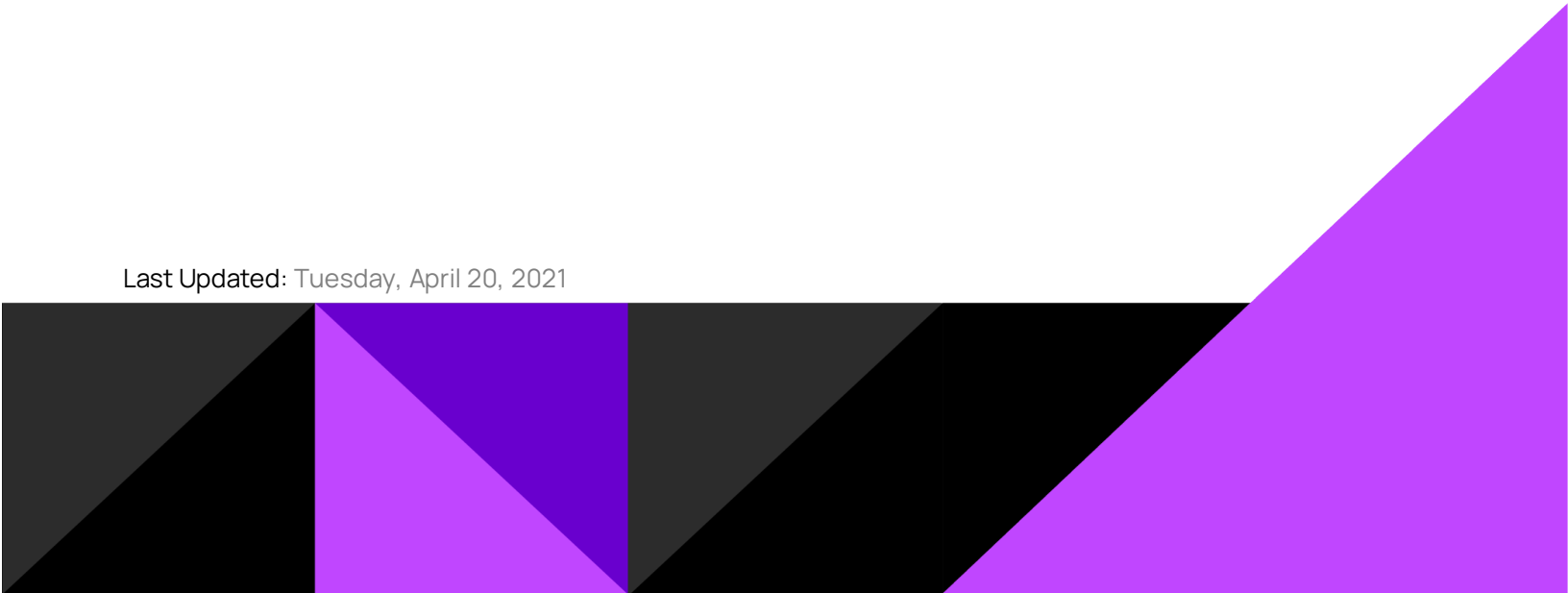
N-central

Release Notes

Version 2021.1 HF3 Build: 2021.1.3.428

Last Updated: Tuesday, April 20, 2021



Upgrade paths and notes

To upgrade to 2021.1 HF3, your N-able N-central server must be running one of the following versions:

- N-able N-central 12.3.0.241 – 850
- N-able N-central 2020.1.0.202
- N-able N-central 2020.1.1.273
- N-able N-central 2020.1.2.326
- N-able N-central 2020.1.3.381
- N-able N-central 2020.1.4.402
- N-able N-central 2020.1.5.411+
- N-able N-central 2020.1.6.478
- N-able N-central 2020.2.0.140+
- N-able N-central 2021.1.0.32+
- N-able N-central 2021.1.1.305
- N-able N-central 2021.1.2.391

Note the following when upgrading N-able N-central.

Scheduled Tasks may expire if the agent on an associated device is being upgraded when the task is scheduled to be completed. Agent upgrades are normally short in duration but may be delayed if a re-start of the device is pending.

Fixed Issues in N-able N-central

Release 2021.1 HF3

Category	Description	Bug
Core	Address CVE-2021-3449 By Upgrading To OpenSSL 1.1.1k	NCCF-16115

Release 2021.1 HF2

Automation Manager	Unable to launch Automation Manager	AM-2631
AV Defender	Granting Access To An Update Server Isn't Being Saved	IAV-1395
Endpoint Detection and Response	EDR Analyze Tab and Edit Policy unable to load	KUIP-2908
Endpoint Detection and Response	The EDR Service Template For macOS Devices Monitors The Wrong Process Name	KUIP-2838
Endpoint Detection and Response	An EDR License Is Still Consumed By Devices That Have Had EDR Disabled	KUIP-2795
Core	Integration management - Can not activate a new integration	KUIP-2880
Core	N-Central agent does not uninstall Ecosystem Agent on 32 bit devices.	KUIP-2662
Core	The License Usage Report Shows 0 EDR Licenses Available	KUIP-2305
Core	Server Stability Affected By Agent Submission of LastLoginUser	NCCF-15849
Core	N-central -> Backup Sync Logic Can Sometimes Change The Backup Profile That Is Assigned To A Device	NCCF-15631
Core	The Windows Agent Crashes Due To An Unhandled Exception In The Take Control Interface Code	NCCF-15399

Core	CVE-2021-3156 sudo: Heap buffer overflow	NCCF-15384
Core	EDF checkbox could be enabled on Device with Essential license ONLY for new installations	NCCF-15114
Core	Feature Flag Logging Doesn't Capture Exceptions	NCCF-15095
Core	The Registration Token Permission Isn't Properly Applied To The customerList And customerListChildren APIs	NCCF-14797
Core	The Custom Protocol Handler Doesn't Properly Handle An Invalid "Application To Run" Value	NCCF-14752
Core	Significant UI delays when performing standard tasks	NCCF-14718
Core	Unexpected Growth Of The "/var/log/n-central/monitor" Directory Impacts Server Stability and Performance	NCCF-14541
Core	Wrong Transition Time Is Used For Notifications If The Notification Delay Is Longer Than The Downtime Window Of The Service	NCCF-13839
Monitoring	The "Veeam Job Monitor" And "Veeam Sure Job Monitor" Services Don't Work With Veeam 11	AM-2609

Release 2021.1 HF1

Category	Description	Bug
AV Defender	Spaces Are Removed From AV Defender Exclusions When An Exclusion Is Added Or Modified	IAV-1801
DNSFilter	The Visibility Of The DNS Filter Permissions Aren't Controlled By The DNS Filter Feature Flag	KUIP-2887
DNSFilter	Deleting a Customer That Contains An EDR-Enabled Device End Up Erroneously Provisioning a DNS Filter Trial	KUIP-2885

Release 2021.1

Category	Description	Bug
Automation Manager	The "Is Application Installed" Object Fails to Find Applications on Windows Devices That Are Using Non-English Locales	AM-2524
Automation Manager	The "Download File From URL" Object Fails To Download The Specified File	AM-2517
Automation Manager	The "Restart System" Automation Manager Policy Fails To Restart The Targeted Device	AM-2512
Automation Manager	Unable To Open An Automation Manager Policy If It Was Built With v2.15 Or Below, And Included The "Restart System" Object	AM-2478
Automation Manager	Output From the "User Not Logged On In N Days" Object Is Not Available For Use In The For/Each Object	AM-2465
Automation Manager	AMP-based Scheduled Tasks Fail with a ""Error: This policy requires administrative rights" Because Automation Manager Doesn't Check If The User Is a Member of the Domain Admins Group	AM-2409
Automation Manager	The "Run Windows Defender Full Scan" Automation Manager Policy Isn't Successfully Running	AM-2384
Automation Manager	Unable to Configure Timeout Value For the "Execute a SQL Query" Object	AM-2380
AV Defender	Granting Access To An Update Server Isn't Being Saved	IAV-1395
Core	Envoy is not restarted when NKO detects a problem with Jetty	NCCF-15364
Core	The Re-signed Versions Of The Automation Manager Designer and Teamviewer Launcher Are Not Installed On Upgrade	NCCF-15102
Core	Digital Certificate Error When Launching Java-Controlled Remote Control Methods	NCCF-15101
Core	Probe Upgrades Failing When Using MSI Fallback Mechanism	NCCF-15012
Core	Windows Probes Fail To Upgrade Due To A Corrupt Version of probeAssetImageMap.txt	NCCF-15011
Core	Reactivations Of N-central Fail Due To Changes To The NableAdmin	NCCF-

Category	Description	Bug
	E-mail Address	14899
Core	Installing the Linux Agent on RHEL 8 Results In A Device With "Other" As The Operating System and Device Class	NCCF-14974
Core	Upgrade Struts To Address CVE-2020-17530	NCCF-14931
Core	2020.2.0.140 - CentOS8 agent Customer/Site specific agent install not working	NCCF-14745
Core	Some Recurring PowerShell/VBS/Batch Scheduled Tasks Created Before Upgrading to 2020.1 HF3 Start Failing After N-central is Upgraded to 2020.1 HF3	NCCF-14743
Core	Upgrade to 2020.2 RC Fails If The Server Was Ever Running Pre-11.1 Versions Of N-central	NCCF-14680
Core	MaintDataExpiry failing due to DataExportStatusServiceImpl expecting the wrong value	NCCF-14648
Core	New Configuration Created in ConnectWise If Existing CI's Configuration Type Is Changed	NCCF-14642
Core	Selecting Specific Users In The "Domain User Management" Screen, Before The Page Fully Loads, Causes All Users To Be Selected	NCCF-14579
Core	NTPdate Error Causes The System Time Of N-central To Be Set To Thu, Feb 7 2036	NCCF-14526
Core	Data Encryption Error Displayed When RDP Remote Control Falls Back From SSH To HTTPS	NCCF-14517
Core	The Probe Fails To Complete The Registration Process When Installed From The Command Line And An Activation Key Is Specified	NCCF-14505
Core	N-central UI Was Inaccessible Due To Performance Issues With JobStatusList.java	NCCF-14486
Core	N-central Stops Accepting SSH Tunnel Requests After 50 R/C Sessions	NCCF-14472
Core	Server Stability Affected By Indefinitely Activated Threads	NCCF-14466

Category	Description	Bug
Core	Logging In To N-central Over HTTP Hangs When Loading deployJava.js	NCCF-14395
Core	AMP Fails To Run When Input Parameters Contain Special Characters	NCCF-14392
Core	Device not being marked as 'Inactive' in Autotask when device is deleted in N-central	NCCF-14356
Core	Choosing "Save and Propagate" For A Custom Organization Property Doesn't Trigger Rule Re-application	NCCF-14321
Core	Agent status is down on Mothership monitoring	NCCF-14265
Core	Contract ID is temporarily removed for Devices already exported to MSP Manager	NCCF-14235
Core	The "License Usage" Report Incorrectly Counts Devices Twice For "Remote Control on Essentials" Licenses	NCCF-14229
Core	Unnecessary Network Traffic Caused By The Windows Agent Communicating with Domain Controllers Over LDAP	NCCF-14222
Core	Modifying The Users Assigned To a Role At A Lower Level Wipes Out Users Associated At A Higher Level	NCCF-14209
Core	System Error Shown When Running A Scheduled Task From Within The Tools Menu	NCCF-14160
Core	The "Create Ticket" Button Is Missing from the Overview -> Active Issues Widget	NCCF-14123
Core	Modifying Device-Level Remote Control Settings Can Modify The Remote Control Settings Of Other Devices	NCCF-14111
Core	The Tools -> Services Tab Shows "The agent has not detected any services"	NCCF-14085
Core	Logic Flaw In The Agent's Config Backup Process Can Result In Agents Losing Their Configuration Settings	NCCF-14075
Core	UI error needed for ticket recipients after setting issue type to inactive in Autotask	NCCF-14072

Category	Description	Bug
Core	System Error When Propagating Remote Control Defaults to Existing Sites	NCCF-14070
Core	Automation Manager will not open or save items to N-Central when logged in using Google SSO Account	NCCF-14069
Core	Apache Releases Security Advisory for Struts 2	NCCF-14068
Core	The Remote Control Icon Is Unavailable To Users That Only Have Access To Take Control	NCCF-14066
Core	CVE-2020-10713 - Boot Hole GRUB2 Vulnerability	NCCF-14062
Core	Audit Trail Shows Incorrect "End Time" Values For Take Control Sessions	NCCF-14048
Core	Custom Protocol Handler Log Files Show The One-Time Credentials Used for RDP Remote Control Sessions	NCCF-14026
Core	A System Error Is Thrown When Selecting The "Launch Moving Devices" Wizard For A Site With Only Unmanaged Devices	NCCF-14011
Core	Changing the Dates in the "Availability of Multiple Services on One Device" Report Incorrectly Shows Different Service Availabilities	NCCF-13965
Core	The "Detailed Status" Report Incorrectly Shows A Service As Disconnected Instead Of Failed	NCCF-13956
Core	Agent & Probe Settings won't load without Registration Tokens permission	NCCF-13951
Core	Session ID Must Be Renewed After Both Password Validation and MFA Validation	NCCF-13928
Core	Active User Sessions Aren't Invalidated When The Users Password Is Changed	NCCF-13927
Core	Filtering By MAC Address Doesn't Return Devices If The MAC Address Isn't Associated To An IP Address	NCCF-13909
Core	MDM: Filtering By "Tracking Status" Doesn't Work As Expected	NCCF-13882

Category	Description	Bug
Core	N-central OS Level Administration and Recovery Users Cannot Log in to the Server Console Due to UID Restrictions	NCCF-13876
Core	RDP Remote Control: Fallback to HTTPS Tunneling Doesn't Occur When The Target Device Blocks Outbound Port 22 (SSH) Traffic	NCCF-13859
Core	When Editing An Access Group At The SO Level, Only 75 Sites Are Displayed For A Given Customer	NCCF-13847
Core	System Error When Attempting To Delete A Device	NCCF-13843
Core	Wrong Transition Time Is Used For Notifications If The Notification Delay Is Longer Than The Downtime Window Of The Service	NCCF-13839
Core	System Error When Filtering the Patch Status Dashboard To Only Display Windows Workstations and Laptops	NCCF-13832
Core	Adding a New Device To A Scheduled Instance Of the Service Metrics Report Removes Previously Selected Service Instances	NCCF-13829
Core	CentOS 7 Agent Crashes When Performing ODBC Monitoring	NCCF-13827
Core	Upgrading N-central Fails If the Azure Agent Had Been Manually Installed	NCCF-13816
Core	Product Admin Cannot Modify Their Own RSS Feed Settings	NCCF-13802
Core	Export Profile targeting by Device Class exports unrelated Devices	NCCF-13767
Core	Error-Level Entries Seen in the Windows Event Log for the "N-able ShadowProtect Monitoring Service"	NCCF-13729
Core	The Asset Tab Shows DDR4 RAM "Unknown"	NCCF-13715
Core	When a Custom Property Is Changed, All Rules Associated To A Device Are Reapplied, Instead Of Only The Rules Associated To The Custom Property	NCCF-13712
Core	Failing To Connect To The Cache Of One Windows Probe Doesn't Cause The Windows Agent To Try Connecting To Other Windows	NCCF-13697

Category	Description	Bug
	Probes In The Environment	
Core	Legacy Security Profile was not Restored with N-central Backup Restore	NCCF-13599
Core	Users With Read-Only Access Can Still Change Their Own MFA Settings	NCCF-13521
Core	Sorting the Script/Software Repository by "Upload Date" sorts by Year and then month alphabetically	NCCF-13480
Core	XMPP Module Causes A Memory Leak In The Linux Agent	NCCF-13456
Core	The Configuration Summary Report Doesn't Respect The "Include Task Execution History" Option When It's Exported To PDF	NCCF-13431
Core	Organizational Custom Properties Inherit From Source Level, Not The Immediate Parent Level	NCCF-13412
Core	Windows Services With A Trailing Space In Their Names Are Not Discovered	NCCF-13258
Core	Launching JNLP-based Remote Control From A macOS Device Prematurely Times Out	NCCF-13193
Core	Virtual Machines Aren't Displayed Under the "Asset -> Hyper-V Guests" Tab	NCCF-12339
Core	Unable To Sort By The Status Column On The "Configuration -> Scheduled Tasks -> Add/Delete" Page	NCCF-11886
Core	Device Does Not Perform An AV scan After Missing Its Scheduled Time	NCCF-11364
Core	N-central Incorrectly Tells An Agent To Uninstall Itself When It Was Only Set to Unmanaged	NCCF-9932
Core	Workflow To Uninstall An Agent Stops When The User Confirms That They Want To Proceed	KUIP-2031
Core	All Devices/Active Issues View: The Integration Column Does Not Stay Hidden	KUIP-1729
Endpoint	"EDR Status" Service applying to devices without EDR	KUIP-2544

Category	Description	Bug
Detection and Response		
Endpoint Detection and Response	The License Usage Report Shows 0 EDR Licenses Available	KUIP-2305
Endpoint Detection and Response	The "EDR Status" Service Reports A "201 Failure error" Misconfigured State	KUIP-2199
Endpoint Detection and Response	Unable To Access EDR Profiles	KUIP-1858
Monitoring	The Windows Probe Crashes When Using SNMPv3 To Poll A Large Number Of Services	BEAT-1982
Monitoring	The Windows Probe Crashes When Using SNMPv3 To Poll A Large Number Of Services	BEAT-1982
Monitoring	Custom SNMP Service Isn't Being Added to Discovery Jobs	BEAT-1824
Monitoring	Windows Service Monitoring Causes WMI To Crash	BEAT-1817
Monitoring	custom service missing "Use Asset Info" option	BEAT-1801
Monitoring	Custom SNMP Service Doesn't Have the "Use Asset Info" Option Within Service Templates	BEAT-1798
Monitoring	When Editing a Custom SNMP Service The "Enable Field Editing" Gets Disabled When The Cancel button Is Pressed	BEAT-1791
Monitoring	Scan Now Isn't Working For Agent-Monitored Services	BEAT-1733
Monitoring	Incorrect Unit Scaling on the "Total known users/sec" Metric in the IIS Service	BEAT-1524
Monitoring	AMP-Based Custom Services Cannot Be Imported When The Description Field Of The AMP Includes The Double-Quote Character	BEAT-1481
Monitoring	LSI Physical Drives Aren't Discovered by the Windows Probe When Scanning a VMware ESXi Server	BEAT-1075
MSP Backup	Information Disclosure Vulnerability In A URL	NCCF-

Category	Description	Bug
		15123
Patch Management	System Error When Running The 'Missing Patches (Summary)' Report	NCPM-4619
Patch Management	System Error When Adding A Scheduled Reboot Window From The All Devices View	NCPM-4594
Patch Manager	Patch Approvals Created By Auto-Approval Are Not Synchronized To The Agent	NCPM-4577
Patch Manager	Automatic Approval Rules Not Approving Patches	NCPM-4485
Patch Manager	Patch status v2 service misconfigured due to "201 Object reference not set to an instance of an object"	NCPM-4435
Security	Enhance the Detection of UI Session Attacks. VE 2020-15909 Session ID anomaly detection has been added, binding the session ID to the client IP address and user agent. This is configurable in N-central, with both protections defaulting to "On". Partners should review the settings under Administration > Mail and Network Settings > Network Security on upgrade and adjust as needed. Please see this KB Article for additional details.	NCCF-13912
Security	Enhance Brute-Force Prevention On UI login MFA	NCCF-13897

Known Limitations

These items for the current version of the N-able N-central software is composed of material issues significantly impacting performance whose cause has been replicated by N-able and where a fix has not yet been released. The list is not exclusive and does not contain items that are under investigation. Any known limitations set forth herein may not impact every customer environment. The N-able N-central software is being provided as it operates today. Any potential modifications, including a specific bug fix or any potential delivery of the same, are not considered part of the current N-able N-central software and are not guaranteed.

Active Issues

Description	Bug
When exporting a large list of Active Issues items to PDF format at either the System or Service Organization level, the server may fail. Exporting to CSV format does not cause this problem.	62860

Agents & Probes

Description	Bug
Communication issues may be encountered for N-able N-central Probes installed on Windows servers that have multiple NICs. For more information, refer to *"KBA20020: Configuring A Server With Multiple NICs"* in the online Help.	67778

Automation Manager

Description	Bug
Running Automation Manager Policies created using Automation Manager 1.6 or earlier may result in `Failed to create an EndDate ...` errors if the Policies are run on a computer using a different date format. This issue does not affect Policies created using Automation Manager 1.7 or later.	65712

AV Defender and Backup Manager – D2D

Description	Bug
Custom Settings option no longer available in 10 for backup profiles.	NSBM-709
The **About Backup Manager** dialog box no longer indicates if the Backup Manager software is licensed.	68226

Custom Services

Description	Bug
Custom services may appear as misconfigured when the system locale of the device is not set to English. For example, in Portuguese the default decimal in c#/.net is not a period, ".", it is a comma, ",". If you are having this issue, please contact N-able Technical Support.	65288

Dashboards

Description	Bug
Modifying a Dashboard that is associated with a large number of services may cause performance issues when using the Firefox browser.	70326

Core Functionality

Description	Bug
Installing N-able N-central on Servers that have an Nvidia Video Card Due to a bug in CentOS 7 with Nvidia's "Nouveau" driver, installing N-able N-central on servers that have an Nvidia video card may result in the N-able N-central console showing a blank screen, or displaying an Anaconda Installer screen with an error message about the video card driver.	NCCF-11842
HDM doesn't not work with the "Last 5 Tickets" widget.	NCCF-10855
Warranty information might be inaccurate when determining the warranty expiry dates of devices that are not located in the USA.	NCCF-3649
URL with embedded username and password prompts for Java upgrade, logging in manually does not prompt.	NCCF-2415
Chrome 42.x does not support NPAPI plugins which means that Java and Direct Connect will not function with that browser version. When attempting to open remote control connections in Chrome 42.x, users will be repeatedly prompted to install either Java or the NTRglobal plugin with no successful connections made. To resolve this issue, perform the following: 1. In the Chrome address bar, type `chrome://flags/`. 2. Under **Enable NPAPI**, click Enable. 3. Restart Chrome.	73359

PSA Integration

Description	Bug
In some instances, tickets closed in PSAs are not being cleared in N-able N-central. This is likely because the ticketing recipient profile in N-able N-central has **Do not change the Ticket Status** selected (in order to manually configure tickets). Then, when the ticket is removed in the PSA, N-able N-central will not be able to update/resolve the ticket's status and new tickets cannot be created for the same issue. Until a solution is available through the UI for this situation, the work around is to set a Return to Normal status and set a non-used status in the 'updatable statuses' section or set the same status as the return to normal one. This will cause N-able N-central to add a note to the ticket on return to normal but will not alter the ticket's status. This will allow the stale ticket check to remove the ticket from the system.	65620

UI

Description	Bug
After re-naming, the **Names** of files or Registry entries may not be displayed properly in the **File System** window and the **Registry** window of the **Tools** tab when using Internet Explorer.	68149

End of support

The following are being deprecated in a future release of N-able N-central:

Linux Agent Support	Due to declining usage in the field, the N-able N-central Linux agents will stop supporting CentOS 6, Ubuntu 14.04 and the 32-bit version of Ubuntu 16.04, in a future release.
Internet Explorer 11	Due to declining usage in the field, a future release of N-able N-central will drop support for the Internet Explorer 11 web browser.
AV Defender 5.x	As of next major release for those of you still utilizing the AV5 Bitdefender Antivirus be advised that monitoring from our AV5 agents will no longer continue. As a result this will leave your environments in a vulnerable state. We encourage you to review your agents to ensure you are now utilizing our latest AV6 agents. Reminder that our online help for Security Manager is available for your reference.
End Of Life: Arcserve Integration And Support	As we continually look to improve our offerings to you, we have decided to discontinue N-central integration and support for Arcserve products, effective March 31, 2021. This will allow us to better focus our resources on continuing to offer the highest quality products and services across the rest of our portfolio.
Azure VHD Images	With the release of N-central support for Azure Managed Disks, we have streamlined the deployment process, including removing the requirement of uploading a full sized VHD image to Azure. As a result, we plan to stop building the 100 GB, 200 GB, 500 GB and 1TB VHD images with a future release of N-central. You can migrate to the newer "Azure Managed Disk"-based N-central by deploying a new N-central server in Azure using the cross Platform PowerShell 7 deployment script (available on the Download page of the Customer Success Center), and restoring the backup of your existing server (of the same N-central version), to the new server. The existing VHD images will remain available for older versions of N-central through the Customer Success Center, in case you need to rebuild and older version of N-central, but we recommend using the newer deployment method for all new releases of N-central.
Windows 8.1/Windows Server 2012 R2	As older Windows Server and Desktop Operating Systems transition into Microsoft's Extended Support Phase and beyond,

	they are no longer receiving OS level TLS version and cipher updates (SCHANNEL). As the .NET Framework relies on SCHANNEL for TLS based communications, and as newer vulnerabilities are discovered in the ciphers available to these older Operating Systems, the available Strong Cipher list for these devices continues to shrink. We continually review the ciphers used by N-central's Modern Security Profile, to ensure we offer only secure ciphers. At this time, there are only two (2) secure RSA key based ciphers available to Windows Server 2012 R2/Windows 8.1 and older. N-central will endeavor to support these two ciphers in our Modern Security profile for as long as they remain secure, but there may come a time where we will need to drop Official support for these Windows versions before the end of their Extended Support Phase. If/when this does occur, they will still be able to connect if you switch to the Legacy Security Profile, but this will reduce the security of all devices connecting to your N-central server. If you monitor Windows Server 2003/2008/Windows XP/Vista devices, we would like to advise you that we will be dropping support for the "TLS_RSA_WITH_3DES_EDE_CBC_SHA" cipher in a future release. Coming changes to the web front end that will support TLS 1.3, have been identified as also disabling "TLS_RSA_WITH_3DES_EDE_CBC_SHA" due to the required version of OpenSSL. Fully patched Windows Server 2008/Vista devices *should* be able to connect to N-central on the Legacy Security profile, using one of the newer, but still weak ciphers. Windows Server 2003/XP will no longer be able to communicate over TLS/HTTPS at that time (using a site-to-site VPN between your firewall devices, and connecting over HTTP may still work).
32-bit versions of the Windows, Linux and macOS operating systems	The number of 32-bit Operating Systems monitored by N-central has continued to drop over the past few years. Windows Agents/Probes have historically been 32-bit, with some 64-bit specific components. In a future release, we intend to convert the Agent and Probe code base to be a native 64-bit application; this will mean a hard deprecation of support for 32-bit Windows versions. N-central's Linux and macOS agents will follow a similar path.

N-able N-central System requirements

The following requirements are for typical usage patterns, acknowledging that some patterns may require greater system resources for a N-able N-central server than others.

If you have any questions about how your needs affect the system requirements of your N-able N-central server, contact your Channel Sales Specialist or email n-able-salesgroup@n-able.com.

Processor	Server class x86_64 CPUs manufactured by Intel or AMD (i.e. Xeon or EPYC). Please refer to the Red Hat Hardware Ecosystem for further details.
Operating System	You do not need to install a separate Operating System to run N-able N-central. The N-able N-central ISO includes a modified version of CentOS 7, based on the upstream Red Hat Enterprise Linux 7.
Physical Hardware	The physical server used to install N-able N-central in a bare metal environment must be certified to run Red Hat Enterprise Linux 7.7 (x64) by Red Hat, or the hardware vendor, without any additional drivers. Please check the Red Hat Hardware Ecosystem for details. Server Grade hard drives connected to a RAID controller with a Battery/Capacitor Backed Cache are Required. Examples include 10K+ RPM SCSI or SAS drives, Enterprise Grade SSDs or NVMes for bare metal and virtualized hosts, or a Fibre Channel connected SAN with Enterprise Grade hard drives for virtualized hosts *(Fibre Channel cards can be used for bare metal if they are configured in the pre-boot environment and do NOT require vendor-provided drivers)*. Although Desktop Hard Drives will work with the Operating System, they do not meet the minimum throughput required for the back-end Database of N-able N-central.

For more details, please refer to the Red Hat Hardware Ecosystem to see if your current hardware will work with our customized version of CentOS 7.

System requirements by number of devices managed

The table below lists the minimum specifications required to manage the number of devices indicated (based on average usage). Performance can be improved by exceeding these requirements. When determining your hardware requirements, consider any growth in managed device count that may occur over time.

Number of Devices	CPU Cores	Memory	Storage
Up to 1,000	2	4 GB RAM	80 GB RAID
Up to 3,000	4	8 GB RAM	150 GB RAID
Up to 6,000	8	16 GB RAM	300 GB RAID
Up to 9,000	12	24 GB RAM	450 GB RAID
Up to 12,000	16	32 GB RAM	600 GB RAID

Number of Devices	CPU Cores	Memory	Storage
Up to 16,000	22	48 GB RAM	800 GB RAID
Up to 20,000	28	64 GB RAM	1 TB RAID
Up to 24,000	34	80 GB RAM	1.2 TB RAID

Notes

1. Server Grade hard drives connected to a RAID controller with a Battery/Capacitor Backed Cache, are **required** to ensure performance and unexpected power-loss data protection.
2. In a virtualized environment, hard drives for the N-able N-central server must not be shared with any other applications or VM guests that have significant I/O workloads. For example, Report Manager, SQL Databases, E-Mail Servers, Active Directory Domain Controllers, SharePoint, or similar should not be installed on the same physical hard drive as N-able N-central.
3. N-able recommends two or more hard drives be placed in a redundant RAID configuration. With two drives, RAID 1 must be used. With more than two drives, RAID 1+0 or RAID 5 are recommended. RAID 6 is an option on servers with less than 1,000 devices (the additional write latency of RAID 6 becomes an issue above 1,000 devices).
4. N-able recommends more, smaller disks in a RAID array, as opposed to fewer larger disks. Database-backed applications, like N-able N-central, have better write performance with an increased number of parallel writes (hard drives).
5. If using Solid State Drives (SSDs), N-able requires Enterprise Grade, SLC based (or better) SSDs with a SAS interface, or Enterprise Grade NVMes. SSD and NVMe drives must have an endurance rating of at least 0.2 DWPD (Drive Writes Per Day), and at least 2 physical disks in a redundant RAID array. On Bare Metal servers, the RAID array must appear to the operating system as a single Block or NVMe Device. Currently, many PCIe and NVMe drives do not meet this last requirement and would only work in a virtualized environment.
6. Configure the RAID controller to use the default stripe size and a Read/Write cache of 50%/50%.

The underlying customized version of CentOS 7 has certain hardware limits that are consistent with the upstream Red Hat Enterprise Linux 7 distribution. Of note are the following:

Subsystem	Limit
Minimum disk space	80GB
Maximum physical disk size (BIOS)	2TB
Maximum physical disk size (UEFI)	50TB
Required minimum memory	4GB for 4 or fewer logical CPUs
	1GB per logical CPU for more than 4 logical CPUs

Subsystem	Limit
Maximum memory	12TB
Maximum logical CPUs	768

Examples of supported servers

Due to the ecosystem of different hardware, N-able does not certify specific hardware configurations. Instead we rely on the upstream Red Hat Enterprise Linux and hardware vendor testing and certification.

Examples of servers that have been Red Hat certified include HPE ProLiant DL360 Gen10 and Dell PowerEdge R620.

Please consult with your hardware vendor to ensure that any server to be used for a bare metal installation meets the above requirements, and is Red Hat Enterprise Linux 7.7 certified, without the need for additional drivers.

N-able recommends that for any Bare Metal server, two or more SAS 10k or faster hard drives be placed in a RAID array to improve redundancy. RAID 1+0 or RAID 5 are supported (at the hardware RAID BIOS level). RAID 6 is an option on servers with less than 1,000 devices (the additional write latency of RAID 6 becomes an issue above 1,000 devices).

Support for virtualized environments

N-able supports VMware ESX Server 6.0 or newer and Windows Server 2012 R2 Hyper-V or newer LTS versions. N-able recommends use of the latest stable versions of VMware or Hyper-V in order to ensure the best performance, feature set and compatibility with N-able N-central.

Hyper-V on Windows Desktop Operating Systems not Supported.

N-able N-central installed on a virtual machine running on a Desktop Operating System (such as Hyper-V on Windows 10, Virtual Box, Parallels, VMWare Fusion or similar) is not a supported configuration. If you are using Windows Hyper-V, it must be installed on a supported server class Windows Operating System.

Windows Server Semi-Annual Releases are not Supported.

Only Long-Term Support (LTS) versions of the Windows Server Operating System are supported as a Hyper-V host for N-able N-central. Microsoft currently releases "Semi-Annual Release" versions of Windows Server as a technology preview for the next LTS version. Due to their technology preview status, these "Semi-Annual Release" versions of Windows Server are not supported as Hyper-V hosts for N-able N-central.

About virtualization

Virtualization provides an abstraction layer between the hardware and the Operating System which permits the operation of multiple logical systems on one physical server unit. The table below includes considerations when using this deployment method.

System Performance	It is impossible to guarantee the scalability or performance of a N-able N-central server deployed on a Virtual Machine due to: ■ variability in field environments resulting from host server configurations, ■ the number of virtual guests run on the host server, and ■ the performance of the underlying host hardware.
Supportability	N-able supports N-able N-central software deployed on VMWare ESX/ESXi 6.0 or newer, Windows Server 2012 R2 Hyper-V or newer LTS releases, Microsoft Azure and Amazon AWS EC2 in the same way that we support N-able N-central deployed on Bare Metal. This support is limited to the components (Software and Operating System) shipped with N-able N-central and does not include the troubleshooting of virtualization systems nor of performance issues related to environmental factors. N-able recommends reaching out to your hardware or virtualization vendor for support on the underlying virtualization and hardware components. Any assistance provided by N-able Support for virtualization or hardware issues is on a best-effort basis only. In the event of serious performance problems, we might ask you to migrate a virtualized N-able N-central system to a physical hardware deployment.

Virtual Hardware Support	In Windows Server 2016 Hyper-V or newer deployments, it is recommended to create a new Generation 2 VM. When configuring the VM virtual hardware, if you choose to enable **Secure Boot**, please select the **Microsoft UEFI Certificate Authority** template. For VMWare ESX/ESXi deployments, it is recommended to select the **Red Hat Enterprise Linux 7** guest OS template, then under the **Boot Options**, select the **UEFI Firmware**.
Network Adapters	N-able recommends using the VMXNET3 network card in VMWare. When the VM is configured as Red Hat Enterprise Linux 7, it will use VMXNET3 by default. Unless you are using Network Interface Bonding, N-able N-central requires only one (1) network adapter added to the VM configuration. Multiple network adapters that are not used in a bonding configuration can cause connectivity and licensing issues.
MAC Addresses	By default, most virtualization environments use a dynamically assigned MAC address for each virtual network card. As your N-able N-central license is generated in part by using the MAC address of its network card, it is required to use a statically assigned MAC address in order to avoid becoming de-licensed.

Recommended configuration for the virtualized server

Although provisioning virtual disks as "thin" or "thick" results in nearly-identical performance, thick provisioning is recommended, particularly when more than 1,000 devices will be connected to your N-able N-central server.

- Assign the highest resource access priority to N-able N-central, as compared to other guest VMs.
- Do not over-provision resources (Memory, CPU, Disk) on the virtualization host. Over-provisioning these resources can causes memory swapping to disk, and other bottlenecks that can impact guest system performance.
- Ensure that the system has enough RAM and hard drive space to provide permanently allocated resources to the N-able N-central guest.

Supported Software

Browsers

N-able N-central supports the latest versions of:

- Internet Explorer®
- Microsoft Edge®
- Mozilla Firefox®
- Desktop versions Google Chrome®. Mobile phone browsers are not supported.

N-able N-central is not supported on Internet Explorer in Compatibility View mode.

Remote Control

Remote control connections require the following software on the computers that initiate connections:

- .NET Framework 4.5.2 on Windows devices
- Oracle Java 1.8 versions that include Java Web Start

Report Manager

To use Report Manager with N-able N-central, ensure the you upgrade to the latest version of Report Manager.

Automation Manager

Automation Manager requires .NET Framework 4.5.2 and PowerShell 3.0 to run AMP-based services with N-able N-central.

SNMP Community String

On HPE ProLiant Generation 9 or older Physical Servers, when monitoring the N-able N-central server using SNMP, the community string used for SNMP queries to the server must use `N-central_SNMP`, not `public`. SNMP is only enabled on HPE ProLiant Generation 9 or older Physical Servers. All other installs do not enable SNMP on the N-able N-central server.

Supported Operating Systems

This section describes the supported operating systems for N-able N-central.

Windows Agents:

- Microsoft .NET Framework 4.5.2 (or later)

Windows Server 2019

- Windows Server 2019 Datacenter
- Windows Server 2019 Standard

Windows Server 2016

- Windows Server 2016 Datacenter
- Windows Server 2016 Standard
- Windows Server 2016 Essentials
- Windows Storage Server 2016
- Windows Server 2016 MultiPoint Premium Server
- Microsoft Hyper-V Server 2016

Windows Server 2012

- R2 Datacenter
- R2 Essentials

- R2 Foundation
- R2 Standard
- Datacenter 64-bit Edition
- Essentials 64-bit Edition
- Foundation 64-bit Edition
- Standard 64-bit Edition
- Microsoft Hyper-V Server 2012
- Microsoft Hyper-V Server 2012 R2
- Storage Server 2012 Enterprise 64-bit Edition
- Storage Server 2012 Express 64-bit Edition
- Storage Server 2012 Standard 64-bit Edition
- Storage Server 2012 Workgroup 64-bit Edition

Windows 10

- Microsoft Windows 10 Enterprise & Professional
- Microsoft Windows 10 Education editions
- Windows 10 Pro for Workstations

Windows 8 and 8.1

- 8.1 Enterprise
- 8.1 Professional
- 8 Enterprise
- 8 Professional

Windows 7

- Microsoft Windows 7 Enterprise & Professional
- Microsoft Windows 7 Ultimate

Mac Agents

- 11.0 (Big Sur)
- 10.15 (Catalina)
- 10.14 (Mojave)
- 10.13 (High Sierra)
- 10.12 (Sierra)

Linux Agents

Independent Agents are required for 32-bit and 64-bit Linux OS installations.

The probe performs an SSH connection a Linux device. To discover a Ubuntu/Debian OS device, the device must have openssh installed.

- Red Hat Enterprise Linux/CentOS 8 (64-bit)
- Red Hat Enterprise Linux/CentOS 7 (x86_64 and i686)
- Red Hat Enterprise Linux/CentOS 6 (x86_64 and i686)
- Ubuntu 18.04 "Bionic Beaver" (x86_64)
- Ubuntu 16.04 "Xenial Xerus" (x86_64 and i686)
- Debian 8.7/Ubuntu 14.04 "Trusty Tahr" (x86_64 and i686)

AV Defender

Workstation Operating Systems

- Microsoft Windows 8, 8.1
- Microsoft Windows 10

Tablet And Embedded Operating Systems

- Windows Embedded Standard 2009
- Windows Embedded POSReady 2009
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 7
- Windows Embedded Standard 7

Server Operating Systems

- Microsoft Windows 2012 Server
- Microsoft Windows 2012 Server R2
- Microsoft Windows 2016 Server
- Microsoft Windows 2019 Server

For Microsoft Windows Embedded Standard 7, TCP/IP, Filter Manager, and Windows Installer must all be enabled.

Patch Manager

Workstation Operating Systems

- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10 version 1607 and later

Server Operating Systems

- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

The following operating systems are not supported with N-able N-central patch manager:

- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 10 Home Edition
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

Windows Update Agent

The minimum version of the Windows Update Agent (WUA) needs to be greater than 7.6.7600.320. The base NT build version of Windows should be 6.1 or later. Older versions of the base NT build cannot upgrade past version 7.6.7600.256 of the Windows Update Agent.

Automation Manager

Workstation Operating Systems

- Microsoft Windows 7 (32/64-bit)
- Microsoft Windows 8 (32/64-bit)
- Microsoft Windows 8.1 (32/64-bit)
- Microsoft Windows 10 (32/64-bit)

Server Operating Systems

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016 (32/64-bit)
- Microsoft Windows Server 2012 R2 (32/64-bit)
- Microsoft Windows Server 2012 (32/64-bit)

Disk Encryption Manager

Hyper-V Server 2012 R2	Hyper-V Server 2016
Windows 7 Enterprise	Windows 7 Home Premium
Windows 7 Professional	Windows 7 Ultimate

Windows 8 Enterprise	Windows 8 Pro
Windows 8 Pro with Media Center	Windows 8.1 Enterprise
Windows 8.1 Pro	Windows 8.1 Pro with Media Center
Windows 10 Education	Windows 10 Enterprise
Windows 10 Enterprise 2015 LTSB	Windows 10 Enterprise 2016 LTSB
Windows 10 Enterprise for Virtual Desktops	Windows 10 Enterprise LTSC 2019
Windows 10 Pro	Windows 10 Pro Education
Windows 10 Pro for Workstations	
Windows Server 2008 R2 Enterprise	Windows Server 2008 R2 Datacenter
Windows Server 2008 R2 Standard	Windows Server 2008 R2 Foundation
Windows Server 2012 Datacenter	Windows Server 2012 Essentials
Windows Server 2012 Foundation	Windows Server 2012 R2 Datacenter
Windows Server 2012 R2 Essentials	Windows Server 2012 R2 Foundation
Windows Server 2012 R2 Standard	Windows Server 2012 R2 Standard Evaluation
Windows Server 2012 Standard	
Windows Server 2016 Datacenter	Windows Server 2016 Datacenter Evaluation
Windows Server 2016 Essentials	Windows Server 2016 Standard
Windows Server 2016 Standard Evaluation	
Windows Server 2019 Datacenter	Windows Server 2019 Essentials
Windows Server 2019 Standard	Windows Server 2019 Standard Evaluation
Windows Server Datacenter	

Windows Small Business Server 2011 Essentials	Windows Small Business Server 2011 Standard

Port access requirements

N-central Server

Access must be permitted to the following ports:

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
20		√			Used for FTP connections, particularly when configured for backups.
21		√			Used for FTP connections, particularly when configured for backups.
22	√			√	SSH - used for remote control sessions. The firewall must be configured to allow access from the Internet to this port on the N-able N-central server.
25		√			SMTP - used for sending mail.
53		√			Used for DNS.
80	√	√		√	HTTP - used for communication between the N-able N-central UI and agents or probes (including MSP Connect and MSP Anywhere). The firewall must be configured to allow access from the Internet to this port on the N-able N-central server. This port must also be open for outbound traffic if the N-able N-central server is monitoring the HTTP service on a managed device.
	Inbound access to port 80 on the N-able N-central server can be blocked provided that all Agents are configured to use HTTPS and the N-able N-central server is accessed over port 443 using HTTPS.				
123		√			Used by the NTP Date service which keeps the server clock synchronized. Normally using UDP (although some servers can use TCP).

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
135			√		Used by Agents and Probes for WMI queries to monitor various services. Inbound from the Windows Probe to the Windows Agent.
139			√		Used by Agents and Probes for WMI queries to monitor various services. Inbound from the Windows Probe to the Windows Agent.
443	√	√		√	HTTPS - used for communication between the N-able N-central UI and Agents or Probes (including MSP Connect and MSP Anywhere). Port 443 is the TCP port needed for SSL (HTTPS) connections. The firewall must be configured to allow access from the Internet to this port on the N-able N-central server. This port must also be open for outbound traffic if the N-able N-central server is monitoring the HTTPS service on a managed device. Backup Manager relies on Port 443 TCP outbound. It is almost always open on workstations but may be closed on servers. This port must be open for outbound traffic on the N-able N-central server. Used by Agents and Probes for XMPP traffic. Outbound access to port 443 for Managed Devices is recommended but not required. To activate EDR the N-able N-central server needs outbound HTTPS access to port 443 and the following domains: ■ *.sentinelone.net ■ sis.n-able.com ■ keybox.solarwindsmsp.com

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
445			√		Used by Agents and Probes for WMI queries to monitor various services.
1234		√		√	Used by MSP Connect in UDP mode.
1235		√		√	
1433		*	*	*	Outbound on the N-able N-central server, port 1433 is used by Report Manager for data export. On managed devices, it is also used by Agents (inbound) and Probes (out- bound) to monitor Backup Exec jobs. Inbound from the local LAN and not the Internet.
	* Port access is only required if you have installed the corresponding product. For example, access to port 1433 is only required if you have installed Report Manager or if you are managing Backup Exec jobs.				
5000		√			Backup Manager will use local port 5000. If this port is unavailable, Backup Manager will detect a free port automatically (starting from 5001, 5002 and up).
8014			√		Backup Manager requires access to port 8014. This value cannot be modified. Inbound from the local LAN and not the Internet.
8800		√			The Feature Flag System in N-able N-central needs to talk to mtls.api.featureflags.prd.sharedsvcs.system-monitor.com. Used by N-able – generally during Early Access Preview and Release Candidate testing – to enable and disable features within N-able N-central.

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
10000	√				HTTPS - used for access to the N-able N-central Administration Console (NAC). The firewall must be configured to allow access from the Internet to this port on the N-able N-central server. N-able recommends excluding all other inbound traffic to port 10000 except from N-able Ports for Support section below.
10004			√	√	N-able N-central Agents must be able to communicate with a Probe on the network over port 10004 in order for Probe caching of software updates to function properly. Inbound from the local LAN and not the Internet.
15000			√	√	For downloading software patches, port 15000 must be accessible for inbound traffic on the Probe device while it must be accessible for outbound traffic on devices with Agents. Inbound from the local LAN and not the Internet.

Supported operating systems for remote control

The availability of remote control connections will vary depending on the operating systems of both the client and target devices. The table below outlines the operating systems and their compatibility with various remote control types.

Remote Control Type	Windows		Linux		Mac OS X	
	Remote System	Technician	Remote System	Technician	Remote System	Technician
Custom	✓	✓	✓	✓	✓	✓
Take Control	✓	✓	✗	✗	✓	✓
Remote Desktop	✓	✓	×	×	×	✓
SSH	✓	✓	✓	✓	✓	✓
TeamViewer	✓	✓	×	×	✓	✓
Telnet	✓	✓	✓	✓	✓	✓
Web	✓	✓	✓	✓	✓	✓

Licensing and Customer Support

Agent/Probe Installation Software

N-able N-central 2021.1 HF3 uses the 7-Zip file archiver for installing agents and probes. 7-Zip is free software redistributed under the terms of the GNU Lesser General Public License as published by the Free Software Foundation. For more information, see http://www.7-zip.org.

Customer Support

Contact N-able to activate your N-able N-central server.

Web Page:	http://www.n-able.com
Technical Support Self-Service Portal:	https://success.n-able.com/
Phone:	Toll Free (U.S./CAN): 1-866-302-4689
	International: +800-6225-3000
	Local: (613) 592-6676, select option 2 for support

About N-able

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale. For more information, visit www.n-able.com.