N-ABLE™

N-central

Release Notes

Version: 2023.8 (Build: 2023.8.0.11)

What's New in N-able N-central 2023.8

Analytics

We are so excited to announce the introduction of Analytics into N-central 2023.8! We have harnessed the industry standard of PowerBI, to bring you your N-central data in full visuals. With our GA release, you will be able to see device data (inventory, summary, warranty, etc.), backup data (last backed up, last checked in, etc.), and patch information (installed, approved, missing, etc.) And those are just the first of more dashboards to come.

Analytics is more than just our dashboards, it is also our reports that help you communicate the value you provide, to your customers. Our executive summary report is a streamlined view of the health of each customer account -- this can be exported, or this can be sent on a repeating schedule as an email. We know reports are of high value, and we will continue to add more reports as our analytics feature set grows beyond GA.

What comes out of the box?

- Device inventory
- Device summary
- Backup Sessions
- Backup Devices
- Patch Status
- Executive Summary Report

And we are adding more often!

Our dashboards and reports were created to help answer common business problems, but we know we can't predict all the questions you may have – you can customize your reports and dashboards to suit your business. Remove items you don't need and adjust the charts to show only the information relevant to you, your users, and your business.

Your data security is important to us – here is a collection of potential questions and answers you may have around security.

To get started, please activate Analytics and set your permissions. Learn how here.

Device Management for Apple Enhancements

Coming to all onprem partners, in this release, are our new MDM capabilities. We're also moving access from the System level to the Service Organization level.

Migrating Account Level Certificates

As we move access of Device Management for Apple to the SO level, we're bringing the account level certificate there as well. This shouldn't affect anything in your environment and is simply a better way to control your certificates. Best practice recommendations, from us and Apple, for Certificates and Device Management for Apple is to use our multi-tenant capabilities and use Customer level certificates to manage individual customers' devices.

Apple Business Manager zero touch deployment

We are pleased to announce that you can now enroll your devices via Apple Business Manager. Doing so enrolls your ABM purchased device or freshly wiped device into Device Management for Apple and, for your Apple workstations, will also deploy the latest N-central mac agent to your device upon completion of the boot up process.

You will now have the ability to enroll iOS and iPadOS devices into Device Management for Apple (DMA). You will no longer be able to enroll Apple or Android devices into our Legacy MDM service.

App Deployment

We are pleased to announce the addition of App Store management to N-central's Device Management for Apple. N-central can now receive a token from an Apple Business Manager or Apple School Manager account and deploy App Store purchases made in those accounts to deploy company-owned apps to Macs, iPhones, iPads, and even AppleTVs enrolled in N-central.

This means that end-users of the devices won't need to use a personal Apple ID or some other workaround to get the business apps they need on managed devices. You'll be able to ensure they have all the apps they need, revoke the licenses as needed, and keep the apps up-to-date.

N-central's Device Management for Apple is multi-tenant, meaning you can set up the tokens for each customer's own ABM/ASM account in one dashboard.
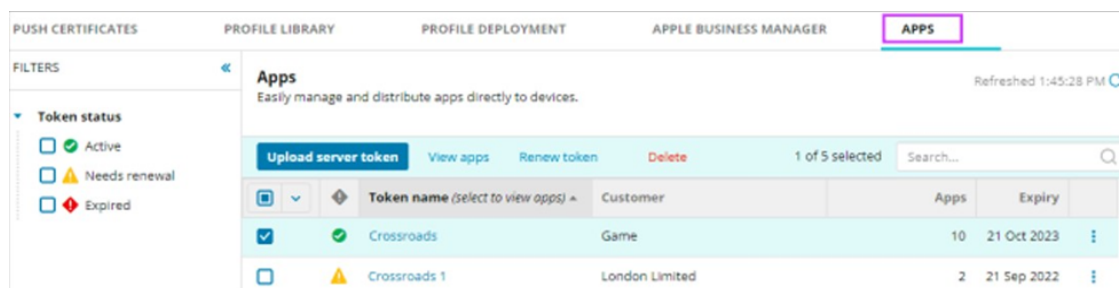
Devices don't need to have been enrolled in N-central via ABM/ASM. Purchased apps can be deployed to devices that were manually enrolled also.

OS Update Commands

There are up to 5 options in the command API:

- Download or install the update, depending on the current state. This lets the OS decide which action it should take based on whether a user is logged in and working or its configuration. This is the safest option and should be considered a default.
- Download the software update without installing it.
- Download the latest update and trigger the restart countdown: In iOS and tvOS, this will install a previously downloaded software update. In macOS it will download the software update and trigger the restart countdown notification via Notification Center.
- Download the software update and notify the user through the App Store. This option is only available in macOS.
- Download or install the latest update, force a restart if required: As it says, this will do the default action, but will make a restart mandatory. This could result in data loss from unsaved work. This option is only available in macOS.

Here are some important things to know about these commands:

- DMA can only send the command to the device. It's up to the device to obey the command. Sometimes it won't. We expect that Apple's APIs and implementation will improve as new OS version are released. It's already far more reliable on macOS Ventura than it was on previous macOS versions. N-able is only supporting these commands on macOS 13 Ventura and iOS 16 or later.
- The commands may succeed on previous OS versions, but they will always download and install the latest full OS version. For example, if you run the command on macOS 12 Monterey, it may or may not execute reliably, and if it does it will upgrade the device to macOS 13 Ventura.
- The behavior of these commands can be modified via Configuration Profiles.

- A lot also depends on whether the device has been provisioned as Supervised. Supervised devices, including those enrolled in DMA by way of Apple Business Manager/Apple School Manager automatic enrollment are far more likely to behave as desired. Non-Supervised devices will likely require user input to complete the process.

Endpoint Detection and Response

This new and improved EDR integration will give you full SentinelOne functionality while continuing to utilize N-central for bulk deployment (Windows and MacOS) and real-time monitoring of your devices. With full dashboard access to SentinelOne, including SSO access via Azure AD, you can now view detailed threat reports, configure granular notifications, and access the SentinelOne API. You can also try advanced security features like Threat Hunting, also known as "Deep Visibility".

Currently, the integration supports new EDR customers. If you are currently using integrated EDR in N-central, you can look forward to an upgrade button in a near future release that will assist you in upgrading to this new EDR integration. For Mac support with this EDR integration, your Mac agents will require v1.8.2 or above.

AI Assisted Scripting

We have introduced a new and exciting feature to the Scheduled Tasks interface, which allows you to leverage ChatGPT's artificial intelligence to generate new scripts and upload them to the script repository. Simply provide some script instructions in the UI, review the script that the AI provides, and upload it to the repository with the click of a button. To see this new feature, your account will need access to Manage the Script/Software Repository. You will also need an account with ChatGPT to provide a user token.

Cove Deployment Amps in the Repository!

With N-central 2023.8, we've made it simpler for you to deploy Cove Data Protection to your managed devices, by adding the deployment AMPs to the Script/Software repository.

Automation Manager Update!

Automation Manager 2.92 has an update in N-central 2023.8. Several bugs have been addressed, and the submission of data from the AM agent to Pendo has been disabled.

Upgrade paths and notes

Upgrade versions

To upgrade to N-able N-central 2023.8, 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+

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

> **i** 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 23.8 GA

Category	Description	Item
Analytics	WorkspaceId is sometimes not provided in embed-dedtoken request	DV-5076
Analytics	Restricting Custom Report creation with duplicated name under the same category	DV-4927
Analytics	"Last sync" is not getting updated for other Golden dataset reports in case of one of them having a proper Last sync value	DV-4622
Analytics	"Last sync" showing wrong value(ie Refreshing) on Dashboards List screen even in case of /reports/status having "Ready" status	DV-4621
Analytics	"Development" value is highlighting always when clicking on the Category dropdown	DV-4513
Analytics	Duplicate report names are allowing for Custom reports	DV-4511
Analytics	Filter functionality on dashboards list screen is giving wrong result set	DV-4467
Analytics	Dropdown list in reports view page is not getting closed when EU clicks on report details	DV-4269
Automation Manager	Disable Pendo on Automation Manager	AM-3861
Automation Manager	Get Windows Events - issues with date formats	AM-3738
Automation Manager	Object Sync Time with External NTP returning Result 0 on error	AM-3560
Automation Manager	Designer logs rotation	AM-3356
Core	[FEATURE] Enhanced EDR Integration available in N-central for New EDR users	NCCF-49731
Core	API-Service Related Enhancements	NCCF-132837
Core	Contact Link Text Adds Escape Slashes to Links	NCCF-131729
Core	Snapshot creation for CentOS and Ubuntu are failing	NCCF-130279
Core	Cove Deployment AMPs need to be added to the N-central repository as stock, permanent items	NCCF-130207
Core	Address code in Cove Integration related classes	NCCF-127943
Core	Excessive Log Rollover Due to Linux Agent Spam	NCCF-121288
Core	Linux agents skipping first entry in endpoint list when ses-	NCCF-121020

	sion is lost	
Core	Incorrect Spelling of N-central	NCCF-120987
Core	Self-Healing is running much to often than is configured	NCCF-120506
Core	Fix string exception HTTPS Monitoring Service mis-configured.	NCCF-115464
Core	N-central Backup Restore throwing DFM restore errors with SQL on Azure	NCCF-111559
Core	Optimize ServerUI API invocation from OS scripts	NCCF-108882
Core	SPX Services not connecting	NCCF-107926
Core	Unlinking SSO Account Does Not Re-Enable MFA	NCCF-65882
Core	Command Prompt Timeouts After 5 Minutes	NCCF-40857
Core	Modify Openfire Settings to Drop Offline Messages and Cleanup	NCCF-30867
Core	configtypesignature Has No Foreign Key Constraint, So it Never Gets Cleaned Up	NCCF-24480
Core	Miss-Spelling of N-central on Server Restart Warning	NCCF-22942
Core	Uploading anything through Direct Support that takes more than 5 minutes has it's request killed	NCCF-18911
Device Management Apple	Change order of parameters when generating AAID	MSAD-3204
Device Management Apple	Make DMA menu only visible at SO level for on-prem and NCOD instances	MSAD-3172
Device Management Apple	Handle mobile device list at System level	MSAD-3163
Device Management Apple	Remove DMA dropdown from System level	MSAD-3162
Device Management Apple	Update Client / Site sync	MSAD-3161
Device Management Apple	Update ABM Polling to loop through SOs	MSAD-3160
Device Management Apple	Update AAID generation to have SO ID	MSAD-3159
Device Management Apple	N-central - Provide client IDs in JWT	MSAD-3113
Ecosystem Framework	Update agent to use new GRPC library.	KUIP-2817

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

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.	NCCF11842
HDM does not work with the "Last 5 Tickets" widget.	NCCF10855

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
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.	NCCF29648

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
- Microsoft Windows 8.1 Professional
- Microsoft Windows 8.0 Professional
- Microsoft Windows 7.0 Enterprise/Ultimate
- Microsoft Windows 7.0 Professional

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
- 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 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	✔	✔	✔	✔	✔	✔

Licensing and Customer Support

Agent/Probe Installation Software

N-able N-central 2023.8 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.