N-central

Release Notes

Version: 2023.1 (Build: 2023.1.0.13)

Last Updated: Thursday, March 16, 2023

What's New in N-able N-central 2023.1

N-central 2023.1 is packed with both fixes as well as a new feature! Please see below for more information on our new feature, and the list of fixed items!

Customizing the N-central UI Port is now GA!

An exciting new feature in 2023.1, is the ability to control the port at which the N-central UI runs. The goal of this feature is to allow our on-premise N-central Partners to increase the security of their N-central instance by controlling how and if their N-central UI is exposed to the internet. This feature is not enabled by default on upgrades and can be enabled via **Administration** > **Mail and Network Settings** > **Network Setup**. New installations of N-central 2023.1 will have 8443 as its default UI port. You can learn more here.

Automation Manager 2.60

Automation Manager 2.60 is now available and included in N-central 2023.1. This version of Automation Manager focuses on bugfixes, including fixes that improve the installation of Scriptrunner.

Mac Agent 1.2.4

Along with N-central 2023.1, the new Mac Agent 1.2.4 was released and contains a fix for the missing CPU and Memory graphs as well as additional improvements!

Major bug fixes

Alongside 40+ other items shown below, there have been several key improvements and fixes in this build! We have resolved a highly impactful issue with the inability to load AMPs when logging in as an IDP linked user (NCCF-35682). We have also resolved an issue with establishing a RDP (NCCF-49091) session as well as an issue with Report Manager data exports (NCCF-49480).

Upgrade paths and notes

We are aware that many partners may have problems with their probes upgrading to 2023.1. Before upgrading N-central to 2023.1, please download and review the instructions in the following zip file: Probe Upgrade Instructions.

Upgrade versions

To upgrade to N-able N-central 2023.1, 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+

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.

IMPORTANT: If you are a Partner running N-central in Azure, review the following article to avoid any potential issues with the upgrade to this release. We have identified an issue that impacts our Azure hosted N-central partners. Fortunately, our team has steps to resolve the issue. Before upgrading your N-central server to any supported version, review the following article: How to Identify a Legacy Azure N-central Instance.

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 2023.1 GA

Category	Description	Item
Core	[USABILITY] Filters missing two Windows 10 OS entries	NCCF-48241
Core	[FEATURE] Custom UI Port (GA)	NCCF-24987
Core	[COMMAND] Lock Device	NCCF-31997
Core	Port :10000 /admin should be disabled when the nacintegration is enabled	NCCF-44808
Core	Direct Support option disappears when creating new device with class Workstions - Mac	NCCF-44658
Core	Linux_Ubuntu_Agent AttributeError: 'NoneType' object has no attribute 'group'	NCCF-44429
Core	Discovery_JobsFAIL Multiple keywords with name 'Verify Target Device'	NCCF-44427
Core	After Upgrading from 2022.7.0.26 to 2022.8.0.12, Mac Agent v1.2.0.98 has had Direct Support impacted	NCCF-43803
Core	Monitoring processes are missing for the Mac agent	NCCF-43095
Core	nacintegration Version Management not working for nsp file upgrade	NCCF-42304
Core	Apireader metric is not cleared on prometheus collect	NCCF-40091
Core	License Key Page Edge Case: Reactivating N-central using NAC when License Key becomes Expired	NCCF-38997
Core	Scraping customer filter should include all customers deleted or not	NCCF-37085
Core	Some 32-bit Linux Agent cleanup was missed in NCCF-24931	NCCF-34211
Core	Custom Service through XML File: Navigating to Administration > Service Management > Custom Services failed with message 'The Menu Panel Item is not clicked'	NCCF-33052
Core	Custom Services: Add Log Scan Custom Services: PR #1517 Introduced a comparison of a string 'true' to a boolean True	NCCF-33050
Core	Remove Arcserve link from UI	NCCF-32960
Core	Adjust N-central install and upgrade scripts with the alternative UI port currently used	NCCF-24830
Core	Insufficient Logging in AMPBasedMonitoringModule.log In Log Level 3	NCCF-17311
Core	DNS filtering Rule Not applying settings to endpoint	KUIP-4433
Core	Intune Compliance Service Deploying Automatically	KUIP-4282
Core	The DNSF integration is not activating properly when having a consistent number of suborgs ~ 2000 +	INT-1075

Core	Windows Update (Oct. MRT) Approval	PMCM-2520
Core	NC agents not reading recent patches as installed.	PMCM-2440
Core	Report Manager Export Hangs on Decryption of Database Values	NCCF-49480
Core	An error occurred while establishing the Remote Control session	NCCF-49091
Core	Fresh Agent installs missing gRPC-related files	NCCF-41156
Core	IDP User cannot access AMP from server within Automation Manager	NCCF-35682
Core	Disk Usage Service Metrics Last 90 days won't load	NCCF-29599
Core	No User role for restricting Deleting customers	NCCF-28678
Core	Missing "Microsoft Windows 11" From supportedos Table	NCCF-22678
Core	System Error On User Delete	NCCF-22155
Core	ApplianceSelfRegistration Contains Sensitive Information	NCCF-51284
Core	Update Firewalld rules	NCCF-31460
Core	Apple Device Management rebranding to Device Management for Apple	NCCF-38736
Core	Include customer and device history tables as well as regular when scraping	NCCF-37086
Core	Expand deviceAssetInfoExportDeviceWithSettings SOAP API endpoint to include Take Control information	NCCF-37028
Core	UI | Analytics Splash Message Removal	NCCF-36388
Core	UI | Eventproduction | Only product admin	NCCF-36387
Core	Update Core Regression Multijob to use New Activation server setup	NCCF-18553

Automation Manager 2.60

Category	Summary	Item
Automation Manager	Issues with downloading file to install software	AM-2984
Automation Manager	AMP Resize VHD string error	AM-2982
Automation Manager	Firewall objects only enable/disable current profile	AM-2980
Automation Manager	AMP Object Bugs - If & If/Else Object	AM-2973
Automation Manager	Installer for Scriptrunner improvements	AM-2955
Automation Manager	Policy upgrade procedure are not working correctly for nested objects	AM-2944
Automation Manager	Bug in reboot prompt	AM-2937
Automation Manager	Exception encountered Sys-tem.Runtime.Serialization.SerializationException [Alliance]	AM-2929
Automation Manager	MinRequiredVersion in AMPs is incorrect if the objects with newer ver-	AM-2798

	sion are nested	
Automation Manager	Accessing Clipboard sometimes throws exception: Failed to copy, CLIPBRD_E_CANT_OPEN	AM-1326

Mac Agent 1.2.4

Category	Description	Item
Core	[USABILITY] Mac Agent 1.2.4 Release	CALM-1971
Core	Message loss to CPU/Memory graphics after adding deep ping	CALM-1967

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

Automation Manager

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

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
For users with the NAC in UI feature enabled, the upgrade process from an earlier version of N-central to 2023.1 will fail to run properly. If you are previewing the NAC in UI feature, please contact support for upgrade assistance.	NCCF-55470
Installing N-able N-central on Servers that have an Nvidia Video Card Due to a bug in CentOS 7 with Nvidia's "Nouveau" driver, installing N-able N-central on servers that have an Nvidia video card may result in the N-able N-central console showing a blank screen, or displaying an Anaconda Installer screen with an error message about the video card driver.	NCCF-11842
HDM does not work with the "Last 5 Tickets" widget.	NCCF-10855

Description	Bug
Warranty information might be inaccurate when determining the warranty expiry dates of devices that are not located in the USA.	NCCF-3649
An issue has been found in 2022.7+ versions where Direct Support functionality is not available for Mac agents, and cannot be turned on for certain Mac device classes. A fix is in progress and will be included in a future release.	NCCF-43803

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.	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.

N-able N-central System requirements

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

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

Processor	Server class x86_64 CPUs manufactured by Intel or AMD (i.e. Xeon or EPYC). Please refer to the Red Hat Hardware Ecosystem for further details.
Operating System	You do not need to install a separate Operating System to run N-able N-central. The N-able N-central ISO includes a modified version of CentOS 7, based on the upstream Red Hat Enterprise Linux 7.
Physical Hardware	The physical server used to install N-able N-central in a bare metal environment must be certified to run Red Hat Enterprise Linux 7.9 (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.

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	N-able recommends using the VMXNET3 network card in VMWare. When the VM is

Adapters	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

- 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 LTSB	Windows 10 Enterprise 2016 LTSB
Windows 10 Enterprise for Virtual Desktops	Windows 10 Enterprise LTSC 2019
Windows 10 Pro	Windows 10 Pro Education
Windows 10 Pro for Workstations	

Windows Server 2008 R2 Enterprise	Windows Server 2008 R2 Datacenter
Windows Server 2008 R2 Standard	Windows Server 2008 R2 Foundation
Windows Server 2012 Datacenter	Windows Server 2012 Essentials
Windows Server 2012 Foundation	Windows Server 2012 R2 Datacenter
Windows Server 2012 R2 Essentials	Windows Server 2012 R2 Foundation
Windows Server 2012 R2 Standard	Windows Server 2012 R2 Standard Evaluation
Windows Server 2012 Standard	
Windows Server 2016 Datacenter	Windows Server 2016 Datacenter Evaluation
Windows Server 2016 Essentials	Windows Server 2016 Standard
Windows Server 2016 Standard Evaluation	
Windows Server 2019 Datacenter	Windows Server 2019 Essentials
Windows Server 2019 Standard	Windows Server 2019 Standard Evaluation
Windows Server Datacenter	
Windows Small Business Server 2011 Essentials	Windows Small Business Server 2011 Standard

Port access requirements

N-central Server

Access must be permitted to the following ports:

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
20		√			Used for FTP connections, particularly when configured for backups.
21		√			Used for FTP connections, particularly when configured for backups.
22	√			√	SSH - used for remote control sessions. The firewall must be configured to allow access from the Internet to this port on the N-able N-central server.
25		√			SMTP - used for sending mail.
53		√			Used for DNS.
80	√	√		√	HTTP - used for communication between the N-able N-central and agents or probes. N-able N-central recommends that you block all access from the internet to this port on the N-able N-central server, unless it is absolutely required. This port may be closed in a future release. This port must also be open for outbound traffic if the N-able N-central server is monitoring HTTP services on remote managed devices.
123		√			Used by the NTP Date service which keeps the server clock synchronized. Normally using UDP (although some servers can use TCP).
135			√		Used by Agents and Probes for WMI queries to monitor various services. Inbound from the Windows Probe to the Windows Agent.
139			√		Used by Agents and Probes for WMI

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
					queries to monitor various services. Inbound from the Windows Probe to the Windows Agent.
443	√	√		√	HTTPS - used for communication between N-able N-central and Agents or Probes (including MSP Connect and MSP Anywhere). Your firewall must be configured to allow access from the Internet to this port on the N-able N-central server. This port must be open for outbound traffic if the N-able N-central server is monitoring HTTPS services on remote managed devices. Backup Manager on endpoint devices uses Port 443 TCP outbound. It is almost always open on workstations but may be closed on servers. Used by Agents and Probes as a failover for XMPP traffic when they cannot reach N-centralon port 5280. To activate EDR the N-able N-central server needs outbound HTTPS access to port 443 and the following domains: ■ *.sentinelone.net ■ sis.n-able.com ■ keybox.solarwindsmsp.com Pendo allows us to provide in-UI messaging and guides when there are important changes, new features onboarding, or other critical messages that we need to tell you about. You can gain access to these important messages, and help us make important design decisions from usage data, by allowing outbound HTTPS/443 access from your N-central server to the following URLs: ■ cdn.pendo.io ■ data.pendo.io

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
					▪ pendo-io-static.storage.googleapis.com ▪ pendo-static*.storage.googleapis.com
445			√		Used by Agents and Probes for WMI queries to monitor various services.
1234		√		√	Used by MSP Connect in UDP mode.
1235		√		√	
1433		*	*	*	Outbound on the N-able N-central server, port 1433 is used by Report Manager for data export. On managed devices, it is also used by Agents (inbound) and Probes (outbound) to monitor Backup Exec jobs. ℹ Inbound from the local LAN and not the Internet.
	* Port access is only required if you have installed the corresponding product. For example, access to port 1433 is only required if you have installed Report Manager or if you are managing Backup Exec jobs.				
5000		√			Backup Manager will use local port 5000. If this port is unavailable, Backup Manager will detect a free port automatically (starting from 5001, 5002 and up).
5280	√			√	Used by Agents and Probes for XMPP traffic. Outbound access to port 5280 for Managed Devices is recommended but not required.
8014			√		Backup Manager requires access to port 8014. This value cannot be modified. ℹ Inbound from the local LAN and not the Internet.
8443	√	√		√	The default port for the N-central UI. TCP port 8443 is used for TLS (HTTPS) connections to the N-central Web UI. Your firewall may be configured to allow access

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
					from the internet to this port on the N-able N-central server, if you require Web UI access outside of the network N-central is deployed to. You can change this port number in the N-central Administrator menu, under "Network Setup".
8800		√			The Feature Flag System in N-able N-central needs to talk to mtls.api.featureflags.prd.sharedsvcs.system-monitor.com. Used by N-able – generally during Early Access Preview and Release Candidate testing – to enable and disable features within N-able N-central.
10000	√				HTTPS - used for access to the N-able N-central Administration Console (NAC). The firewall must be configured to allow access from the Internet to this port on the N-able N-central server. N-able recommends excluding all other inbound traffic to port 10000 except from N-able Ports for Support section below.
10004			√	√	N-able N-central Agents must be able to communicate with a Probe on the network over port 10004 in order for Probe caching of software updates to function properly. Inbound from the local LAN and not the Internet.
15000			√	√	For downloading software patches, port 15000 must be accessible for inbound traffic on the Probe device while it must be accessible for outbound traffic on devices with Agents. Inbound from the local LAN and not the Internet.

Supported operating systems for remote control

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

Remote Control Type	Windows		Linux		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 2023.1 uses the 7-Zip file archiver for installing agents and probes. 7-Zip is free software redistributed under the terms of the GNU Lesser General Public License as published by the Free Software Foundation. For more information, see http://www.7-zip.org.

Customer Support

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

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

About N-able

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