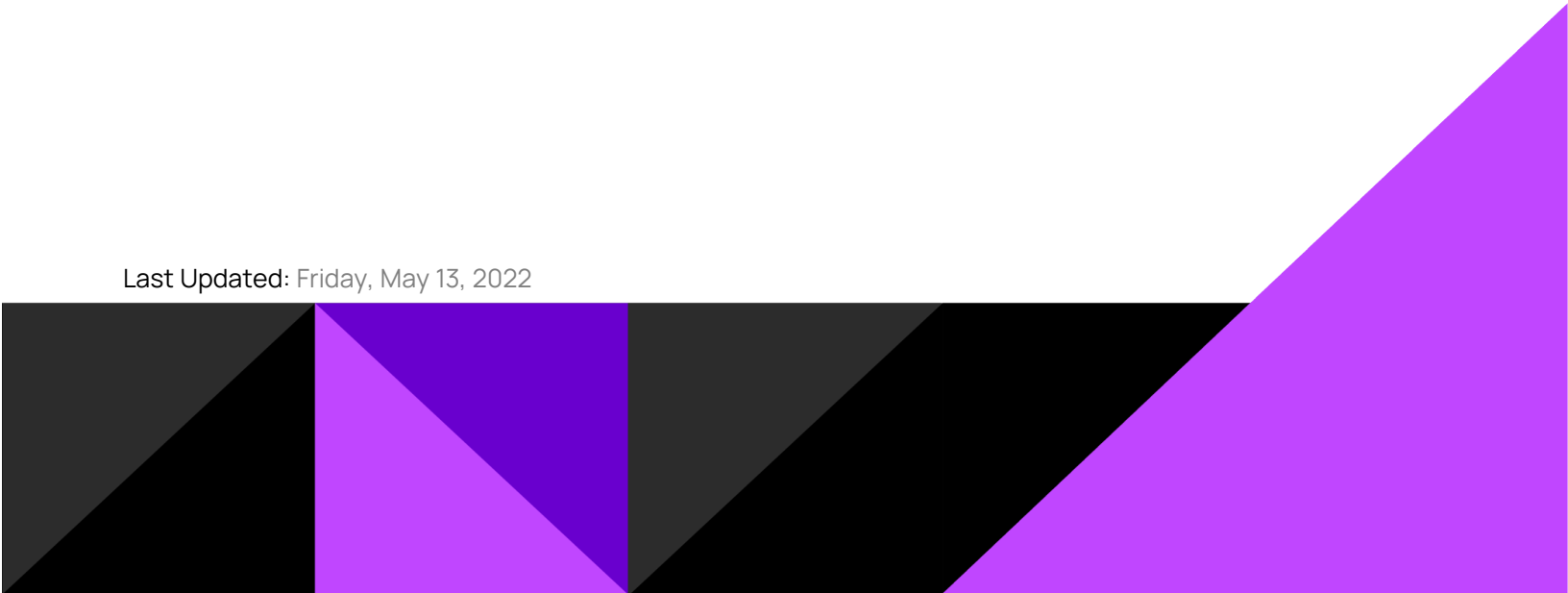
N-ABLE™

N-central

Release Notes

Version: 2022.3 (Build: 2022.3.0.46)

Last Updated: Friday, May 13, 2022



What's New in N-able N-central 2022.3

Preview of the new macOS Agent

Our awesome Engineering teams have been hard at work thoroughly overhauling N-central's macOS agent, and we're really excited to let you try out a Preview of this new agent. Available as a separate download from the **Actions** → **Download Agent/Probe** page, the new macOS agent includes the following improvements:

- Support for M1 processors
- Proper notarization/signing of the installer
- The macOS agent is now a separately releasable component, which means that once its installed, it'll update itself with the latest bug fixes and new features, without requiring an upgrade to your N-central server
- The foundation for supporting more real-time actions, such as the Tools menu, the Overview tab, and the real-time CPU and Memory graphs are included in this version of the macOS agent, and will be enabled in an upcoming release
- Over 70 bug fixes in comparison to the "legacy" macOS agent

This first Preview of the new macOS agent allows you to install/uninstall the agent on test devices; in a future release of N-central, we'll also allow you to push the new macOS agent via the Windows Probe, and upgrade the "legacy" macOS agent to the new binary.

Support for Ubuntu 20.04

N-central's Linux agent has been updated to support Ubuntu 20.04; you'll find a new installer that is specific to Ubuntu 20.04 under the Actions → Download Agent/Probe page, and in the Add/Import Devices wizard. The Operating System drop-down menu has also been updated to include Ubuntu 20.04.

Updates to Automation Manager

N-central 2022.3 comes bundled with Automation Manager 2.40, which is a significant upgrade over the version of Automation Manager (v2.19) that was included in earlier versions of N-central. Notable changes between v2.19 and v2.40 of Automation Manager include:

- The AM Designer executable is now signed with the "N-able Solutions ULC and N-able Technologies LTD" software signing certificate.
- Automation Manager is now a separately releasable component, which means that once its installed, it'll update itself with the latest bug fixes, new objects and new features, without requiring an upgrade to your N-central server.
- The "Reboot Prompt" object has been updated to include a new "Allow user to postpone past the limit" option. This new option is a "parent" of the existing "Allow user to decline reboot" option and makes it possible to further fine-tune how what options you want to present to your users when their machine needs to be rebooted.
- A number of Partner-reported bugs have been addressed; please see the "Fixed Bugs" list in this document for details.

HP and HPE (HP Enterprise) Warranty Lookups

Due to changes by the vendor, N-central is unable to perform warranty lookups on HP and HPE devices. This functionality has been removed in N-central 2022.3, which allows you to manually specify the warranty expiry date and purchase date of your HP/HPE devices, without needing to worry about N-central overwriting those values. We will continue to work with the vendor, and look forward to re-enabling this functionality in the future.

Upgrade paths and notes

To upgrade to N-able N-central 2022.3, your N-able N-central server must be running one of the following versions:

- N-able N-central 2021.1.0.32+
- N-able N-central 2021.1.1.305
- N-able N-central 2021.1.2.391
- N-able N-central 2021.1.3.428
- N-able N-central 2021.1.4.467+
- N-able N-central 2021.1.5.526
- N-able N-central 2021.1.6.727+
- N-able N-central 2021.1.7.830+
- N-able N-central 2021.1.8.881
- N-able N-central 2021.2.0.140+
- N-able N-central 2021.3.0.79+
- N-able N-central 2022.1.0.47+
- N-able N-central 2022.2.0.77+
- N-able N-central 2022.3.0.46

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

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

Fixed Issues in N-able N-central

Release 2022.3

Category	Description	Bug
Automation Manager	The "Remove Local Profiles" Object Throws A "Error: The file or assembly \"WindowsInput, Version=1.0.4.0, Culture=neutral, PublicKeyToken=9b287f7dc5073cad\" Error Message	AM-2815
Automation Manager	Script Runner Error: System.Runtime.Serialization.SerializationException	AM-2769
Automation Manager	AM 2.30 -> Should support the 8.3 shortname notation	AM-2763
Automation Manager	HTTP-compressed Files Are Not Decompressed When Using The "Download File From URL" Object	AM-2760
Automation Manager	AMP based monitoring misconfigured after upgrade to 2021.2.0.140 agent	AM-2757
Automation Manager	The "Get N-able RMM Agent Information" Object Doesn't Return Information About the Group Policy Advanced Monitoring Agent	AM-2753
Automation Manager	When Saving a New Copy Of An AMP, Automation Manager Doesn't Open The New Copy	AM-2750
Automation Manager	AM Designer Launches with a SW Software Publisher	AM-2747
Automation Manager	Download File from URL module failing to download Agent using RMM API	AM-2742
Automation Manager	#ST00066055 Unknown Script error	AM-2741
Automation Manager	The "Open Session" Object Reports "Failed to negotiate key exchange algorithm"	AM-2740
Automation Manager	The "Get Domain Information" and "Get AD Forest Information" Objects Return "Unknown" For Output Parameters When The Domain And Forest Are Both In 2016 Mode	AM-2729
Automation Manager	The "Get Folder List" Object Does Not Preserve non-ASCII Characters	AM-2727

Category	Description	Bug
Automation Manager	The "File Exists" Object Doesn't Find Files In C:\Windows\System32	AM-2726
Automation Manager	The "Delete Temporary Files" Object Fails If C:\Users\<username>\AppData\Local\Microsoft\Windows\INetCookies Does Not Exist	AM-2724
Automation Manager	The "Veeam Job Monitor" Service Can Report A Failed State If It Scans When A Veeam Job Is In Progress	AM-2719
Automation Manager	Automation Manager log location consuming Huge Disk Space	AM-2706
Automation Manager	Update the Required Version of PowerShell In The "Windows Firewall Profiles" AMP From v2.0 To v3.0	AM-2700
Automation Manager	The "Uninstall Software" Object fails for Windows Server 2019	AM-2698
Automation Manager	The "Get Top N Processes by CPU" Does Not Work on Windows Server 2019	AM-2697
Automation Manager	Typo "Priotity" in The "Get Network Security Events (Meraki)" Object	AM-2665
Automation Manager	AM Designer Prompts To Save Changes When No Changes Have Been Made	AM-2662
Automation Manager	The "F-Secure AV Scan Results" Service Doesn't Work With Newer Versions of F-Secure	AM-2651
Automation Manager	Error: "script failed to start" after update to Script Runner version 2.18.0.25	AM-2643
Automation Manager	script checks failing sporadically with time out or output not found	AM-2639
Automation Manager	Input prompt object displays behind other apps	AM-2635
Automation Manager	The "Download File From URL" Object Throws An Exception	AM-2615
Automation Manager	WARNING: Your connection has been redirected to the following URI	AM-2611
Automation	Why does Stop Policy fail my amp?	AM-2596

Category	Description	Bug
Manager		
Automation Manager	Windows Firewall Profiles False positive working as designed?	AM-2594
Automation Manager	The "Uninstall Software" Object Fails To Uninstall The PME "File Cache Service Agentâ€ Application	AM-2593
Automation Manager	The "Get Logical Disk Information" Doesn't Return Information If There Is Only One Logical Disk	AM-2589
Automation Manager	The "Run Powershell Script" Object Returns a "System.Xml.XmlDocument" Error When It Invokes The Chocolatey Installation Script	AM-2456
Automation Manager	The "Run Windows Defender Full Scan" Automation Manager Policy Isn't Successfully Running	AM-2384
Automation Manager	Handling Disabled Veeam backup Jobs	AM-2339
N-central Core	Searching the All DevicesView Is Too Slow	NCCF-22314
N-central Core	Incorrect Active Issues Filter results by Customer in SO level	NCCF-20577
N-central Core	Remove Prometheus 'remote_write' IP Pointing to vRA Server	NCCF-20089
N-central Core	Users With the Default Administrator Role Are Unable to Modify Some Roles	NCCF-18910
N-central Core	Services Reports A Misconfigured State When The Service Identifier Contains Conflicting Character Encodings(ISO-8859-1 vs UTF-8 vs ASCII)	NCCF-17320
N-central Core	Netpath graphs not available(including Keybox errors in N-central)	NCCF-17010
N-central Core	Separate Permission For Downloading Agent Logs	NCCF-14246
N-central Core	The Download Link for Customer A's Customer-Specific Agent Installer Can Be Accessed By A User Who Only Has Access to Customer B	NCCF-14244
Patch Management CM	In Specific Situations, Processing Patch Metadata Causes The Windows Agent To Crash	PMCM-903

Category	Description	Bug
Patch Management CM	Patches Become "Approved for install" Even Though They Were Declined	PMCM-886
Patch Management CM	Declined Patches Are Showing a "Not Installed" Status	PMCM-573

Known Limitations

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

Active Issues

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

Agents & Probes

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

Automation Manager

Description	Bug
Running Automation Manager Policies created using Automation Manager 1.6 or earlier may result in `Failed to create an EndDate ...` errors if the Policies are run on a computer using a different date format. This issue does not affect Policies created using Automation Manager 1.7 or later.	65712
If you installed Automation Manager designer version 2.20.0.18 from N-central 2021.2 RC1 or RC2 and then upgraded N-central to 2022.3 (which contains AM 2.40.0.10), the following happens: When you open Automation Manager from the N-central dashboard, it will open AM 2.30.0.11 (this is the last version on the SIS server and replaced the 2.20.0.18 version). The workaround is to force the re-installation of Automation Manager designer 2.40.0.10 by manually deleting designer-update.config from C:\ProgramData\N-Able Technologies\AutomationManager.	AM-2841

AV Defender and Backup Manager – D2D

Description	Bug
The **About Backup Manager** dialog box no longer indicates if the Backup Manager software is licensed.	68226

Custom Services

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

Core Functionality

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

Description	Bug
N-central is unable to perform warranty lookups on HP and HP Enterprise (HPE) devices.	NCCF-16190

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
The main N-central login page will fail to load when accessed from the Safari web browser. To work around this issue, please use a supported browser, such as Chrome, Edge or Firefox, or access N-central via https://<yourNCserver.com>/login.	NCCF-19768

End of support

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

Linux Agent Support	Due to declining usage in the field, the N-able N-central Linux agents will stop supporting CentOS 6, Ubuntu 14.04 and the 32-bit version of Ubuntu 16.04, in a future release.
Internet Explorer 11	Due to declining usage in the field, a future release of N-able N-central will drop support for the Internet Explorer 11 web browser.
AV Defender 5.x	As of next major release for those of you still utilizing the AV5 Bitdefender Antivirus be advised that monitoring from our AV5 agents will no longer continue. As a result this will leave your environments in a vulnerable state. We encourage you to review your agents to ensure you are now utilizing our latest AV6 agents. Reminder that our online help for Security Manager is available for your reference.
Windows 8.1/Windows Server 2012 R2	As older Windows Server and Desktop Operating Systems transition into Microsoft's Extended Support Phase and beyond, they are no longer receiving OS level TLS version and cipher updates (SCHANNEL). As the .NET Framework relies on SCHANNEL for TLS based communications, and as newer vulnerabilities are discovered in the ciphers available to these older Operating Systems, the available Strong Cipher list for these devices continues to shrink. We continually review the ciphers used by N-central's Modern Security Profile, to ensure we offer only secure ciphers. At this time, there are only two (2) secure RSA key based ciphers available to Windows Server 2012 R2/Windows 8.1 and older. N-central will endeavor to support these two ciphers in our Modern Security profile for as long as they remain secure, but there may come a time where we will need to drop Official support for these Windows versions before the end of their Extended Support Phase. If/when this does occur, they will still be able to connect if you switch to the Legacy Security Profile, but this will reduce the security of all devices connecting to your N-central server. If you monitor Windows Server 2003/2008/Windows XP/Vista devices, we would like to advise you that we will be dropping support for the "TLS_RSA_WITH_3DES_EDE_CBC_SHA" cipher

	in a future release. Coming changes to the web front end that will support TLS 1.3, have been identified as also disabling "TLS_RSA_WITH_3DES_EDE_CBC_SHA" due to the required version of OpenSSL. Fully patched Windows Server 2008/Vista devices *should* be able to connect to N-central on the Legacy Security profile, using one of the newer, but still weak ciphers. Windows Server 2003/XP will no longer be able to communicate over TLS/HTTPS at that time (using a site-to-site VPN between your firewall devices, and connecting over HTTP may still work).
32-bit versions of the Windows, Linux and macOS operating systems	The number of 32-bit Operating Systems monitored by N-central has continued to drop over the past few years. Windows Agents/Probes have historically been 32-bit, with some 64-bit specific components. In a future release, we intend to convert the Agent and Probe code base to be a native 64-bit application; this will mean a hard deprecation of support for 32-bit Windows versions. N-central's Linux and macOS agents will follow a similar path.

N-able N-central System requirements

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

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

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

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

System requirements by number of devices managed

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

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

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

Notes

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

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

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

Subsystem	Limit
Maximum memory	12TB
Maximum logical CPUs	768

Examples of supported servers

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

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

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

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

Support for virtualized environments

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

Hyper-V on Windows Desktop Operating Systems not Supported.

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

Windows Server Semi-Annual Releases are not Supported.

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

About virtualization

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

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

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

Recommended configuration for the virtualized server

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

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

Supported Software

Browsers

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

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

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

Remote Control

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

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

Report Manager

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

Automation Manager

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

SNMP Community String

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

Supported Operating Systems

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

Windows Agents:

- Microsoft .NET Framework 4.5.2 (or later)

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

Windows 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

Windows 8 and 8.1

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

Windows 7

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

macOS Agents

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

Linux Agents

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

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

- Red Hat Enterprise Linux/CentOS 8 (64-bit)
- Red Hat Enterprise Linux/CentOS 7 (x86_64 and i686)
- Red Hat Enterprise Linux/CentOS 6 (x86_64 and i686)
- Ubuntu 20.04 LTS (64-bit)
- Ubuntu 18.04 "Bionic Beaver" (x86_64)
- Ubuntu 16.04 "Xenial Xerus" (x86_64 and i686)
- Debian 8.7/Ubuntu 14.04 "Trusty Tahr" (x86_64 and i686)

AV Defender

Workstation Operating Systems

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

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

- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 10 Home Edition
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows 11 Home Edition (Monitoring status is supported)

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

Networking Requirements

On-Premise: Set up port access requirements

N-central Server

Access must be permitted to the following ports:

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

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

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
					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 ■ 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 (out- bound) to monitor Backup Exec jobs. ⓘ Inbound from the local LAN and not the Internet.

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
	* 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. Inbound from the local LAN and not the Internet.
8443	√	√		√	The default port for the N-central UI. Port 8443 is the TCP port needed for SSL (HTTPS) connections. The firewall must be configured to allow access from the Internet to this port on the N-able N-central server. This port must also be open for outbound traffic if the N-able N-central server is monitoring the HTTPS service on a managed device.
8800		√			The Feature Flag System in N-able N-central needs to talk to mtls.api.featureflags.prd.sharedsvcs.system-monitor.com. Used by N-able – generally during Early Access Preview and Release Candidate testing – to enable and disable features within N-able N-central.

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

Mobile Device Management (MDM)

The table below outlines the TCP open port configurations required to send/receive push notifications for MDM.

Port Number	Port Location				Description
	N-able N-central Server		Target Network Server		
	Inbound	Outbound	Inbound	Outbound	
80		√	√		
443		√	√		

Port Number	Port Location				Description
	N-able N-central Server		Target Network Server		
	Inbound	Outbound	Inbound	Outbound	
2195		√			Access to ports 2195 and 2196 must be granted to gateway.push-apple.com.akadns.net.
2196		√			
5222			√		
5223			√		
5228			√		TCP and UDP mode.

AV Defender

Ports used for AV Defender and other services include:

Port	Source/Destination	Description
80	submit.bitdefender.com	Port used for submitting endpoint dumps in case of crashes.
	update-solarwinds.2d585.cdn.bitdefender.net	Bitdefender update server.
	upgrade.bitdefender.com	Bitdefender upgrade server.
	lv2.bitdefender.com	License validation.
53	*.v1.bdnsrt.org	DNS requests for signature update checks.
7074	Update Server	Downloading updates from local Update Server. An update server cannot acquire updates from another local Update Server; it is not possible to cascade them.
443	avc-fu.nimbus.bitdefender.net	Antimalware behavior scanning with Bitdefender Cloud servers.
	nimbus.bitdefender.net/elam/blob	Early Launch Anti-Malware (ELAM) cloud server.
	elam-fu.nimbus.bitdefender.net/submission	Submission to Bitdefender cloud servers of unrecognized applications by Early Launch Anti-Malware (ELAM) module.
	nimbus.bitdefender.net	Antimalware, antiphishing and content control scanning with Bitdefender Cloud servers.

The Probe automatically creates firewall rules for these ports.

To ensure signature updates and minor updates to AV Defender can occur, ensure that DNS and outbound TCP port 80 access to http://upgrade.bitdefender.com are available through the firewall.

Report Manager

You can also configure N-able N-central to communicate with Report Manager over port 80 or 443. If you choose 443, you must setup the proper SSL certificate.

Configure the external and internal addresses by opening the Report Manager administration console and clicking **System setup and logs** > **Server IP Configuration** and setting the **External** and **Internal** IP address.

The internal address or FQDN must be accessible from N-able N-central over port 1433 and either port 80 or 443.

Remote Desktop

When using Remote Desktop for remote connections, configure the following ports:

- On the Operator Machine:
  - TCP 443 outbound (required)
  - TCP 22 outbound (recommended for best remote control experience) to N-central
- For the Target Machine/Probe:
  - TCP 443 outbound (required)
  - TCP 22 outbound (recommended for best remote control experience) to N-central
- For the Probe:
  - If using a probe as the connecting device, it must be able to reach the Target Machine on port 3389 (or custom port if specified) on the local network (and N-central as above).

Take Control

The ports identified in the tables below must be accessible for Take Control (MSP Anywhere) remote control connections.

Mac OS uses TCP Mode only.

TCP Mode (Required)

If the agent has a direct TCP port configured, the same port must be open at the agent's firewall and be accessible by the viewer.

Port Number	Port Location			
	Take Control Viewer		Target Device	
	Inbound	Outbound	Inbound	Outbound
Port 80		√		√
Port 443		√		√
Port 3377 Take Control fails over to this port as an alternative connection method.		√		√

When using Take Control, the N-able N-central server, remote endpoints, and devices running the Viewer (those devices that are used to establish the remote session) must be able to resolve and reach hosts with the following domain names:

- `*.n-able.com`
- `sis.n-able.com`

The following domain also needs to be resolved for update downloads:

- `swi-rc.cdn-sw.net`
- `*.beanywhere.com`
- `mspa.n-able.com`
- `*.pubnub.com`

UDP Mode (Optional)

Take Control can use the UDP transmission model to connect to devices in addition to TCP.

Initially, the Take Control viewer requires access to port 1234. After the system administrator modifies the firewall to enable the identified IP addresses to communicate with the server, the ports can be random.

Port Number	Port Location			
	Take Control Viewer		Target Device	
	Inbound	Outbound	Inbound	Outbound
Port 1234		√		√
Port 1235		√		√

- BASupApp.exe
- BASupTSHelper.exe
- agent.exe
- AgentMaint.exe
- NCentralRDViewer.exe
- BASEClient.exe

Backup Manager

Port 443 TCP outbound. It is almost always open on workstations but may be closed on servers.

Local port 5000. If this port is unavailable, the Backup Manager detects a free port automatically (starting from 5001, 5002 and up).

In most cases, no firewall configuration is required.

NetPath

Port/Type	Protocol	Source	Destination	Description
Type: 11 (ICMP Time Exceeded)	ICMP	Networking devices along your path	NetPath probe	Used by NetPath probe to discover network paths.
Port: User Configured	TCP	NetPath agent	Path destination	Used by NetPath probe to discover the service status over the entered path port.
Port 43	TCP	Main polling engine	BGP data providers	Used by NetPath to query IP ownership and other information about the discovered IP addresses.

Ports for Support

Port Access Requirements

For N-able Technical Support to troubleshoot and diagnose your issue, you will need to permit the following incoming connections to N-able N-central:

- TCP Port 22 (SSH) used for Remote Control sessions and by N-able Support.
- TCP Port 80 (HTTP) UI and agent/probe communication.
- TCP Port 443 (HTTPS) UI and agent/probe communication.
- TCP Port 10000 (HTTPS) is used for the Administration Console.

The following outbound access is required from your N-able N-central server to troubleshoot it:

- TCP Ports 20, 21 (FTP) for backing up N-able N-central and by N-able Support to update their tools.
- TCP Port 25 (SMTP) for sending email from N-able N-central if not using a local mail relay.
- TCP/UDP Port 53 (DNS) is used for DNS lookups.
- TCP/UDP Port 123 (NTP) to keep the N-able N-central server clock in sync.
- TCP Port 1433 is used by N-able N-central to export data to Report Manager if enabled.

Required inbound access IPs

N-able Support

Open access to all the listed IP addresses. Although most Support connections will come from your local Support office, some shifts are covered by other offices.

Americas

- 32.60.115.209-222 – Ottawa, Ontario, Canada (Support and Development)
- 207.35.253.229 – Ottawa, Ontario, Canada (Support and Development)
- 209.120.234.64-79 – Ottawa, Ontario, Canada (Support and Development)
- 216.85.162.34 – Durham, North Carolina, United States of America (Support)
- 4.35.232.2 – Durham, North Carolina, United States of America (Support)
- 174.99.133.19 – Durham, North Carolina, United States of America (Support)
- 4.7.118.146 - Durham, North Carolina, United States of America (Support)

APAC

- 122.53.149.180 – Manila, Philippines (Support)
- 122.53.149.190 – Manila, Philippines (Support)
- 120.28.59.197 – Manila, Philippines (Support)
- 122.3.252.208/28 – Manila, Philippines (Support)
- 180.232.22.208/29 – Manila, Philippines (Support)

EMEA

- 62.253.153.163 – Dundee, Scotland (Support)
- 212.187.250.0/28 – Dundee, Scotland (Support)
- 62.28.208.190 – Lisbon, Portugal (Support and Development)
- 62.209.223.224-255 – Brno, Czech Republic (Development)
- 82.113.44.0-31 – Brno, Czech Republic (Development)
- 128.140.241.11 – Minsk, Republic of Belarus (Development)
- 78.11.93.114 – Krakow, Poland (Development)
- 82.177.176.130 – Krakow, Poland (Development)

Mothership monitoring, licensing updates and renewals

- mothership.n-able.com - Primary Mothership Monitoring
- mothership2.n-able.com - Supplemental Mothership Monitoring
- licensing.n-able.com - Activations, License Renewals, License Updates

Required Outbound Domain Access

The N-able server must be able to resolve and access over FTP - TCP ports 20, 21, UDP ports above 1024 for Passive Transfer, the following domain name:

- send.n-able.com

The N-able N-central server must be able to resolve and access over TCP port 80 (HTTP) and 443 (HTTPS), the following domain name:

- sis.n-able.com

The N-able N-central server must be able to resolve and access using HTTPS TCP port 443, the following domain names:

- update.n-able.com
- feeds.n-able.com
- servermetrics.n-able.com
- push.n-able.com
- scep.n-able.com
- licensing.n-able.com
- updatewarranty.com
- microsoft.com
- https://keybox.n-able.com
- https://ui.netpath.n-able.com

Hosted & On-Premise: Set up the firewall to allow traffic to domains

To ensure the flow of information between the N-able N-central server and outside sources, ensure the following domains and URLs are added to your firewall allow list. These domains are needed for outbound communication.

send.n-able.com	The N-able internal FTP server where a partner can upload and download files such as logs, executables and scripts. This is also the location where you download scripts from Scripto for additional troubleshooting tools for N-able N-central. Ports required: TCP 20 and 21, ports above UDP 1024 for passive transfer.

sis.n-able.com	A repository of XML files. Each XML lists download links for .exe, patches and so on. For example, when the agent is installed on a device and it needs to download AV Defender, the agent goes to http://sis.n-able.com/GenericFiles.xml and get the link to download the files compatible for the agent version. Port required: HTTP (80) and HTTPS (443)
All domains below require port TCP 443.	
update.n-able.com	The location where N-able N-central obtains the NSP file for upgrade. It also has .ISO, vdh.gz files for a N-able N-central installation. There is also an alias of this domain at releases.n-able.com.
feeds.n-able.com	The location where the N-able N-central gets RSS feeds.
sis.n-able.com	A repository of XML files. Each XML lists download links for .exe, patches and so on.
servermetrics.n-able.com On-Premise only	When an N-able N-central server is installed, all information about it is sent to the N-able internal Activation Server.
licensing.n-able.com On-Premise only	Once the N-able N-central server is validated, it communicates with the internal Activation Server to get the full license depending on the contract details.
push.n-able.com	Used for Apple Push Notification service (APN) and CSR certificate request for Mobile Device Management.
scep.n-able.com	Used for MDM installation, pushing profile to the target device
updatewarranty.com On-Premise only	Used by N-able N-central to check the warranty expiration dates of managed devices.
microsoft.com	Used For Windows Update, which is needed for Patch Management or any other patch solution software.
https://keybox.n-able.com	Used with Netpath, EDR and future integrated components.
https://keybox.solarwindsmsp.com	Used with Netpath, EDR and future integrated components.
*.sentinelone.net	Used by EDR.
https://api.ecosystem-middleware.eu-central-1.prd.esp.system-monitor.com	Used by Microsoft Intune.

https://api.ecosystem-middleware.eu-west-1.prd.esp.system-monitor.com https://api.ecosystem-middleware.us-west-2.prd.esp.system-monitor.com https://api.ecosystem-middleware.ap-southeast-2.prd.esp.system-monitor.com https://ui.ecosystem-middleware.prd.esp.system-monitor.com/	
api.ecosystem-middleware.eu-east-1.prd.esp.system-monitor.com api.ecosystem-middleware.us-west-1.prd.esp.system-monitor.com	Middleware endpoints.
rest.ecosystem.ap-southeast-2.prd.esp.system-monitor.com rest.ecosystem.eu-east-1.prd.esp.system-monitor.com rest.ecosystem.eu-west-1.prd.esp.system-monitor.com rest.ecosystem.us-west-1.prd.esp.system-monitor.com	Rest endpoints.
grpc.ecosystem.ap-southeast-2.prd.esp.system-monitor.com grpc.ecosystem.eu-east-1.prd.esp.system-monitor.com grpc.ecosystem.eu-west-1.prd.esp.system-monitor.com grpc.ecosystem.us-west-1.prd.esp.system-monitor.com	GRPC endpoints.
cdn.pendo.io data.pendo.io	Used by Pendo to receive data. Port required: HTTPS (443)

pendo-io-static.storage.googleapis.com pendo-static*.storage.googleapis.com	

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 2022.3 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.