N-ABLE™

N-central

Release Notes

Version: 2023.9 (Build: 2023.9.0.26)

Last Updated: Friday, December 22, 2023

What's New in N-able N-central 2023.9

REST APIs

This release contains our very first set of REST APIs. These new APIs enable partner systems to programmatically interface with N-central to execute common N-central tasks. For this first release, Partners and Vendor integrators alike will be able to develop services to utilize the new 'Scheduled Tasks' API to run scripts against target devices and pass variables to those scripts. This first iteration will run tasks immediately, with more features to come in a future release. This release also includes a handful of REST APIs with GET methods for device and customer related information.

N-able Admin Console moved!

N-able Admin Console is now GA with 2023.9. If you have not been previewing this important security enhancement already, when you upgrade to 2023.9, you'll be able to turn off port 10000 to outside access. The items that were previously in the port 10000 interface can now be found at the System level of N-central, under the System Settings menu, and Administration > Defaults. This also means that on-premise servers can enable MFA on the productadmin account! For more information on this feature, please refer to The N-able N-central Administrator Console overview.

Automation Manager

Automation Manager 2.93 is released alongside N-central 2023.9. This version of Automation Manager has added a new set of Meraki objects that use the v1 API. The previous objects are still available for compatibility, but if you have created custom AMPs around the first iteration, you should update those AMPs to use the new objects. We anticipate having the Services for Meraki from the Automation Cookbook updated in the near future. For a detailed list of fixes, please refer to the fixed issues list later in this document.

New Customer Name Limitations

As of N-central 2023.9, new Service Organization, Customer and Site levels may no longer start with the following characters: =,-,+, or @. Additionally, the names may not contain the following characters: % & $ # < > ; " / \

If you already have these characters in existing level names, they will not be modified by the upgrade. However, to edit those level names in the future, they will need to adhere to the same rules as newly created ones. If you have rules existing based on these levels, and the names do not meet the new criteria, you may see a system error attempting to edit those customers. If so, rename the related rules first, then rename the customer level.

Cove-related Enhancements

With 2023.9, N-central continues to enhance capabilities around Cove Data Protection! In addition to the previously released new left hand menu item, and the deployment AMPs, 2023.9 adds a new icon in the Features column of the All Devices view to show you Windows devices where Cove is installed on the device. There's also a new Cove App Monitoring service that will be automatically added to the Windows device.

Ecosystem Agent Changes

Ecosystem agent will no longer get installed on devices and will only be installed on devices where Intune and/or DNSF integrations have been enabled on that device. If all integrations have been disabled on a device, the Ecosystem agent will automatically be uninstalled.

Key Bug Fixes

NCCF-56348 - Correct agent version not reflecting in N-central UI.

NCCF-101768 - Custom IDP providers can now be configured with OKTA.

KUIP-5591 - Fixed an issue where the Title Header does not update to 'Integration Management' when that is the selected view for the user and displays the previous screen title.

KUIP-5397 - Fixed an issue where clicking the Activate button from the Integration Management page did not update the activated state, without logging in and out and clicking Activate again.

KUIP-4449 - Fixed an issue where EDR and DNSF were not getting uninstalled automatically upon trial/contract expiration.

KUIP-3155 - Fixed some noisy logs around ecosystem-agent-updated-configurations that may affect performance for larger partners.

Upgrade paths and notes

Upgrade versions

To upgrade to N-able N-central 2023.9, your N-able N-central server must be running the following version:

- N-able N-central 2022.7.1.44
- N-able N-central 2023.4.0.32
- N-able N-central 2023.5.0.12
- N-able N-central 2023.6.0.9
- N-able N-central 2023.7.0.10+
- N-able N-central 2023.8.0.11+

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

> ℹ️ 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.

Available Ciphers for Non Agent/Probe Communication with N-central

N-central updated its cipher list in the 2022.5 release and removed support for older ciphers.

The change primarily affects third-party applications running on Windows Server 2012 R2 and earlier operating systems as the host operating system no longer meet the cipher requirements for communicating with N-central 2022.5 and later.

Affected on-premise applications include:

- Report Manager
- Helpdesk Manager
- ConnectWise (on Premise)
- Custom PSA Solutions
- SQL Servers configured using Data Export and LDAP or Active Directory (those running an ECDSA certificate may function normally)

The cipher change does not generally affect third-party applications running on Windows 2016 and later where the host operating system supports the below cyphers.

For further information, please refer to the article: N-central is unable to communicate with third-party applications hosted on windows servers 2012 R2 and older after the upgrade to N-central 2022.5

TLSv1.3:

- TLS_AKE_WITH_AES_128_GCM_SHA256
- TLS_AKE_WITH_AES_256_GCM_SHA384

TLS 1.2:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Included updates in N-able N-central

Release 2023.9 GA

> ℹ️ Please note that because of the PostgreSQL upgrade included with N-central 2023.9, on-premise partners can expect this upgrade to take longer than previous upgrades may have. Please do NOT reboot your N-central server if the upgrade appears to be stuck. Please check the server console for error messages, or contact Support and they can advise on the progress and status of the upgrade.

Category	Description	Item
Analytics	Info icon for "Recipients" field on scheduler modal dialog window	DV-5359
Analytics	Missing Mouse-Over tooltip for Schedulers Subject field in Manage scheduler list screen	DV-5355
Analytics	Export buttons(ppt/pdf) should be disabled immediately after export is requested	DV-5354
Analytics	Wrong naming definition	DV-5224
Automation Manager	AM registry record is not updated	AM-3740
Automation Manager	AM Object: DVD Get DVD Drive Information	AM-2514
Automation Manager	Check if downloaded DLLs version matches expected version obtained from metadata	AM-2618
Automation Manager	"Stop Process" object runs until timeout when run as different user than owner of process	AM-2743
Automation Manager	Reboot Prompt object runs multiple times causing duplication of alerts	AM-2780
Automation Manager	AM "Get Last Boot Time" object doesn't handle well exception	AM-3421
Automation Manager	AM object - GetRegistryKeys output property PathNoRoot contains the root for HKCU registers	AM-3465
Automation Manager	201 Cannot convert value "rror: 0x800705B" to type "System.Double". Error: "Input string was not in a correct format."	AM-3561
Automation Manager	RemoveUserFromLocalGroup object does not compose username correctly	AM-3763
Automation Manager	GetDate object formats output incorrectly	AM-3766
Automation Manager	Send Mail object keeps attachments locked	AM-3822
Automation Manager	EnableWirelessAdapters	AM-3851
Automation Manager	Get Windows Events - Designer execution error until object is seen under the Policy Builder	AM-3852

Automation Manager	ScriptRunner installation breaks - doesn't comply with custom path from installation parameters	AM-3866
Automation Manager	Possible Security issue with Automation Manager Service	AM-3906
Automation Manager	NC - AM creates app domain with unsigned assemblies	AM-3911
Core	Fixed errors introduced via newly added customer name restrictions	NCCF-174998
Core	N-central 2023.9 contains an upgrade to the Apache Struts version to v2.5.33	NCCF-170867
Core	Not able to create SOs manually on N-central server build	NCCF-165357
Core	Analytics:Users Can Export A Report & Users Can Export A Report After Downloading - Keyword 'Element Should Be Visible' failed after retrying for 2 minutes. The last error was: Element with locator '//span[contains(text (),'Patch Missing')]' not found.	NCCF-158477
Core	Error cleaning up /tmp/migration directory	NCCF-158456
Core	Failed eventing startup can result in a null pinter exception in MspRelayPublisher that never gets cleared and blocks eventing forever.	NCCF-152628
Core	Adjust cli migration parameters template to match current cli app parameters	NCCF-150297
Core	Linux agent installation script does not exit properly	NCCF-147130
Core	Add a new column to the "Script/Software Repository" table that allows making a script runnable by REST APIs	NCCF-145883
Core	Add the ability to determine which scripts can be invoked from REST APIs	NCCF-145880
Core	N-central: add a new UI status for failed URLs pre-checks	NCCF-143691
Core	[Disaster Recovery] Rerun the migrate command when NC fails during a migration	NCCF-141917
Core	Create new Cove filter to get devices with Cove Backup Manager installed	NCCF-139882
Core	Link monitoring status with Cove device backup status	NCCF-139610
Core	Agent Module to support Cove App Monitoring service	NCCF-139609
Core	Automatically assign/remove Cove services based on asset discovery	NCCF-139608
Core	Create new service for "Cove App Monitoring" pro-	NCCF-139607

Core	duction status	
Core	N-Central should not be monitoring integrations if none are turned on	NCCF-137409
Core	DMA:Commands from Device View don't work	NCCF-137255
Core	Patch Status title is missing on the report	NCCF-134769
Core	Windows OS Version not showing correctly	NCCF-134250
Core	Password Reset Successful Change Email Shows IP Instead of FQDN	NCCF-131240
Core	Windows Agent: ComponentStatusUpdate should be called only after installation status was changed	NCCF-130229
Core	Change the Cove Icon and report on Cove status	NCCF-130209
Core	Verify Windows Log Event Has Single Backslash	NCCF-127838
Core	Issue with EDR status on Ncentral UI when S1 Uninstallation triggered from EDR Tab.	NCCF-127371
Core	Upgrade 2023.4,2023.5,2023.6 to 2023.7 on Probe/Agent device is showing duplicate windows agent on USeNewUpdate=False	NCCF-120402
Core	Copy of Device Name has preceding white space	NCCF-109980
Core	VSS Script Service for EDR (Not API Data Driven)	NCCF-109180
Core	Okta Support for Custom (OpenID Connect) SSO Provider	NCCF-101768
Core	Cove Icon for Enabled "Features"	NCCF-100243
Core	Custom Device Property "Password" Should Save at Device Level	NCCF-101757
Core	Modify how agent checks for Take Control being functional	NCCF-92486
Core	LDAP Login Adding Extra Backslash Just to UI Display	NCCF-91561
Core	Move MSP Backup / BUi to its own Backup menu in the left nav	NCCF-58745
Core	Correct agent version not reflecting in N-central UI	NCCF-56348
Core	N-central needs to limit the amount of Soap data from agents scheduled tasks output	NCCF-16873
Core	"My Links" update to fix the Default Links and point to correct URLs	NCCF-16813
Core	Add Usage Example for {{Device Property}} in Notification Templates	NCCF-15112

Ecosystem Framework	"Integration Management" Title Header missing in UI view	KUIP-5591
Ecosystem Framework	Failed Devices List - UI	KUIP-5492
Ecosystem Framework	Add New Hidden Registry Key to Point to New Agent Path (v5)	KUIP-5482
Ecosystem Framework	DMS: REST endpoint to return the current status of the migration for ON-PREM migrations	KUIP-5435
Ecosystem Framework	DMS: REST endpoint to run migration script on ON-PREM servers	KUIP-5434
Ecosystem Framework	Remove Reinstall of Ecosystem Agent from N-central Agent	KUIP-5424
Ecosystem Framework	Automatic Install of Ecosystem Agent - Upgrades	KUIP-5404
Ecosystem Framework	Automatic Install of Ecosystem Agent- New N-Central Installs	KUIP-5403
Ecosystem Framework	Remove Ecosystem Agent if all integrations are disabled	KUIP-5402
Ecosystem Framework	Remove automatic install of Ecosystem Agent	KUIP-5401
Ecosystem Framework	NC agent to uninstall Eco agent based on device UUID (not Publisher)	KUIP-4263
Integrated AV	Syntax issue in N-Central UI when no threats were found	IAV-1924

Known Issues

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.

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:ConfiguringAServer WithMultipleNICs"in the online Help.	67778
If you have multiple registry entries for older versions of the Windows agent, one entry will be cleaned up upon upgrade of the agent to 2023.9. If others remain, they will be cleaned up upon agent upgrade to a future version of N-central.	NCCF-163178

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

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

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
If you have the need to use Conditional Access Policies for your Azure AD/Entra ID linked users, there is a known issue that prevents your users from logging in. We have identified a workaround	NCCF-31030

by using Custom (OpenID Connect) instead. To learn more, click HERE.	
HDM does not work with the "Last 5 Tickets" widget.	NCCF-10855

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

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
When Cove Data Protection is installed on a device, the device details view will not light up the Cove icon in the features row correctly.	NCCF-162108
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

User Access Management

Description	Bug
Login window reappears when new tab is loaded. When already logged into N-central and a user opens a new tab and browses to N-central from this new tab, the login screen reappears yet the user is already logged in. The left hand navigation is functional.	NCCF-29648

End of support

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

Transport Layer Security (TLS)	N-able N-central now disallows traffic over TLS 1.0 and TLS 1.1. This causes any Windows Agents or Windows Probes that are running on Windows XP and Windows Server 2003, as well as pre-v12.1 versions of the MacOS agent, to lose the ability to communicate with your N-able N-central server. We strongly recommend using a Windows Probe to monitor those devices.
Linux Agent Support	Due to declining usage in the field, N-able N-central Linux agents no longer support CentOS 6, Ubuntu 14.04, and the 32-bit version of Ubuntu 16.04.
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.

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 7.9 (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.

> ℹ These requirements are only for on-premise deployments of N-able N-central.

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
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
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 7.9 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 is not Supported.**
>
> N-able N-central installed on a virtual machine running on a Desktop Operating System (such as Hyper-V on Windows 10/11, 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 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 2016 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 cause 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 desktop versions of:

- Microsoft Edge®
- Mozilla Firefox®
- Google Chrome®
- Apple Safari®
- Mobile phone browsers are not supported.

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 that you upgrade to the latest version of Report Manager.

Automation Manager

- .NET Framework 4.6
- PowerShell version 5.x is the minimum PowerShell version required to run automation manager:
  - PowerShell 5.x is backwards compatible with previous versions of PowerShell
  - You can run both PowerShell 5.x and 7.x on your endpoints, however Automation manager objects will depend on PowerShell 5.x and its backwards compatibility with previous versions.
  - Currently to-date, we do not have any objects that call PowerShell version 7.x

Microsoft Azure - Managed Disks

To deploy N-able N-central to Azure with Managed Disks using the deployment script, you require PowerShell 7.x. See Deployment script for Microsoft Azure - Managed Disks for details.

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 2022

- Windows Server 2022 Standard
- Windows Server 2022 Datacenter
- Windows Server 2022 Datacenter: Azure

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

Windows 11

- Microsoft Windows 11 Enterprise & Professional
- Microsoft Windows 11 Education editions
- Microsoft Windows 11 Pro for Workstations

Windows 10

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

macOS Agents

- 14.x (Sonoma)
- 13.x (Ventura)
- 12.x (Monterey)
- 11.x (Big Sur)
- 10.15 (Catalina)
- 10.14 (Mojave)

Linux Agents

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

> 💡 The probe performs an SSH connection to a Linux device. To discover a Linux OS device, the device must have openssh installed.

- Red Hat Enterprise Linux/CentOS 8 (64-bit)
- Red Hat Enterprise Linux/CentOS 7 (64-bit)
- Ubuntu 22.04 LTS (64-bit)
- Ubuntu 20.04 LTS (64-bit)
- Debian 11 (64-bit)

AV Defender

Workstation Operating Systems

- Microsoft Windows 11
- Microsoft Windows 10 Enterprise
- Microsoft Windows 10 Pro

Tablet And Embedded Operating Systems

- Windows 10 IoT Enterprise
- Windows Embedded 8.1 Industry
- Windows Embedded 8 Standard
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 7
- Windows Embedded Standard 7
- Windows Embedded Compact 7

Server Operating Systems

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019 (Core Mode)
- Microsoft Windows Server 2019
- Microsoft Windows Server Standard 2016 (Core Mode)
- Microsoft Windows Server 2016

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

Patch Manager

Workstation Operating Systems

- Microsoft Windows 11
- Microsoft Windows 10 version 1607 and later

Server Operating Systems

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012

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

- Home Editions of Windows Desktop Operating Systems

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 11
- Microsoft Windows 10 (32/64-bit)

Server Operating Systems

- Microsoft Windows Server 2022
- 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

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		macOS	
	Remote System	Technician	Remote System	Technician	Remote System	Technician
Custom	✓	✓	✓	✓	✓	✓
Take Control	✓	✓	✗	✗	✓	✓
Remote Desktop	✓	✓	✗	✗	✗	✓
SSH	✓	✓	✓	✓	✓	✓
Telnet	✓	✓	✓	✓	✓	✓
Web	✓	✓	✓	✓	✓	✓

Internal notes: Reviewed by Sabrin - Dec 2023

Licensing and Customer Support

Agent/Probe Installation Software

N-able N-central 2023.9 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://me.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.