAddress": "user2@demodomain.com",
                "FirstLoginTime": 1541777548,
                "FirstName": "User2",
                "Flags": [
                    "AllowApiAuthentication"
                ],
                "FullName": "Demo",
                "Id": 654321,
                "LastLoginTime": 1541777548,
                "Name": "user2@demodomain.com",
                "PartnerId": 123456,
                "Password": null,
                "PhoneNumber": "",
                "RoleId": 1,
                "Title": "End-User"
            }
        ]
    },
    "visa": "{{visa}}"
}
```


Getting user information in JSON-RPC API

To get information about a user using their name, use the `GetUserInfo` method.

Required parameters

Parameter	Description	Supported values
`partnerId` (required)	The ID of the customer the user is created for (retrieved through the `GetPartnerInfo` method)	`<int>` Integer
`nameOrEmail` (required)	The name or email address of the user to show details for	`<std::String>`
`password`	The password for the user to show details for	`<std::String>`

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
```

```
    "method": "GetUserInfo",
    "jsonrpc": "2.0",
    "params": {
       "partnerId": 123456,
       "nameOrEmail": "user@domain.com"
       }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": {
               "EmailAddress": "user@domain.com",
               "FirstLoginTime": 1544458672,
               "FirstName": "User",
               "Flags": [
                       "SecurityOfficer"
               ],
               "FullName": "Test",
               "Id": 987654,
               "LastLoginTime": 1555593295,
               "Name": "user@domain.com",
               "PartnerId": 123456,
               "Password": null,
               "PhoneNumber": "",
               "RoleId": 1,
               "Title": "Reseller"
       }
    },
    "visa": "{{visa}}"
}
```

Getting user information by user ID in JSON-RPC API

To get information about a user using the user ID, use the `GetUserInfoById` method.

Required parameters

Parameter	Description	Supported values
`userId`	The User ID of the user (retrieved through the `GetUserInfo` method)	`<int>` Integer

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "GetUserInfoById",
    "jsonrpc": "2.0",
    "params": {
       "userId": 123456
       }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": {
               "EmailAddress": "user@domain.com",
               "FirstLoginTime": 1544458672,
               "FirstName": "User",
               "Flags": [
                       "SecurityOfficer"
               ],
               "FullName": "Test",
               "Id": 123456,
               "LastLoginTime": 1555593295,
               "Name": "user@domain.com",
               "PartnerId": 246802,
               "Password": null,
               "PhoneNumber": "",
               "RoleId": 1,
               "Title": "Reseller",
               "TwoFactorAuthenticationStatus": "Enabled"
       }
    },
    "visa": "{{visa}}"
}
```

Changing user properties in JSON-RPC API

To modify a backup user, use the `ModifyUser` method. You can change the following properties:

- Re-assign the user to another customer
- Change the users name, title, email address or phone number

> ! Usernames and passwords cannot be changed.

Required parameters

Parameter	Description	Supported values
`userInfo`	A group of parameters related to the user	`UserInfo` (has child parameters of its own see the UserInfo child parameters table below)

UserInfo child parameters

Parameter	Description	Supported values
`ID`	The ID number of the user	`<int>` Integer
`PartnerId`	The ID of the customer the user is created for (retrieved through the `GetPartnerInfo` method)	`<int>` Integer
`Name` (required)	A login name for the user (must be the same as the `EmailAddress`)	`OptionalNonEmptyString`
`Password`	Set a password for the new user	`OptionalNonEmptyString`
`RoleId`	The ID of the role the user will be given (retrieved through the `enumerateUserRoles` method)	`<int>` Integer Choose Int that correlates to the role below: - `1` - SuperUser - `2` - Administrator - `3` - Manager - `4` - Operator - `5` - Supporter - `6` - Reporter - `7` - Notifier
`ContactPersonId`	The ID of the contact person that this new user will be associated with	`<int>` Integer
`TwoFactorAuthenticationStatus`	An array of 2FA state's to give to the new user	`TwoFactorAuthenticationState::Enum`

Parameter	Description	Supported values
		▪ Undefined ▪ Disabled ▪ Enabled ▪ Count
EmailAddress	The email address of the user (must be the same as the Name given)	<std::String>
Flags	Flag the user with certain feature access	UserFlag::FlagsType ▪ Undefined ▪ TeamViewer ▪ AuthorizedSigner ▪ Administrative ▪ Technical ▪ Sales ▪ Billing ▪ Count
FirstLoginTime	The time-stamp of the first time the user has logged in successfully	<std::time_t> Integer in Unix format. For example, 1535673599 stands for August 30, 2018
LastLoginTime	The time-stamp of the last time the user has logged in successfully	<std::time_t> Integer in Unix format. For example, 1535673599 stands for August 30, 2018
FirstName	The first name of the user	<std::String>
FullName	The surname of the user	<std::String>
Title	A title given to the user of the user	<std::String>
PhoneNumber	The phone number of the user	<std::String>

Sample request

```
{
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "id":"jsonrpc",
```

```
    "method" : "ModifyUser",
    "params" : {
       "userInfo" : {
           "Id" : 987654,
           "RoleId" : 1,
           "Flags": ["Technical","Sales"]
       }
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": null,
    "visa": "{{visa}}"
}
```

Removing users in JSON-RPC API

To remove a user, use the `RemoveUser` method.

> ✖ Once a User is removed, this cannot be undone. There is no way to undo the deletion of a user.

Required parameters

Parameter	Description	Supported values
`userId`	The ID of the user to remove	`<int>` Integer

Sample request

```
{
    "id": "jsonrpc",
    "visa": "{{visa}}",
    "method": "RemoveUser",
    "jsonrpc": "2.0",
    "params": {
       "userId": 12345
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": null,
    "visa": "{{visa}}"
}
```

Miscellaneous methods in JSON-RPC API

There are several miscellaneous JSON-RPC API's that are useful for gathering information relating to the Management Console's Dashboard views, columns, audit actions, device profiles, locations and regions.

Below is the list of **methods** for these:

- Getting Dashboard view settings (the `GetUserSettings` method)
- Getting a list of User Dashboard View settings (the `EnumerateUserSettings` method)
- Getting a list of regions (the `EnumerateRegions` method)
- Getting a list of storage locations (the `EnumerateLocations` method)
- Getting a list of profiles (the `EnumerateAccountProfiles` method)

Get Dashboard View settings in JSON-RPC API

You can get information on a Backup Dashboard view, including a list of columns displayed in this view, using the `GetUserSettings` method.

Required parameters

Parameter	Description	Supported values
`settingsId`	The ID of the view to view the settings for	`<int>`

Sample request

```
{
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "id":"jsonrpc",
    "method" : "GetUserSettings",
    "params" : {
       "settingsId" : 0
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": {
           "Current": true,
           "Id": 0,
           "Name": "Default View",
           "Type": "Predefined",
           "View": {
               "Columns": [
                   "AN",
                   "AR",
                   "MN",
                   "TL",
                   "T0",
                   "US",
                   "TB",
                   "VN",
                   "T7",
                   "T3"
               ],
               "Mode": "Standard",
               "RecordCount": 40
           }
       }
    },{{visa}}"
}
```

Enumerating User Dashboard View settings in JSON-RPC API

You can get the list of BackupDashboard views for a user and the view's settings, including a list of columns displayed in these views, using the the `EnumerateUserSettings` method.

Required parameters

Parameter	Description	Supported values
`userId`	The ID of the user whose Dashboard views you want to see	`<int>`
`settingsType`	An array of the types of views	`UserViewType::Enum` ▪ `Undefined` ▪ `Predefined`

Parameter	Description	Supported values
		▪ Custom ▪ Count

Sample request

```
{
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "id":"jsonrpc",
    "method" : "EnumerateUserSettings",
    "params" : {
           "userId" : 123456,
           "settingsType" : "Custom"
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": [
           {
               "Current": true,
               "Id": 7806,
               "Name": "Basic View",
               "Type": "Custom",
               "UserId": 123456,
               "View": {
                   "Columns": [
                       "AN",
                       "AR",
                       "I78",
                       "US",
                       "TB",
                       "T0",
                       "OS"
                   ],
                   "Mode": "Standard",
                   "NormalStatisticsFilter": "",
```

```
                    "PartnerId": 135791,
                    "RecordCount": 40,
                    "SortColumns": [
                        {
                            "Name": "TL",
                            "SortOrder": "Descending"
                        }
                    ],
                    "StatisticsFilter": ""
                }
            }
        ]
    },
    "visa": "{{visa}}"
}
```

Enumerating Regions in JSON-RPC API

You can get the list of geographic regions, using the `EnumerateRegions` method.

Required parameters

This method has no required or optional parameters and does not require a visa.

Sample request

```
{
    "jsonrpc":"2.0",
    "id":"jsonrpc",
    "method" : "EnumerateRegions",
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": [
            {
                "Id": 1,
                "Name": "USA"
            },
            {
```

```
                "Id": 2,
                "Name": "Canada"
            },
            {
                "Id": 3,
                "Name": "UK"
            },
            {
                "Id": 4,
                "Name": "Germany"
            },
            {
                "Id": 5,
                "Name": "France"
            },
            {
                "Id": 6,
                "Name": "Netherlands"
            },
            {
                "Id": 7,
                "Name": "Belgium"
            },
            {
                "Id": 8,
                "Name": "Other"
            },
            {
                "Id": 9,
                "Name": "Australia"
            }
        ]
    },
    "visa": "{{visa}}"
}
```


Enumerating Storage Locations in JSON-RPC API

You can get the list of storage Locations, using the `EnumerateLocations` method.

Required parameters

This method has no required or optional parameters and does not require a visa.

Sample request

```
{
    "jsonrpc":"2.0",
    "id":"jsonrpc",
    "method" : "EnumerateLocations",
}
```

Sample response


```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": [
           {
                   "Flags": [
                       "StrictLocationPolicy"
                   ],
                   "Id": 1,
                   "Name": "Netherlands"
           },
           {
                   "Flags": [
                       "StrictLocationPolicy"
                   ],
                   "Id": 2,
                   "Name": "Australia"
           },
           {
                   "Flags": [
                       "StrictLocationPolicy"
                   ],
                   "Id": 3,
                   "Name": "Belgium"
           },
           {
                   "Id": 4,
                   "Name": "Belarus"
           },
           {
                   "Flags": [
                       "StrictLocationPolicy"
                   ],
```

```
                "Id": 5,
                "Name": "Canada"
        },
        {
                "Flags": [
                    "StrictLocationPolicy"
                ],
                "Id": 6,
                "Name": "Germany"
        },
        {
                "Flags": [
                    "StrictLocationPolicy"
                ],
                "Id": 7,
                "Name": "Denmark"
        },
        {
                "Flags": [
                    "StrictLocationPolicy"
                ],
                "Id": 8,
                "Name": "Spain"
        },
        {
                "Id": 9,
                "Name": "Finland"
        },
        {
                "Flags": [
                    "StrictLocationPolicy"
                ],
                "Id": 10,
                "Name": "France"
        },
        {
                "Flags": [
                    "StrictLocationPolicy"
                ],
                "Id": 11,
                "Name": "United Kingdom"
        },
        {
                "Id": 12,
```

```
                "Name": "Hungary"
        },
        {
                "Id": 13,
                "Name": "Israel"
        },
        {
                "Id": 14,
                "Name": "Kenya"
        },
        {
                "Id": 15,
                "Name": "Luxembourg"
        },
        {
                "Id": 16,
                "Name": "Poland"
        },
            {
                "Id": 17,
                "Name": "Thailand"
        },
        {
                "Flags": [
                    "StrictLocationPolicy"
                ],
                "Id": 18,
                "Name": "United States"
        },
        {
                "Id": 19,
                "Name": "Croatia"
        },
        {
                "Flags": [
                    "StrictLocationPolicy"
                ],
                "Id": 20,
                "Name": "Italy"
        },
        {
                "Flags": [
                    "StrictLocationPolicy"
                ],
```

```
                "Id": 21,
                "Name": "Switzerland"
        },
        {
                "Flags": [
                    "StrictLocationPolicy"
                ],
                "Id": 22,
                "Name": "South Africa"
        },
        {
                "Flags": [
                    "StrictLocationPolicy"
                ],
                "Id": 23,
                "Name": "Norway"
        },
        {
                "Flags": [
                    "StrictLocationPolicy"
                ],
                "Id": 24,
                "Name": "Sweden"
        },
        {
                "Flags": [
                    "StrictLocationPolicy"
                ],
                "Id": 25,
                "Name": "Portugal"
        },
        {
                "Flags": [
                    "StrictLocationPolicy"
                ],
                "Id": 28,
                "Name": "Brazil"
        },
        {
                "Id": 34,
                "Name": "Ireland"
        }
    ]
},
```

```
    "visa": "{{visa}}"
}
```

Enumerating Device's Profiles in JSON-RPC API

You can get the list of profiles available to your devices of your own company and your customers using the `EnumerateAccountProfiles` method.

Required parameters

Parameter	Description	Supported values
`partnerId`	The ID of the customer whose devices you wish to list (retrieved through the `GetPartnerInfo` method)	`<int>` Integer

Sample request

```
{
    "id":"jsonrpc",
    "jsonrpc":"2.0",
    "visa": "{{visa}}",
    "method" : "EnumerateAccountProfiles",
    "params" : {
           "partnerId" : 123456
    }
}
```

Sample response

```
{
    "id": "jsonrpc",
    "jsonrpc": "2.0",
    "result": {
       "result": [
           {
               "Id": 098765,
               "Name": "demo-prof",
               "PartnerId": 123456,
               "ProfileData": {
                   "BackupDataSourceSettings": [
                       {
                           "DataSource": "WorkstationFileSystem",
```

```
                "ExclusionFilter": null,
                "Policy": "Force",
                "SelectionCollection": [
                    {
                        "Selection": "/"
                    }
                ],
                "SelectionModification": "ForbidAnyModification"
            },
            {
                "DataSource": "ServerFileSystem",
                "ExclusionFilter": null,
                "Policy": "Force",
                "SelectionCollection": [
                    {
                        "Selection": "/"
                    }
                ],
                "SelectionModification": "ForbidAnyModification"
            },
            {
                "DataSource": "SystemState",
                "ExclusionFilter": null,
                "Policy": "Force",
                "SelectionCollection": [
                    {
                        "Selection": "/"
                    }
                ]
            },
            {
                "DataSource": "NetworkShares",
                "ExclusionFilter": null,
                "Policy": "AllowedManualConfiguration",
                "SelectionCollection": [
                    {
                        "Selection": "/"
                    }
                ]
            },
            {
                "DataSource": "MsSql",
                "ExclusionFilter": null,
                "Policy": "ForceIfExists",
```

```
                "SelectionCollection": [
                    {
                        "Selection": "/"
                    }
                ]
            },
            {
                "DataSource": "Exchange",
                "ExclusionFilter": null,
                "Policy": "ForceIfExists",
                "SelectionCollection": [
                    {
                        "Selection": "/"
                    }
                ]
            },
            {
                "DataSource": "VMWare",
                "ExclusionFilter": null,
                "Policy": "AllowedManualConfiguration",
                "SelectionCollection": [
                    {
                        "Selection": "/"
                    }
                ]
            },
            {
                "DataSource": "SharePoint",
                "ExclusionFilter": null,
                "Policy": "ForceIfExists",
                "SelectionCollection": [
                    {
                        "Selection": "/"
                    }
                ]
            },
            {
                "DataSource": "Oracle",
                "ExclusionFilter": null,
                "Policy": "AllowedManualConfiguration",
                "SelectionCollection": [
                    {
                        "Selection": "/"
                    }
```

```
                ]
            },
            {
                "DataSource": "HyperV",
                "ExclusionFilter": null,
                "Policy": "AllowedManualConfiguration",
                "SelectionCollection": [
                    {
                        "Selection": "/"
                    }
                ]
            },
            {
                "DataSource": "MySql",
                "ExclusionFilter": null,
                "Policy": "AllowedManualConfiguration",
                "SelectionCollection": [
                    {
                        "Selection": "/"
                    }
                ]
            }
        ],
        "BackupSchedule": [
            {
                "DataSourceCollection": [
                    "WorkstationFileSystem",
                    "ServerFileSystem",
                    "SystemState",
                    "NetworkShares",
                    "MsSql",
                    "Exchange",
                    "VMWare",
                    "SharePoint",
                    "Oracle",
                    "HyperV",
                    "MySql"
                ],
                "DayOfWeekCollection": [
                    "Sunday",
                    "Monday",
                    "Tuesday",
                    "Wednesday",
                    "Thursday",
```

```
                    "Friday",
                    "Saturday"
                ],
                "FireTimeInterval": {
                    "LowerBound": {
                        "Hour": 0,
                        "Minute": 0
                    },
                    "UpperBound": {
                        "Hour": 0,
                        "Minute": 0
                    }
                },
                "Name": "GeneratedSchedule"
            }
        ],
        "HighFrequentBackupSchedule": {
            "BackupScheduleItems": [
                {
                    "DoNotStartDuringWorkingHours": false,
                    "Frequency": "Every24Hours",
                    "PluginId": "WorkstationFileSystem",
                    "TimeOfFirstBackup": 0
                },
                {
                    "DoNotStartDuringWorkingHours": false,
                    "Frequency": "Every24Hours",
                    "PluginId": "ServerFileSystem",
                    "TimeOfFirstBackup": 0
                },
                {
                    "DoNotStartDuringWorkingHours": false,
                    "Frequency": "Every24Hours",
                    "PluginId": "SystemState",
                    "TimeOfFirstBackup": 0
                },
                {
                    "DoNotStartDuringWorkingHours": false,
                    "Frequency": "Every24Hours",
                    "PluginId": "NetworkShares",
                    "TimeOfFirstBackup": 0
                },
                {
                    "DoNotStartDuringWorkingHours": false,
```

```
                "Frequency": "Every24Hours",
                "PluginId": "MsSql",
                "TimeOfFirstBackup": 0
            },
            {
                "DoNotStartDuringWorkingHours": false,
                "Frequency": "Every24Hours",
                "PluginId": "Exchange",
                "TimeOfFirstBackup": 0
            },
            {
                "DoNotStartDuringWorkingHours": false,
                "Frequency": "Every24Hours",
                "PluginId": "VMWare",
                "TimeOfFirstBackup": 0
            },
            {
                "DoNotStartDuringWorkingHours": false,
                "Frequency": "Every24Hours",
                "PluginId": "SharePoint",
                "TimeOfFirstBackup": 0
            },
            {
                "DoNotStartDuringWorkingHours": false,
                "Frequency": "Every24Hours",
                "PluginId": "Oracle",
                "TimeOfFirstBackup": 0
            },
            {
                "DoNotStartDuringWorkingHours": false,
                "Frequency": "Every24Hours",
                "PluginId": "HyperV",
                "TimeOfFirstBackup": 0
            },
            {
                "DoNotStartDuringWorkingHours": false,
                "Frequency": "Every24Hours",
                "PluginId": "MySql",
                "TimeOfFirstBackup": 0
            }
        ],
        "WorkingHours": {
            "Days": [
                "Monday",
```

```
                                "Tuesday",
                                "Wednesday",
                                "Thursday",
                                "Friday"
                            ],
                            "EndTime": 64800,
                            "StartTime": 28800
                        }
                    },
                    "Language": "en",
                    "TemporaryFolderPath": null
                },
                "Version": 1
            }
        ]
    },
    "visa": {{visa}}
}
```

Management Console column codes for API

When using certain JSON-RPC API methods, you may be given or asked for column vectors or column codes and data source codes.

> Please note, the old legacy shortnames will still work for the time being, but we would strongly recommend you change the API methods to use the below notations as soon as possible.

Example

If you want to output the information from the creation date, computer name, used storage and active data sources columns for a list of devices. Use the Enumerating Account Statistics method.

Using the "Columns" parameter in the **old notation**, this would be written as:

```
"Columns": ["CD", "MN", "US", "AP"],
```

Using the **new notation**, you are replacing `"CD"`, `"MN"`, `"US"` and `"AP"` with `"I4"`, `"I18"`, `"I14"` and `"I78"`. This would mean the parameter in your JSON call now looks as below:

```
"Columns": ["I4", "I18", "I14", "I78"],
```

> There is no limit to the number of column vectors that can be requested using this Column parameter.

The response showing this information will be displayed as:

```
"Settings": [
    {
       "I4": "1536906195"
    },
    {
       "I18": "ComputerName1"
    },
    {
       "I14": "188702358870"
    },
    {
       "I78": "D1,D2"
    }
]
```

Example Breakdown

In the above example, the Columns parameter is calling the following Settings to be displayed:

- **`I4`**: Creation Date
  - The response for this has come back as "1536906195", which is the date and time in Unix format. Converted, this is Sept 14th, 2018, 07:23:15 relative to my timezone
- **`I18`**: Computer Name
  - This is the unique computer name for the device in question
- **`I14`**: Used Storage
  - The response for this has come back as "188702358870", which is the total size of storage used for the device in Bytes. Converted, this is 188.7 GB.
- **`I78`**: Active Data Sources
  - The data sources active on the device as denoted by their respective ID numbers. The response here is D1 and D2, which mean that the Files and Folders and System State Data Sources are active on the device.

Expressions for active data sources

See the list of Backup data sources here, with the legacy shortnames detailed for ease:

Full Name	New ID	Legacy Shortname
Files and Folders	D1	F
System State	D2	S
MsSql	D3	Q
VssExchange	D4	X
Microsoft 365 SharePoint	D5	--

Full Name	New ID	Legacy Shortname
NetworkShares	D6	N
VssSystemState	D7	S
VMware Virtual Machines	D8	W
Total	D9	T
VssMsSql	D10	Z
VssSharePoint	D11	P
Oracle	D12	Y
Hyper-V	D14	H
MySql	D15	L
Virtual Disaster Recovery	D16	V
Bare Metal Restore	D17	B
Microsoft 365 Exchange	D19	G
Microsoft 365 OneDrive	D20	J
Microsoft 365 Teams	D23	--
Removable Media	--	R

Column Codes

See the list of Backup column codes below:

Primary device properties

Column Title	New ID	Legacy Shortname	Type of data
Device ID	I0	AU	String
Device name	I1	AN	String
Device name alias	I2	AL	String
Password	I3	QW	String
Creation date	I4	CD	Time
Expiration date	I5	ED	Time
Customer	I8	AR	String

Column Title	New ID	Legacy Shortname	Type of data
Product ID	I9	PD	Int
Product	I10	PN	String
Email	I15	EM	String
Retention units	I39	RU	String
Profile ID	I54	OI	Int

Installation details

Column Title	New ID	Legacy Shortname	Type of data
OS version ?[1]	I16	OS	String
Client version	I17	VN	String
Computer name	I18	MN	String
Internal IPs	I19	IP	String
MAC address	I21	MA	String
Time offset	I24	TZ	Number
OS type ?[2]	I32	OT	▪ `1` - workstation ▪ `2` - server ▪ `0` - undefined
Computer manufacturer	I44	MF	String
Computer model	I45	MO	String
Installation ID	I46	II	String
Installation Mode	I47	IM	Int
Unattended Installation account ID	I74	AI	String
First Installation Flag	I75	IF	Int

[1]Name and version of Operating System
[2]Operating System type

Storage info

Column Title	New ID	Legacy Shortname	Type of data
Storage location ?[1]	I11	LN	String
Used storage	I14	US	Size
Cabinet Storage Efficiency	I26	SE	Int
Total Cabinets Count	I27	CC	Int
Efficient Cabinet Count 0-25	I28	E0	Int
Efficient Cabinet Count 26-50	I29	E1	Int
Efficient Cabinet Count 50-75	I30	E2	Int
Used Virtual Storage	I31	UV	Size
Storage status	I36	YS	▪ `-2` - Offline ▪ `-1` - Failed ▪ `0` - Undefined ▪ `50` - Running ▪ `100` - Synchronized

Feature usage

Column Title	New ID	Legacy Shortname	Type of data
Active data sources	I78	AP	String
Seeding mode	I33	IS	▪ `0` - Undefined ▪ `1` - Normal ▪ `2` - Seeding ▪ `3` - PreSeeding ▪ `4` - PostSeeding
LSV ?[2]	I35	VE	▪ `0` - Disabled ▪ `1` - Enabled
LSV status	I37	YV	▪ `-2` - Offline ▪ `-1` - Failed

---

[1] Location of the home node
[2] LocalSpeedVault enabled

Column Title	New ID	Legacy Shortname	Type of data
			▪ 0 - Undefined ▪ 50 - Running ▪ 100 - Synchronized

Data source statistics fields

Column title	NeW ID	Legacy Shortname	Type of data
Last Session Status	F00	0	▪ 1 - In process ▪ 2 - Failed ▪ 3 - Aborted ▪ 5 - Completed ▪ 6 - Interrupted ▪ 7 - NotStarted ▪ 8 - CompletedWithErrors ▪ 9 - InProgressWithFaults ▪ 10 - OverQuota ▪ 11 - NoSelection ▪ 12 - Restarted
Last Session Selected Count	F01	1	Int
Last Session Processed Count	F02	2	Int
Last Session Selected Size	F03	3	Size
Last Session Processed Size	F04	4	Size
Last Session Sent Size	F05	5	Size
Last Session Errors Count	F06	7	Int
Protected size	F07	6	Size
Color bar - last 28 days	F08	B	ColourBar
Last successful session Timestamp	F09	L	Time
Pre Recent Session Selected Count	F10	8	Int
Pre Recent Session Selected Size	F11	9	Size

Column title	NeW ID	Legacy Shortname	Type of data
Session duration	F12	A	Int
Last Session License Items count ?[1]	F13	I	Int
Retention	F14	R	Int
Last Session Timestamp	F15	G	Time
Last Successful Session Status	F16	Q	Status
Last Completed Session Status	F17	J	Status
Last Completed Session Timestamp	F18	O	Time
Last Session Verification Data	F19	K	String
Last Session User Mailboxes Count	F20	M	Int
Last Session Shared Mailboxes Count ?[2]	F21	@	Int

Company Information

Column Title	New ID	Legacy Shortname	Type of data
Company Name	I63	NC	String
Address	I64	AD	String
Zip Code	I65	ZP	String
Country	I66	CY	String
City	I67	CT	String
Phone Number	I68	PH	String

---

[1]Only available for the following data sources:

- Total
- Microsoft 365 Exchange
- Microsoft 365 OneDrive

[2]Only available for the following data sources:

- Total
- Microsoft 365 Exchange
- Microsoft 365 OneDrive

Column Title	New ID	Legacy Shortname	Type of data
Fax Number	I69	FX	String
Contract Name	I70	CP	String
Group Name	I71	GN	String
Demo	I72	DE	Int
Edu	I73	EU	Int
Maximum Allowed Version	I76	MV	String

Miscellaneous

Column Title	New ID	Legacy Shortname	Type of data
Timestamp	I6	TS	Unix time
Device group name	I12	AG	String
Own user name	I13	OU	String
External IPs	I20	EI	String
Dashboard frequency	I22	DF	Bitmask
Dashboard language	I23	DL	String
Anti Crypto enabled	I34	AC	Int
Archived size	I38	AS	String
Activity description	I40	DS	String
Number of Hyper-V virtual machines	I41	HN	String
Number of ESX virtual machines	I42	EN	String
Encryption status	I43	ES	String
Restore email	I48	REM	String
Restore dashboard frequency	I49	RDF	Bitmask
Restore dashboards language	I50	RDL	String
Profile version	I55	OV	String
Profile	I56	OP	String
Stock Keeping Unit	I57	KU	String

Column Title	New ID	Legacy Shortname	Type of data
Stock Keeping Unit of the previous month	I58	PU	String
Account type	I59	AT	String
Proxy Type	I60	PT	Int
Most Recent Restore Plugin	I62	RP	String
Customer reference	I77	PF	String
Recovery Testing	I80	--	▪ Disabled ▪ Enabled
Physicality	I81	--	▪ Undefined ▪ Physical ▪ Virtual
Passphrase	I82	--	▪ Yes ▪ No

Management Console column codes for API (Legacy)

When using certain JSON-RPC API methods, you may be given or asked for column vectors or column codes.

See the list of Backup column codes below.

Primary device properties

Short name	Column title	Type of data
AN	Device name	String
QW	Password	String
AU	Device ID	String
AL	Device name alias	String
AR	Customer	String
CD	Creation date	Time
ED	Expiration date	Time
PN	Product	String
RU	Retention units	String
EM	Email	String

Installation details

Short name	Column title	Type of data
VN	Client version	String
MN	Computer name	String
MF	Computer manufacturer	String
MO	Computer model	String
OS	OS version ?[1]	String
OT	OS type ?[2]	▪ `1` - workstation ▪ `2` - server ▪ `0` - undefined
MA	MAC address	String
IP	Internal IPs	String
TZ	Time offset	Number

Storage info

Short name	Column title	Type of data
LN	Storage location ?[3]	String
US	Used storage	Size
YS	Storage status	▪ `-2` - Offline ▪ `-1` - Failed ▪ `0` - Undefined ▪ `50` - Running ▪ `100` - Synchronized

---

[1]Name and version of Operating System
[2]Operating System type
[3]Location of the home node

Feature usage

Short name	Column title	Type of data
AP	Active data sources	String
VE	LSV ?[1]	▪ `0` - Disabled ▪ `1` - Enabled
YV	LSV status	▪ `-2` - Offline ▪ `-1` - Failed ▪ `0` - Undefined ▪ `50` - Running ▪ `100` - Synchronized
IS	Seeding mode	▪ `0` - Undefined ▪ `1` - Normal ▪ `2` - Seeding ▪ `3` - PreSeeding ▪ `4` - PostSeeding

Miscellaneous

Short name	Column title	Type of data
AG	Device group name	String
AS	Archived size	String
AT	Account type	String
DF	Dashboard frequency	Bitmask
DL	Dashboard language	String
DS	Activity description	String
EI	External IPs	String
EN	Number of ESX virtual machines	String
ES	Encryption status	String
HN	Number of Hyper-V virtual machines	String

---

[1] LocalSpeedVault enabled

Short name	Column title	Type of data
KU	SKU	String
OP	Profile	String
OU	Own user name	String
OV	Profile version	String
PF	Customer reference	String
PU	SKU of the previous month	String
REM	Restore email	String
RDF	Restore dashboard frequency	Bitmask
RDL	Restore dashboards language	String
TS	Timestamp	Unix time

Backup statistics by the data source (continued)

Column title	System State	Files and Folders	Network Shares	VSS MSSQL	Exchange Stores	SharePoint data	Oracle	VMware virtual machines	Hyper-V data	MySQL status
Status	S0	F0	N0	Z0	X0	P0	Y0	W0	H0	L0
Number of files in selection	S1	F1	N1	Z1	X1	P1	Y1	W1	H1	L1
Number of changed files	S2	F2	N2	Z2	X2	P2	Y2	W2	H2	L2
Selected size	S3	F3	N3	Z3	X3	P3	Y3	W3	H3	L3
Processed size	S4	F4	N4	Z4	X4	P4	Y4	W4	H4	L4
Sent size	S5	F5	N5	Z5	X5	P5	Y5	W5	H5	L5
Pro-	S6	F6	N6	Z6	X6	P6	Y6	W6	H6	L6

Column title	System State	Files and Folders	Network Shares	VSS MSSQL	Exchange Stores	SharePoint data	Oracle	VMware virtual machines	Hyper-V data	MySQL status
tected size										
Number of errors	S7	F7	N7	Z7	X7	P7	Y7	W7	H7	L7
Session duration	SA	FA	NA	ZA	XA	PA	YA	WA	HA	LA
Last successful session	SL	FL	NL	ZL	XL	PL	YL	WL	HL	LL
Status of the last successful session	SQ	FQ	NQ	ZQ	XQ	PQ	YQ	WQ	HQ	LQ
Status of the last completed session	SJ	FJ	NJ	ZJ	XJ	PJ	YJ	WJ	HJ	LJ
Timestamp of the last completed session	SO	FO	NO	ZO	XO	PO	YO	WO	HO	LO
Retention	SR	FR	NR	ZR	XR	PR	YR	WR	HR	LR
Color bar - last 28 days	SB	FB	NB	ZB	XB	PB	YB	WB	HB	LB
Session verification details	SK	FK	NK	ZK	XK	PK	YK	WK	HK	LK

Column title	System State	Files and Folders	Network Shares	VSS MSSQL	Exchange Stores	SharePoint data	Oracle	VMware virtual machines	Hyper-V data	MySQL status
Licence items count	-	-	NI	-	-	-	-	WI	HI	-

Backup statistics by the data source (continued)

Column title	Total	Microsoft 365 Exchange	Microsoft 365 OneDrive
Status	T0	G0	J0
Selected count	T1	-	-
Number of files in selection	-	G1	J1
Changed count	T2	-	-
Number of changed files	-	G2	J2
Selected size	T3	G3	J3
Processed size	T4	G4	J4
Sent size	T5	G5	J5
Protected size	T6	G6	J6
Errors	T7	-	-
Number of errors	-	G7	J7
Session Duration	-	GA	JA
Last successful session	TL	GL	JL
Last successful session status	TQ	-	-
Status of the last successful session	-	GQ	JQ
Last session status	TJ	-	-
Status of the last completed session	-	GJ	JJ
Last session time	TO	-	-
Timestamp of the last completed session	-	GO	JO

Column title	Total	Microsoft 365 Exchange	Microsoft 365 OneDrive
Retention	-	GR	JR
Last 28 days	TB	-	-
Color bar - last 28 days	-	GB	JB
Session verification details	TK	GK	JK
Protected user accounts	TM	-	JM
Protected shared accounts	T@	-	-
Protected regular mailboxes	-	GM	-
Protected shared mailboxes	-	G@	-
Protected grouped accounts	-	-	J@

Status outputs are displayed as one of the following numeric values:

Value	Meaning
[1]	InProcess
[2]	Failed
[3]	Aborted
[5]	Completed
[6]	Interrupted
[7]	NotStarted
[8]	CompletedWithErrors
[9]	InProgressWithFaults
[10]	OverQuota
[11]	NoSelection
[12]	Restarted

Restore statistics by the data source

Column title	System State	Files and Folders	Bare Metal Recovery data	Virtual Disaster Recovery data	MySQL
Status (restore)	RS0	RF0	RB0	RV0	RL0
Number of files in selection (restore)	RS1	RF1	RB1	RV1	RL1
Number of changed files (restore)	RS2	RF2	RB2	RV2	RL2
Selected size (restore)	RS3	RF3	RB3	RV3	RL3
Processed size (restore)	RS4	RF4	RB4	RV4	RL4
Sent size (restore)	RS5	RF5	RB5	RV5	RL5
Number of errors (restore)	RS7	RF7	RB7	RV7	RL7
Session duration (restore)	RSA	RFA	RBA	RVA	RLA
Last successful session (restore)	RSL	RFL	RBL	RVL	RLL
Status of the last successful session (restore)	RSQ	RFQ	RBQ	RVQ	RLQ
Status of the last completed session (restore)	RSJ	RFJ	-	RVJ	RLJ
Timestamp of the last completed session (restore)	RSO	RFO	RBO	RVO	RLO
Color bar - last 28 days (restore)	RSB	RFB	RBB	RVB	RLB
Session verification details (restore)	RSK	RFK	RBK	RVK	RLK

Restore statistics by the data source (continued)

Column title	Total	Microsoft 365 Exchange	Microsoft 365 OneDrive	Network Shares	VSS MSSQL	Exchange stores	SharePoint data	Oracle	VMware virtual machines	Hyper-V data
Status	RT0	RG0	RJ0	RN0	RZ0	RX0	RP0	RY0	RW0	RH0

Column title	Total	Microsoft 365 Exchange	Microsoft 365 OneDrive	Network Shares	VSS MSSQL	Exchange stores	SharePoint data	Oracle	VMware virtual machines	Hyper-V data
(restore)										
Number of files in selection (restore)	RT1	RG1	RJ1	RN1	RZ1	RX1	RP1	RY1	RW1	RH1
Number of changed files (restore)	RT2	RG2	RJ2	RN2	RZ2	RX2	RP2	RY2	RW2	RH2
Selected size (restore)	RT3	RG3	RJ3	RN3	RZ3	RX3	RP3	RY3	RW3	RH3
Processed size (restore)	RT4	RG4	RJ4	RN4	RZ4	RX4	RP4	RY4	RW4	RH4
Sent size (restore)	RT5	RG5	RJ5	RN5	RZ5	RX5	RP5	RY5	RW5	RH5
Number of errors (restore)	RT7	RG7	RJ7	RN7	RZ7	RX7	RP7	RY7	RW7	RH7
Session duration (restore)	-	RGA	RJA	RNA	RZA	RXA	RPA	RYA	RWA	RHA
Last successful session (restore)	RTL	RGL	RJL	RNL	RZL	RXL	RPL	RYL	RWL	RHL
Status of the last successful	RTQ	RGQ	RJQ	RNQ	RZQ	RXQ	RPQ	RYQ	RWQ	RHQ

Column title	Total	Microsoft 365 Exchange	Microsoft 365 OneDrive	Network Shares	VSS MSSQL	Exchange stores	SharePoint data	Oracle	VMware virtual machines	Hyper-V data
session (restore)										
Status of the last completed session (restore)	RTJ	RGJ	RJJ	RNJ	RZJ	RXJ	RPJ	RYJ	RWJ	RHJ
Timestamp of the last completed session (restore)	RTO	RGO	RJO	RNO	RZO	RXO	RPO	RYO	RWO	RHO
Color bar - last 28 days (restore)	RTB	RGB	RJB	RNB	RZB	RXB	RPB	RYB	RWB	RHB
Session verification details (restore)	RTK	RGK	RJK	RNK	RZK	RXK	RPK	RYK	RWK	RHK
Microsoft 365 protected user accounts (restore)	RTM	-	-	-	-	-	-	-	-	-
Microsoft 365 protected shared accounts (restore)	RT@	-	-	-	-	-	-	-	-	-

Column title	Total	Microsoft 365 Exchange	Microsoft 365 OneDrive	Network Shares	VSS MSSQL	Exchange stores	SharePoint data	Oracle	VMware virtual machines	Hyper-V data
Protected regular mailboxes (restore)	-	RGM	-	-	-	-	-	-	-	-
Protected shared mailboxes (restore)	-	RG@	-	-	-	-	-	-	-	-
Protected user accounts (restore)	-	-	RJM	-	-	-	-	-	-	-
Protected grouped accounts (restore)	-	-	RJ@	-	-	-	-	-	-	-

User Guide for Cloud Management Console (legacy)

The Cloud Management Console is an older desktop-based version of the Management Console. Its supported ended in December 2017.

The current guide describes some of the less frequently used features that have not been migrated to the Management Console yet.

Legacy - Getting started with Cloud Management Console

The Cloud Management Console is an older desktop-based version of the Management Console. Its supported ended in December 2017.

Installation

Hardware requirements

The hardware requirements are very basic:

- Processor: Intel Pentium dual-core or better
- Memory (RAM): 128 MB
- Hard disk space: 80 MB (Windows), 110 MB (macOS)
- A working Internet connection

Software requirements

You can install the Cloud Management Console on the following operating systems:

- **Windows** - all versions starting from Windows XP and Windows Server 2003
- **macOS** - all versions starting from 10.6 Snow Leopard (64-bit)

Installation instructions

On **Windows**, download the Cloud Management Console and follow the installation wizard.

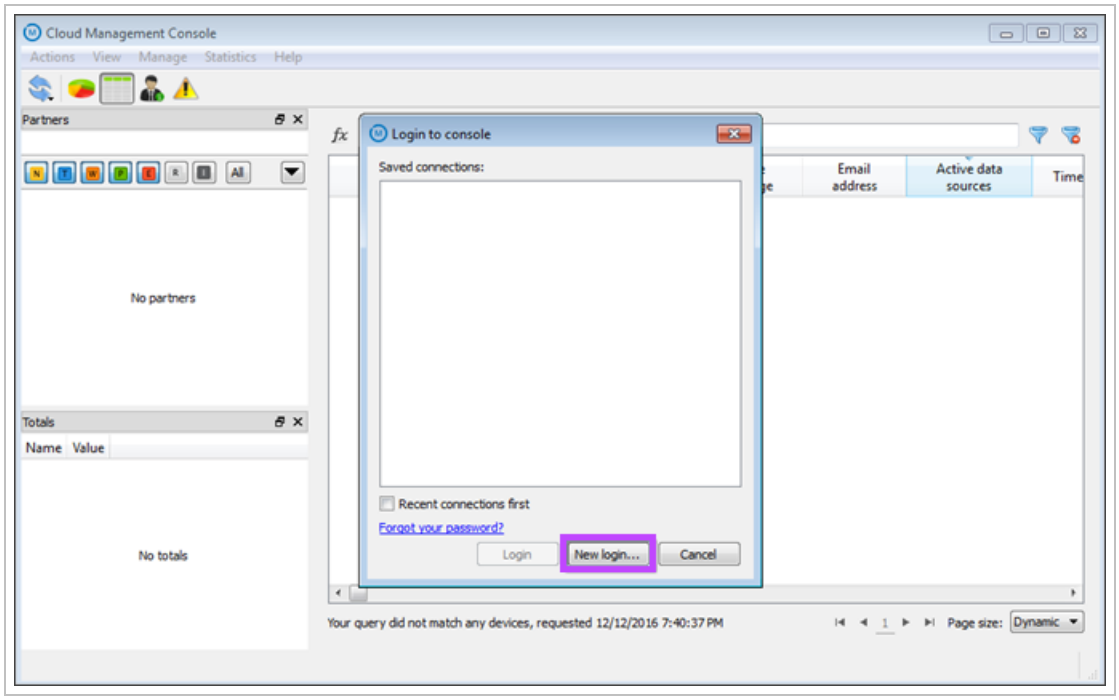
On **macOS**, do the following:

1. Download the Cloud Management Console
2. Open the "Downloads" folder in the Finder
3. Drag CloudManagementConsole to "Applications"

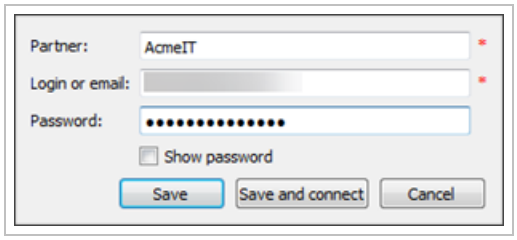
The installation is complete. Double-click on the application icon (M) to start the software.

User authorization

1. When you start the Cloud Management Console for the first time, you must log in to your account

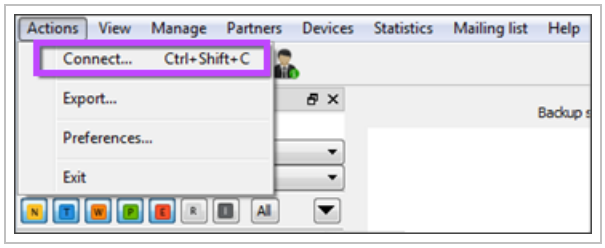


2. Click **New login** and enter your access details:
   - **Partner** - the name of the company you are trying to log in under
   - **Email** - the email address your user account is registered on
   - **Password** - the password for your user account
3. Click **Save and Connect**

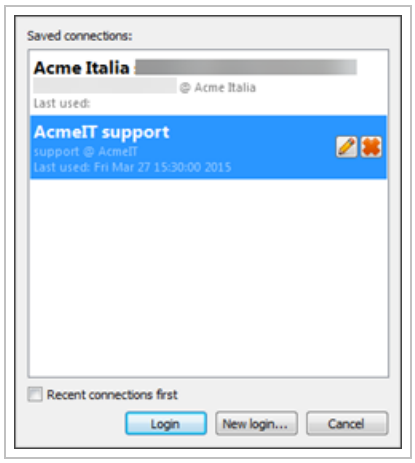


Managing existing connections

To manage existing connections, choose **Actions > Connect** from the menu bar at the top.



- To connect as another user, click **New login**
- To update your account credentials or to remove a connection from the list, click on its name and choose an appropriate option



One-time email notifications in Cloud Management Console

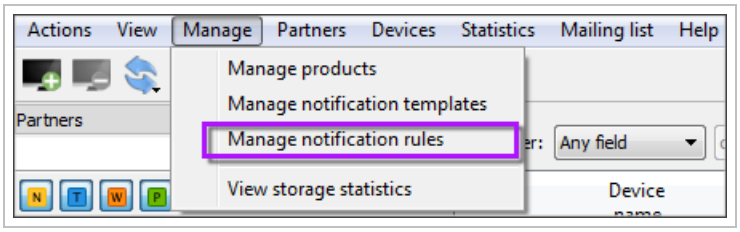
Cove Data Protection (Cove) provides 2 types of email notifications:

- **Scheduled** notifications (used for the delivery of Backup and Continuity dashboards on a regular basis). They are set up through the Management Console (instructions)
- **One-time** notifications (based on a certain event). At the moment, these can be set up only through the Cloud Management Console

Instructions

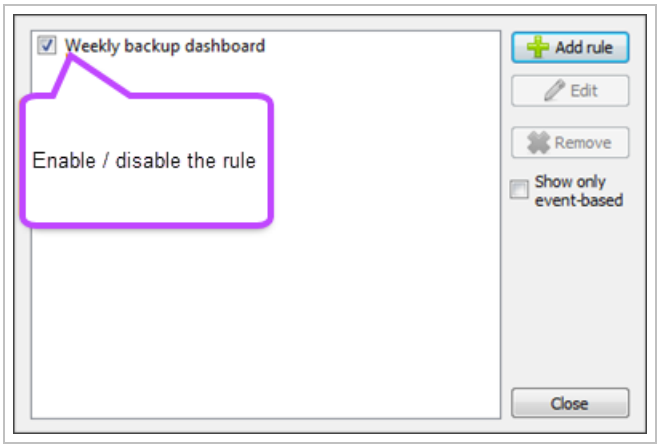
Here is how to create one-time notifications:

1. Log in to the Cloud Management Console under a SuperUser account
2. Select a customer on the **Partners** panel (the rule will work for this customer and its customers)
3. Click **Manage > Manage notification rules**



4. Click **Add rule**
5. Format the rule as appropriate
6. **Save** the changes

If the rule has been formatted correctly, it will start working as soon as it is created. You can disable it using the checkbox next to its name (and enable it again when necessary).



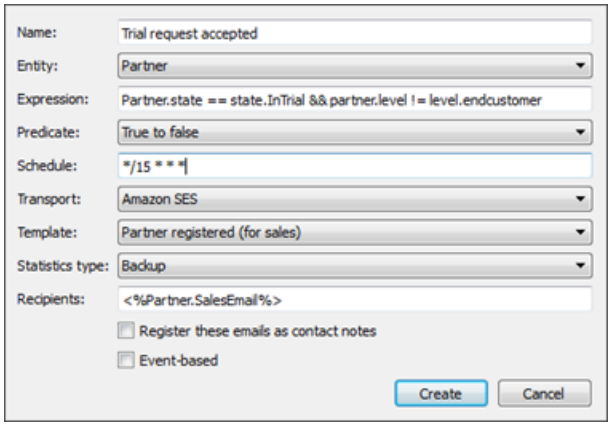
Formatting rules

Rules related to customers and their activities

Field name	Value	Definition
Entity	Partner	
Event-based	Not selected	
Expression	partner.state == state.registered && partner.level != level.endcustomer	Customer registered for trial
	partner.state == state.InTrial && partner.level != level.endcustomer	Trial request accepted
	partner.state == state.rejected	Trial request rejected
	partner.state == state.intrial && partner.begintrialdate + 8.days() < Time.now() && partner.level != level.endcustomer	8th day of trial is over
	partner.state == state.intrial && partner.begintrialdate + 15.days() < Time.now() && partner.level != level.endcustomer	15th day of trial is over
	partner.state == state.waitingforproduction && partner.level != level.endcustomer	Customer ready for production
	partner.state == state.InProduction && partner.level != level.endcustomer	Customer approved for production

Field name	Value	Definition
	partner.state == state.NotActive	Customer disabled for inactivity
Predicate	False to true	
Schedule[1]	`*/1 * * *`	Every minute (recommended for urgent emails, for example those that require the delivery of access details)
	`*/15 * * *`	Every 15 minutes
	`0 */6 * *`	Every 6 hours
Statistics type	(Not applicable)	

Here is a sample one-time notification rule related to customers' activities.



Rules related to session statuses

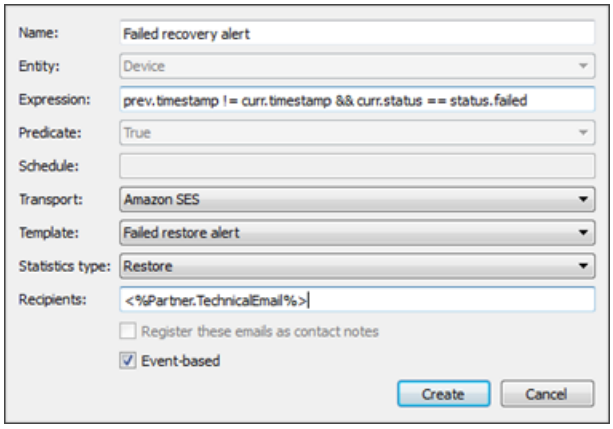
You can create rules for the delivery of email alerts based on certain session statuses of backup devices. For example, if a backup session fails, all people concerned will immediately get an email notification. This is possible both for backup sessions and restore sessions.

Field name	Value	Definition/comments
Event-based	Selected	
Expression	prev.timestamp != curr.timestamp && curr.status == status.failed	Create an alert if a session fails.
	prev.timestamp != curr.timestamp && curr.status == status.aborted	Create an alert if a session gets aborted.

[1]This is how often the system will be checking if the event has occurred.

Field name	Value	Definition/comments
	prev.timestamp != curr.timestamp && curr.status == status.inprocess	Create an alert if a session is in progress. If the session lasts more than 15 minutes, there will be several notifications with 15-minute intervals.
	prev.timestamp != curr.timestamp && curr.status == status.completedwitherrors	Create an alert if a session is completed with errors.
	prev.timestamp != curr.timestamp && curr.status == status.notstarted	Create an alert if a session does not start as due.
	prev.timestamp != curr.timestamp && curr.status == status.overquota	Create an alert if a session fails with the "Overquota" status (product limitations exceeded: maximum file size, maximum selection size or maximum used storage).
	prev.timestamp != curr.timestamp && curr.status == status.completed	Create an alert if a session is successfully completed.
	prev.timestamp != curr.timestamp && (curr.status == status.completed || curr.status == status.completedwitherrors) && curr.plugin==plugin.VirtualDisasterRecoveryPlugin	Create an alert if a virtual disaster recovery session is successfully completed or completed with errors. If the **Start the virtual machine after restore and take screenshot** setting has been enabled in the virtual disaster recovery settings, the email notification will contain a screenshot confirmation of the booted virtual machine along with the following details: ▪ the machine name ▪ the system time ▪ the recovery session time ▪ the list of stopped services with the `autostart` property ▪ system log records (you can customize their number through the advanced settings (the `VdrCheckReportSystemLogCount` parameter)
Statistics type	▪ Backup ▪ Restore	Determines whether the rule applies to backup sessions or to restore sessions.

Here is a sample rule for a failed recovery session.



Rules related to LocalSpeedVault and Cloud storage statuses

Field name	Value	Definition/comments
Event-based	Selected	
Expression	curr.lsvStatus == synchronizationStatus.failed && prev.lsvStatus != curr.lsvStatus	Create an alert if the LocalSpeedVault fails to synchronize with the Cloud (or with remote storage for software-only customers).
	(curr.lsvStatus == synchronizationStatus.running || curr.lsvStatus == synchronizationStatus.synchronized) && prev.lsvStatus == synchronizationStatus.failed	Create an alert if the LocalSpeedVault status changes from "Failed" to "Synchronized" or "Synchronizing"
	curr.lsvStatus == synchronizationStatus.synchronized && prev.lsvStatus == synchronizationStatus.failed	Create an alert if the LocalSpeedVault status changes from "Failed" to "Synchronized"
Statistics type	Backup	

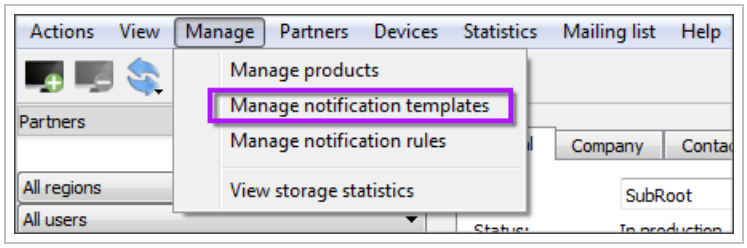
> To create notification rules based on Cloud storage statuses, replace `lsvStatus` with `backupServerStatus` in the expression.

Templates for one-time notifications in Cloud Management Console

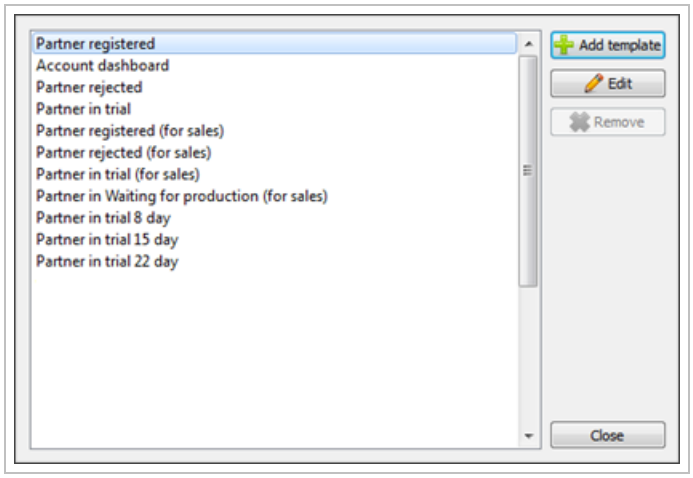
The content of email notifications in the Cloud Management Console is based on **templates**.

Here is how to manage the templates:

1. Log in to the Cloud Management Console using a SuperUser account
2. On the **Partners** pane, click the customer whose email templates you want to access
3. Go to **Manage > Manage notification templates**



There is a set of **predefined templates** to choose from. You can fine-tune these templates **(Edit)** or create new ones from scratch **(Add)**. They can be formatted as HTML or pure text. An extensive set of variables is supported.



> You can delete unneeded templates created by your company and your customers **(Remove)**. This is possible if there any no notification rules involving the template.

Variables supported by templates

You can insert variables to the **Subject** field and to the body of your messages.

> HTML file headers do not support variables.

Variables related to customers in Cloud Management Console

There is a group of variables that display information related to **customers and their devices**.

Customer properties

Variable	Description	Output
`<%Partner.Name%>`	The name of the customer the email noti-fication is related to	Text

Variable	Description	Output
`<%ManagementLocation%>`	The address of the cloud services assigned to the customer	URL, for example `https://cloud-backup.management:443`
`<%Partner.AdministrativeFullName%>`	The full name of the customer's contact person of the "Administrative" type. If there are several people, the name of the first person in the list is displayed.	Text (first and last name)
`<%Partner.UserAdministrativeFullName%>`	The full name of the customer's user of the "Administrative" type. If there are several people, the name of the first person in the list is displayed.	Text (first and last name)

Totals for customer's devices

Variable	Description	Output
`<%DeviceCount%>`	The total number of devices belonging to the company and its own customers	Number
`<%SelectedSize%>`	The total amount of data currently selected for backup on all devices belonging to the customer and its own customers	Number with unit of measurement, for example "4.99 GB"
`<%UsedStorage%>`	The total amount of storage space taken by all devices belonging to the customer and its own customers	Number with unit of measurement, for example "245.59 MB"

Customer's devices by status

Use these variables to display the number of devices with a particular status. The backup status is identified by the last backup session.

Variable	Description
<%BackupStatusCompleted%>	The number of devices on which the last backup session was completed successfully
<%BackupStatusCompletedWithErrors%>	The number of devices on which the last backup session was completed with errors
<%BackupStatusInProgress%>	The number of devices on which a backup is currently running
<%NotStarted%>	The number of devices on which the last backup session was not started
<%NoSuccessfulBackup%>	The number of devices with no successful backups
<%LastBackupLessThan24Count%>	The number of devices backed up less than 24 hours ago
<%LastBackupLessThan48MoreThan24Count%>	The number of devices backed up between 24 and 48 hours ago
<%LastBackupMoreThan48Count%>	The number of devices backed up more than 48 hours ago

Ratio of devices with a status

Use these variables to display the ratio of devices with a particular status to the total number of devices. The status is identified by the last backup session.

Variable	Description
<%CompletedPercentage%>	The ratio of devices that have been successfully backed up
<%CompletedWithErrorsPercentage%>	The ratio of devices backed up with some errors
<%FailedPercentage%>	The ratio of devices on which the last backup session failed
<%InProcessPercentage%>	The ratio of devices that are currently backed up
<%LastBackupLess24Percentage%>	The ratio of devices backed up less than 24 hours ago
<%LastBackupMore24Less48Percentage%>	The ratio of devices backed up between 24 and 48 hours ago
<%LastBackupMore48Percentage%>	The ratio of devices backed up more than 48 hours ago
<%NoSuccessfulBackupsPercentage%>	The ratio of devices with no successful backups
<%NotStartedPercentage%>	The ratio of devices on which the last backup session was not started

Auxiliary variables

Variable	Description	Output
`<%HasFailedStatuses%>`	Indicates the presence of failed backup/recovery sessions on the devices belonging to the customer and its child customers. This is useful for formatting. For example, the background color of the message can be set to red if the value is `1`.	▪ `0` (no failed sessions) ▪ `1` (there is at least 1 failed session)

Variables related to devices in Cloud Management Console

Most of the variables can be applied to backup and restore sessions so you can use them in notification rules of both types (backup and restore).

General statistics

This group of variables displays basic device characteristics (their names, the names of customers they belong to, etc.) as well as creation dates for the notifications.

Variable	Description	Output
`<%computer%>`	The name of the computer that the device is installed on. If there are several installations, the system will display the computer that the most recent backup/restore activity was detected on.	Text
`<%countPlugins%>`	The number of data sources that have been active during the last backup/restore session (depending on the type of the rule).	Number
`<%date%>`	Shows when the notification was created.	Day, date and time. Example: Wed, 20 Jan 2015 08:49:37 GMT
`<%device%>`	The name of the device a notification has been created for	Text, for example "sales-lenovo"
`<%partner%>`	The name of the customer the device belongs to	Text

Variable	Description	Output
`<%product%>`	The product assigned to the backup device (determines access to features and storage options)	Text
`<%timestamp%>`	Shows when the most recent backup/restore activity on the device took place.	**Time** for today's activities (for example "6:13:09 PM"), **month and date** for activities that took place this year ("Mar 16") or **month and year** for older activities ("Dec 2014").
`<%localSpeedVaultEnabled%>`	Shows if the LocalSpeedVault feature is enabled on the device.	▪ true ▪ false
`<%backupServerSynchronizationStatus%>`	Shows if the local data on the client machine is synchronized with the Cloud (or with remote storage for software-only customers)	▪ Failed ▪ Disabled ▪ Synchronizing ▪ Synchronized ▪ <None> (undefined)
`<%localSpeedVaultSynchronizationStatus%>`	Shows if the LocalSpeedVault is synchronized with the Cloud (or with remote storage for software-only customers)	▪ Failed ▪ Disabled ▪ Synchronizing ▪ Synchronized ▪ <None> (undefined)

Statistics for each data source

The following variables display statistics for each data source protected on a device: its name, the duration of sessions related to it, the amount of storage its data occupies and more.

Variable	Description	Applies to sessions	Output
`<%plugin.backupStatus%>`	The status of the last session	Backup only	▪ In progress ▪ Completed ▪ Completed with errors ▪ Failed

Variable	Description	Applies to sessions	Output
`<%plugin.duration%>`	The duration of the last session	Backup & restore	HH:MM:SS. For example, 00:25:08
`<%plugin.errorsCount%>`	The number of errors in the last session		Number
`<%plugin.name%>`	The name of a data source		One of the following: ▪ Files and folders ▪ Network shares ▪ System state ▪ Oracle ▪ MySQL ▪ MS SQL ▪ VMware ▪ Hyper-V ▪ MS Exchange ▪ MS SharePoint ▪ Virtual disaster recovery *(for restore sessions only)* ▪ Bare-metal recovery *(for restore sessions only)*
`<%plugin.processedCount%>`	The number of files processed during the last session		Number
`<%plugin.processedSize%>`	The amount of data processed during the last session		Number with unit of measurement, for example "44.3 MB"
`<%plugin.protectedSize%>`	The amount of data protected on the current backup device. All files in the backup selection and their older ver-	Backup only	Number with unit of measurement, for example "44.3 MB"

Variable	Description	Applies to sessions	Output
	sions from previous backup sessions are taken into account.		
`<%plugin.restoreStatus%>`	The status of the last restore session	Restore only	▪ In progress ▪ Completed ▪ Completed with errors ▪ Failed
`<%plugin.selectedCount%>`	The number of files in the selection	Backup & restore	Number
`<%plugin.selectedSize%>`	The amount of data selected for backup or recovery		Number with unit of measurement, for example "44.3 MB"
`<%plugin.sentSize%>`	The amount of data submitted to the storage (or from the storage) during the last session		Number with unit of measurement, for example "44.3 MB"
`<%plugin.sessionStatus%>`	The status of the last backup or restore session (depending on the type of the rule).		▪ In progress ▪ Completed ▪ Completed with errors ▪ Failed

Predefined text

The default email templates for failed backup and restore alerts may contain variables displaying **predefined text**. This text changes automatically depending on a user's locale (if a translation into that language is available). To use your own text, remove the corresponding variable from the notification template. If necessary, update the translated versions as well.

Variable	Text displayed
`<%computerCaption%>`	Computer name:
`<%helloMessage%>`	Dear customer,
`<%infoMessage%>`	We are writing to let you know that something has gone wrong with one of your recent backups. We hope the details provided below help you resolve the issue.
`<%restoreInfoMessage%>`	We are writing to let you know that something has gone wrong with one of your recent restores. We hope the details provided below help you resolve the issue.
`<%detailsMessage%>`	Details:

Variable	Text displayed
`<%datasourceCaption%>`	Data source:
`<%deviceCaption%>`	Device name:
`<%partnerCaption%>`	Partner name:
`<%productCaption%>`	Product:
`<%sessionStatusCaption%>`	Status:
`<%signMessage%>`	Please don't hesitate to contact us if you need help. Best regards, your backup team

Common settings for notification templates in Cloud Management Console

Name

Each notification rule requires a unique name. This name does not appear anywhere outside of the Cloud Management Console. Its purpose is to help you find the rules you need faster.

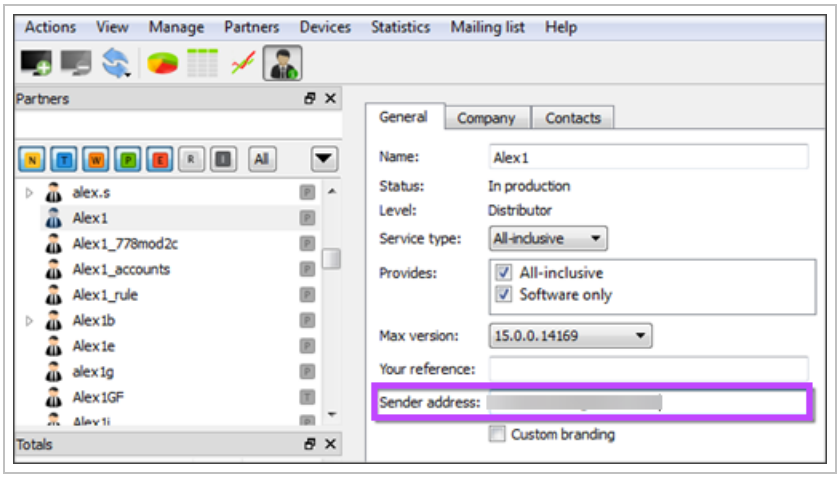
Template

Each notification rule requires a template. The template selected determines what kind of message your customers will be receiving. You can use one of the predefined templates or create your own.

Templates for one-time notifications in Cloud Management Console

Transport

All email notifications are delivered through a specialized mail service (Amazon SES). It is done on behalf of an existing mail account (this account shows in the **From** field of your email notifications). The address of this account is taken from the **Sender address** field of the customer's profile in the Cloud Management Console.



If no email address is specified there, the Cloud Management Console will use the address specified for the parent customer. If it is also missing, it will not be possible to send notifications.

> Amazon SES allows only those mail accounts that users actually have access to. When you enter a new sender address, Amazon sends an email with a confirmation link to that email address. It is necessary to open the message and follow the link in it to confirm your ownership of the account.

Recipients

When you create a new email notification rule, you must specify recipients. You can enter one or several email addresses separated by a comma (,) or a semicolon (;). It can be a good idea to use variables, especially for customers that have customers of their own.

1. `<%Partner.SalesEmail%>` - the email address of a contact person with the "Sales" role. Works for notifications related to customers (where **Entity** is set to "Partner" or "PartnerWithAccounts")
2. `<%Partner.AdministrativeEmail%>` - the email address of a contact person with the "Administrative" role. Works for notifications related to customers (where **Entity** is set to "Partner" or "PartnerWithAccounts")
3. `<%Partner.TechnicalEmail%>` - the email address of a contact person with the "Technical" role. Works for notifications related to customers (where **Entity** is set to "Partner" or "PartnerWithAccounts")
4. `<%Partner.AuthorizedSignerEmail%>` - the email address of a contact person with the "Authorized Signer" role. Works for notifications related to customers (where **Entity** is set to "Partner" or "PartnerWithAccounts")
5. `<%DashboardEmail%>` - the email address a device is associated with. Works for notifications related to devices (where **Entity** is set to "Account")

> If you have several contact people with the same role, only one of them will receive the notification (the one who comes first in the list).

Register these emails as contact notes

There is a feature letting you trace communication with customers better. If you select the **Register these e-mails as Contact Notes** checkbox, right after an email is sent according to the rule, a corresponding note will appear in Contact Notes. To view the notes, switch to **Partner information view** and open the **Contacts** tab.

ConnectWise Billing integration with Cloud Management Console

> ✖ ConnectWise Billing integration is no longer supported within the Management Console and there are no plans to reinstate it.

Autotask integration with Cloud Management Console

> ✖ Autotask integration is no longer supported within the Management Console

PDF version of Documentation

If you would like access to a PDF version of this documentation for offline use, this can be found here.

Please be aware that this version of the documentation may not be as up to date as the online version.

This documentation is comprehensive and so, very large; it contains over 1300 pages when in a PDF format so please be conscious of the environment when printing.

Glossary of Cove Data Protection (Cove) terms