



N-central

Release Notes

Version: 2023.4 (Build: 2023.4.0.30)

Last Updated: Monday, June 12, 2023



What's New in N-able N-central 2023.4

IMPORTANT - Security Improvements

- Before upgrading to 2023.4, we strongly recommend reviewing the following KB article to help prepare you for this upgrade. [Checklist for upgrading your N-able N-central Server to 2023.4](#)

N-central 2023.4 provides a major security enhancement which requires additional attention to your N-central network and client environments. Now, the N-central server will require a valid SSL/TLS certificate to be applied. This will include any certificate where the whole chain is validated to a root CA within the system trust store. To support these changes, there are updates to a few screens in the UI, such as the Network Setup page, as well as the Generate and Download certificate page. We also have modified the upgrade process so that if you don't have a valid certificate in place before attempting this upgrade, you will receive an error message before any database changes are made. As a result, you can try the upgrade again without needing Support to remove a flag.

- If you are a hosted partner, please note that N-able manages the SSL/TLS certificate for your hosted server and no action is required to modify your certificate.

Agent and probe behavior is also part of the security enhancement in N-central 2023.4. Agents and probes will not attempt to upgrade to 2023.4 and beyond unless the operating system of that device recognizes N-central's certificate as valid. We are also adding the FQDN from the Network Setup page to the top of the Server Address list on the Communication Settings page. This list is still fully editable for individual devices and in the defaults if you desire to make changes afterward.

For new installations of N-central 2023.4, you will need to provide the FQDN for this N-central server on the initial login wizard page.

Navigation Improvements

We've included a change to how the left navigation menu functions to continue to load if N-central is having trouble receiving N-able infrastructure traffic on port 443.

Automation Manager 2.80

Automation Manager 2.80 is included with N-central 2023.4. This version focuses on supporting the security changes in this release of N-central. We've also included fixes for a few existing objects and added a new Search Windows Events object.

Patch Management Updates

We've added logic to the N-central agent to prioritize the installation of the Windows Feature Upgrade via Enablement package before the larger Feature Upgrade ISO installer, when both versions are approved for install. This is to ensure the best possible experience and minimal end user impact. We also fixed an issue where installed patches were showing as pending install in N-central.

Upgrade paths and notes

- We are aware that many partners may have problems with their probes upgrading to 2023.1 and newer from versions 2022.6 thru 2022.8. Before upgrading N-central to 2023.1 or newer, please download and review the instructions in the following zip file: [Probe Upgrade Instructions](#).

Upgrade versions

To upgrade to N-able N-central 2023.4, your N-able N-central server must be running one of the following versions:

- N-able N-central 2022.6.0.20+
- N-able N-central 2022.7.0.22+
- N-able N-central 2022.8.0.14+
- N-able N-central 2023.1.0.12+
- N-able N-central 2023.2.0.13+
- N-able N-central 2023.3.0.19+

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

- 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 2023.4 RC3

Category	Description	Item
Core	Upgrade Certificate Check Hanging Upgrade When OCSP/CRL/Certificate Download URL is Resolvable, but Outbound 'http' Traffic is Blocked	NCCF-100107
Core	Agent fails to upgrade using HTTP on certificate check	NCCF-94172

Release 2023.4 RC2

Category	Description	Item
Core	Agent upgrades not being blocked when invalid server address is detected	NCCF-98511

Release 2023.4 RC

Category	Description	Item
Automation Manager	Create new object Search Windows Events	AM-2926
Automation Manager	Could not load file or assembly Newtonsoft.Json	AM-3057
Automation Manager	AM Engine upgrade: add verification for the number of files in Engine folder	AM-3064
Automation Manager	Get OS Architecture appears as failed when run from designer as standard user	AM-3074
Automation Manager	AM crashes when deleting Start Date/End Date from Get Windows Event	AM-3086
Automation Manager	Automation Manager: Is Application Installed Object wildcard not working as expected.	AM-3093
Automation Manager	AutomationManager.ScriptRunner process not killed after service timeout in N-central	AM-3095
Automation Manager	Consider levels 0 and 4 to Event Type/Level: Information on Get Windows Events object	AM-3098
Automation Manager	Date fields marked as mandatory despite of input parameter on Get Windows Event	AM-3106
Automation Manager	Result code collision	AM-3113
Automation Manager	Get Windows Events object not including results with eventdate = TimeCreated	AM-3119



Automation Manager	Fix the template related to Date input parameter	AM-3131
Automation Manager	Validate TLS Certificates	AM-3137
Automation Manager	TLS Validation - Message on Designer when Certificate is not valid	AM-3244
Automation Manager	TLS Validation - Agent - Force Default to 'True' By Reading N-central Agent Version	AM-3245
Core	[DMS] Maint task to clear out old device registration list	NCCF-42794
Core	[DMS]Update invitation usage information on Invitation display for the DMA mobile device	NCCF-68995
Core	[UI] Add DMA dropdown to Mobile Devices list	NCCF-37643
Core	[UI] Mobile devices not added at SO/System level if only Customer DMA cert is available	NCCF-68904
Core	[UI] Populate IMEI field in mobile device details view	NCCF-70723
Core	[UI] Update certificate warning message	NCCF-36926
Core	[UI] Update 'Setup Prerequisites' dialog to have path to DMA	NCCF-41138
Core	Remove RebootWindows.vbs, killing the agent while running a scheduled task, resets downtime window early	NCCF-14669
Core	Proadmin/Support Admin cannot edit filters	NCCF-15447
Core	Missing slash from tool tip	NCCF-16494
Core	Country field in Customer settings not saved when cleared	NCCF-16816
Core	Re-use of the remotecontroltaskid, the remotecontroltaskauditlog can record two different devices	NCCF-16920
Core	Filter by Column on the Custom Services Index Page	NCCF-17333
Core	Domain User Management - Require Password Change Greyed out	NCCF-22447
Core	ConnectWise customFields Not handled Correctly	NCCF-23387
Core	Self-Healing didn't trigger - Windows Service - MagTAC.Service	NCCF-25719
Core	Service Template Self Healing Notifications System level PSA ticketing recipients not available as recipients	NCCF-28940
Core	SNMP Profile Names with Special Characters in Discovery Jobs Causes System Errors	NCCF-29102
Core	Mis-direct caused by additions of '/login' and 'static_index.http'	NCCF-29610
Core	DeviceModify Not Checking All Products on Device Save	NCCF-40194
Core	OAuth2 Grant Type Missing for Custom IDP configuration	NCCF-41628
Core	Using Select All Under Filters and Then Reducing Selection Keeps Items Selected	NCCF-42262



Core	java.net.SocketException: Socket closed on LDClient initialization or idle connections	NCCF-52468
Core	DMA Command - Command History	NCCF-53891
Core	Restrict devices enrolling based on available licenses	NCCF-57604
Core	VPP Handle moving enrolled devices between Customers/Sites	NCCF-57646
Core	Proper path-separators need to be used in upgrademodule.dll when downloading files from server	NCCF-59749
Core	Update N-central to Add Certificate Verification	NCCF-60210
Core	In Administration Utilities - Active Sessions: Clicking in Refresh button should do the same thing as clicking in Administration Utilities - Active Sessions.	NCCF-60718
Core	Windows Agent: Extract the feature zip for installation module	NCCF-61348
Core	Update N-central Server Network/Appliance Configuration Settings	NCCF-64247
Core	VPP Customers/Sites sync maintenance task	NCCF-65179
Core	Provide customer and site names to the platform API during user token retrieving	NCCF-65845
Core	Handle mobile device enrollment when DMA only has partial info	NCCF-66157
Core	Scheduled Task Profiles Not Refreshing Customer Org Properties	NCCF-67983
Core	Update logging for Client Certificate revocation failures	NCCF-68006
Core	Clean Up ConfigType Errors in Agent Logs	NCCF-68548
Core	Automated N-central OS Package Update - March 01, 2023	NCCF-69842
Core	Refresh token when user switches to a different SO	NCCF-69897
Core	Implement token caching for current SO level	NCCF-69898
Core	Modify the analytics-rest-proxy to support v2.0 APIs	NCCF-69991
Core	Device Configuration: Policy endpoint	NCCF-70369
Core	Add a roles to the generic API payload	NCCF-70374
Core	Add permissions to getUserToken call	NCCF-70407
Core	Send customer filter parameters to iframe	NCCF-70412
Core	Provide more detail about SSL SOAP ERROR in install_nagent.log for Linux agent	NCCF-70416
Core	Handling qAPI URL (N-central side)	NCCF-71536
Core	Permissions - V2 Request DTO Permission Property Needed	NCCF-71602
Core	Update Backup and Restore to support the Certificate changes	NCCF-71603

Core	Add Index to 'notificationtrigger' Table for Performance	NCCF-71649
Core	Adjust partner id to contain bizappsid and server guid	NCCF-72116
Core	VPP Permission - Read Only/Managed/None	NCCF-72131
Core	Reset Password button fails in Domain User Management UI View	NCCF-73409
Core	Check for active paths before renewing SQS credentials	NCCF-73999
Core	Clicking on Device in Device list causing System error	NCCF-74071
Core	Scheduled Task Scripting During Agent Offline: Status not Completed	NCCF-74550
Core	Automated N-central OS Package Update - March 20, 2023	NCCF-74788
Core	Handle get token error when opening the mobile device list view	NCCF-74990
Core	Make DbContext Immutable to Prevent Race Condition Risk	NCCF-75824
Core	Make DbContext Immutable	NCCF-75825
Core	Left-hand menu for Analytics needs to show we are (Preview)	NCCF-77002
Core	Take Control UI changes not implemented properly	NCCF-78780
Core	Disabling AMP-based monitoring service doesn't stop execution of AM policies	NCCF-90163
Ecosystem Framework	Left Hand Nav bar slow or will not load when 443 traffic blocked	KUIP-3750
Patch Management	[NC Agent] Installation of Enablement Package - Handle approvals of both standard FU and EP	PMCM-2522
Patch Management	[NC Agent] agents not reading recent patches as installed when changing approval	PMCM-3234



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.

Agents & Probes

Description	Bug
New Windows Agent installations must have a valid FQDN as the first entry in the server address list in order to install successfully. Upgrades and existing agent communication should continue to work as expected.	NCCF-79152
The pre-upgrade check and Installation checks will still require a valid HTTPS connection to verify the N-central server certificate before allowing the connection. This is still required for Devices set to connect only through HTTP. Once the agents are upgraded, basic functionality will work over HTTP but Remote control and Direct Support will still connect over HTTPS and require a valid certificate connection.	NCCF-94172
Communication issues may be encountered for N-able N-central Probes installed on Windows servers that have multiple NICs. For more information, refer to " <i>KBA20020: Configuring A Server With Multiple NICs</i> " 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

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
In certain situations, some logs may not roll over properly where the N-central UI port is set to something other than port 443. This could consume N-central disk space more rapidly than expected. If you are using a customized UI port, please contact Support for a finger fix.	NCCF-81833

Description	Bug
<p>Installing N-able N-central on Servers that have an Nvidia Video Card</p> <p>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.</p>	NCCF-11842
HDM does 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

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
<p>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.</p>	65620

UI

Description	Bug
The Remote Control icon may show yellow for devices where Take Control is not the default Remote Control method, or Take Control is not installed.	NCCF-82944
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
<p>Login window reappears when new tab is loaded.</p> <p>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.</p>	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 Bit-defender 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	<p>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.</p> <p>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 NVMe for bare metal and virtualized hosts, or a Fibre Channel connected SAN with Enterprise Grade hard drives for virtualized hosts (<i>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</i>).</p> <p>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.</p>

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 DDPD (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	<p>It is impossible to guarantee the scalability or performance of a N-able N-central server deployed on a Virtual Machine due to:</p> <ul style="list-style-type: none"> ▪ 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	<p>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.</p> <p>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.</p>
Virtual Hardware Support	<p>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.</p>

	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	<p>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.</p> <p>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.</p>
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

- 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)

AV Defender

Workstation Operating Systems


- Microsoft Windows 11
- Microsoft Windows 10
- Microsoft Windows 8, 8.1

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

 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
- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7

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)
- Microsoft Windows 8.1 (32/64-bit)
- Microsoft Windows 8 (32/64-bit)
- Microsoft Windows 7 (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 LTSC	Windows 10 Enterprise 2016 LTSC
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	✓	✓	✓	✓	✓	✓



Licensing and Customer Support

Agent/Probe Installation Software

N-able N-central 2023.4 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



© 2023 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of N-able. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of N-able, its affiliates, and/or its respective licensors.

N-ABLE DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL N-ABLE, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF N-ABLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The N-ABLE, N-CENTRAL, and other N-able trademarks and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. and may be common law marks, are registered, or are pending registration with the U.S. Patent and Trademark Office and with other countries. All other trademarks mentioned herein are used for identification purposes only and are trademarks (and may be registered trademarks) of their respective companies.

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.