



N-central

Release Notes

Version: 2022.8 (Build: 2022.8.0.14)

Last Updated: Wednesday, December 7, 2022



What's New in N-able N-central 2022.8

What's new in N-central 2022.8

N-central 2022.8 includes over 80 fixed items, an important addition to Patch Management profiles, an update to Take Control behavior, and a new feature in preview!

New Patch Profile Option!

New to N-central 2022.8 is an option in Patch Profiles regarding upgrades to our Patch Management Engine (PME).

PME installation profiles allow the choice of the General Availability or Release Candidate version of Engine installed on the devices associated to that patch profile. The two options are:


- General Availability (GA): The default option, which installs the most current version of PME.
- Release Candidate (RC): The non-default option, which installs a functional preview of the next PME version.

The Release Candidate option is ideal for testing the upcoming PME version in advance to ensure everything is working to your standards. After an RC version is determined to be stable after a few weeks of release, we will promote it to GA, which will auto-update on all devices. Release Candidate Agents undergo extensive testing before you can download them, but if you choose to download an RC Agent, it may include some minor bugs.

Third Party Patch (TPP) applications will behave similar to PME, where there will be both a GA and an RC version for Third Party Patches. If you select to install the GA version of PME, you will also be selecting the GA version of TPP, and likewise for the RC version.

Integrated Take Control - Connection without Take Control heartbeat now possible!

In N-central 2022.8, we've made it easier for you to get a Take Control session started, even if N-central hasn't received a heartbeat from the device. If the Take Control heartbeat isn't available, when you hover over the remote control icon in the All Devices view, you will see a message that indicates how long since N-central has seen a Take Control heartbeat and that your connection may not succeed.

 Please note that this change means that the remote control icon will be green for more situations than it was previously. If you have been relying on the Remote Control icon to tell you if a device is entirely offline, or just if the N-central agent isn't checking in, you'll want to start relying more on the Status icon for the device, and attempt a remote control session to verify if the device is entirely offline or not.

Securely Access the N-central Administration Console (preview)

A new feature in preview for 2022.8 allows your N-central server's administration console to be part of the regular user interface, rather than only being available on port 10000. With this change, you'll also be able to secure the Product Administrator account with MFA, all of the time!

If you are interested in testing this important security enhancement, please email ncpreview@n-able.com once your On-Premise N-central server has been upgraded to 2022.8.

Ubuntu 22.04 agent

New to N-central 2022.8 is support for Ubuntu 22.04 agent installation. You'll find this new agent available from the [Download Agent/Probe software page](#).

New Pendo Onboarding Guides and tooltips

If you're a newly-added user to N-able N-central, take advantage of our new onboarding guides and tooltips.

See [Onboarding Guides and tooltips](#) for details!


New Cove Dashboard in N-central!


Introducing the new main Cove dashboard in N-Central. The Backup dashboard has a similar design to the Recovery dashboard and includes:

- a dedicated donut chart for Microsoft 365 management
- new filters selection panel
- new columns management

Enhanced DNS Filtering

We've made usability improvements to the DNS Filtering Insights user interface and well as other improvements throughout the user interface.

 We have been recently made aware of an issue in N-central 2022.8.0.14 where RDP connections do not connect properly. Take Control sessions are not affected. We are actively working on a solution. In the meantime, there is an agent side code drop available to use on Windows devices, with an N-central agent installed, where Take Control isn't an option. If you need this temporary solution, please log a case with Support referencing NCCF-49091.

 We have recently been made aware of an issue in N-central 2022.8 that stops export to Report Manager after upgrades. If you are using Report Manager with N-central and have upgraded to 2022.8 or are planning to upgrade soon, please log a case with Support referring to NCCF-49480. This fix will be included in the next release of N-central.

Upgrade paths and notes

i After the upgrade to N-central Version: 2022.8, an additional restart of the Windows Agent Service, Windows Agent Maintenance Service, and Windows Software Probe Service (Manually or Scheduled Task) or a full device reboot (not hibernate or sleep) may be required on Windows devices with misconfigured AMP-based services in order for them to go back to Normal state.

Upgrade versions

To upgrade to N-able N-central 2022.8, 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 2021.2.0.140+
- 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+
- N-able N-central 2022.4.0.6+
- N-able N-central 2022.5.0.6+
- N-able N-central 2022.5.1.33
- N-able N-central 2022.5.2.35
- N-able N-central 2022.6.0.20+
- N-able N-central 2022.7.0.22+
- N-able N-central 2022.8.0.12+

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

i 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 restart of the device is pending.

i **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



Fixed Issues in N-able N-central

Release 2022.8 GA

Category	Description	Bug
Core	Direct Support option disappears when creating new device with class Workstations - Mac CORE	NCCF-44658
Core	Port :10000 /admin should be disabled when the NAC integration is enabled	NCCF-44808

Release 2022.8 RC

Category	Description	Bug
Core	Monitoring Processes are missing for the Mac agent	NCCF-43095
Core	Allow Take Control Connection even if heartbeat is not received	NCCF-40646
Core	'ScriptDownloadURI' Version Not Updating After Upgrading of N-central	NCCF-40053
Core	Parent Level View - Permission Evaluation is not performed for lower levels	NCCF-39485
Core	PatchApproval has actionDate set as null	NCCF-39060
Core	RPM Error with the new Ubuntu 22.04 Agent	NCCF-38585
Core	Fix PatchApprovalLog scraping logic	NCCF-38535
Core	Probe fails to install N-central Agent on the same device	NCCF-38236
Core	Agent download labels incorrect	NCCF-38026
Core	Review and adjust synchronized method in EventBufferController	NCCF-38023
Core	Include customer and device history tables as well as regular when scraping	NCCF-37086
Core	Adjust event service watchdog to monitor heartbeat of executor service	NCCF-37913
Core	Add statistics on indicating completed customer event scrape	NCCF-37761
Core	When acknowledgementcontroller shuts down and resets counts it needs to notify observers	NCCF-37512

Core	The parameters table should be filtered to patch data	NCCF-37456
Core	Collect stats on live eventing executor service queue	NCCF-37455
Core	Watchdog restart service is not triggering a restart when component appears offline	NCCF-37454
Core	Scraping customer filter should include all customers deleted or not	NCCF-37085
Core	Probe cannot install Linux and new Mac agents	NCCF-36534
Core	Interrupt exception can cause event processing and/or acknowledgement processing to stop permanently and needs a watchdog	NCCF-36410
Core	After n-central upgrade from version which contains old Linux agents to n-central where old agents are deprecated the links to old agents are visible on Download Agent/Probe page	NCCF-36295
Core	Collect stats on eventing service restarts	NCCF-36887
Core	Ensure time series tables are not processed for scraping unless within 24h	NCCF-35851
Core	Memory consumption is too high when buffering events	NCCF-35840
Core	File Ownership on Openfire and Envoy are Different Depending on Upgrade or New Install	NCCF-35500
Core	LinkedBlockingDeque performance is bad in AcknowledgementController and PersistedEventBuffer class	NCCF-35492
Core	Billing Profiles Not Saving	NCCF-34519
Core	[Usability] Add Windows 10 Pro for Workstations to Filters	NCCF-34389
Core	Use TLS protocol instead of SSL 3.2 in Linux libmodule.so shared library	NCCF-34193
Core	Add Devices Wizard. Seeing Customer Specific Agent available on drop down instead of System Specific.	NCCF-33020
Core	[Command] Restart Device	NCCF-32001
Core	[Command] Shut Down Device	NCCF-32000
Core	Front end menu to issue commands in All Devices	NCCF-31994
Core	N-central Page Title Must be Updated When Selecting Different	NCCF-30599

	NAC Pages	
Core	Modify the NAC Angular Code to Support Loading Pages from the N-central Nav Menu	NCCF-30022
Core	Update the "Agent tab"Page with Ubuntu 22.04	NCCF-29190
Core	Update the "Add Devices Wizard" with Ubuntu 22.04	NCCF-29189
Core	NAC Data Export configuration settings not decrypted from database	NCCF-29162
Core	Probe discovery of Ubuntu 22.04 devices	NCCF-28101
Core	Update the "Download Agent/Probe" Page with Ubuntu 22.04	NCCF-28099
Core	Push Third Party Task Reports Success but Application fails to install	NCCF-27981
Core	Duplicate save network setting call logged In dmsservice.log when customuiport feature flag is on	NCCF-27885
Core	Having a lot of Customers and Sites, it can cause high garbage collection or out of memory problems	NCCF-27271
Core	Fix Jetty JVM gc.log not rolling over except on Jetty restarts	NCCF-24449
Core	Notification profile generated multiple tickets	NCCF-22741
Core	Clean Up Old Admin Console Code	NCCF-21343
Core	Modify Pages related to Services for Admin Console	NCCF-21340
Core	monitor.pl Causes Performance Issues on Servers with Large applianceTask Tables	NCCF-21703
Core	SYSTEM ERROR when user tries to reset it's own 2FA	NCCF-20862
Core	[FEATURE] Support Ubuntu 22.04 LTS	NCCF-19869
Core	Custom Services: Allow For the Configuration Of The MaxInstances Value	NCCF-17330
Core	Optimize the ServerUI:patchApprovalValidate API call	NCCF-16834
Core	The Linux/Mac code sometimes returns 32-bit for 64-bit OSs	NCCF-16219
Core	Probe MSI upgrade no longer functional due to lack of credentials	NCCF-15093

Core	Locking the "MFA Not Required" Option Isn't Being Saved	NCCF-15617
Core	Agent version not updated on 32bit Windows Apps & Feature panel after upgrade	NCCF-14924
Ecosystem Framework	When a managed device's warranty expiry date on N-central updates from an Asset Scan or from manually setting the warranty expiry on the device, EDR or other integrations will get uninstalled.	KUIP-4432
Ecosystem Framework	Add additional server side debug logs to S1 Agent upgrade task	KUIP-4180
Ecosystem Framework	Make Software Upgrade scheduled task cron configurable via server properties	KUIP-4179
Ecosystem Framework	Update Ecosystem server side to read new global entities and configurations for msi or exe package upgrade type.	KUIP-4166
Ecosystem Framework	Searching for list of devices with enabled DNSF hits Postgres limitations for IN clause	KUIP-4102
Ecosystem Framework	Circuit breaker to reduce back-pressure from the Keybox	KUIP-3735
Ecosystem Framework	License - EDR Control not Complete which has a cron job making it replicate Control	KUIP-3733
Ecosystem Framework	MS Intune integration icon shows enabled even when not being used - Dev Work	KUIP-2898
Integrations	The Content F and Block Page entries are not deleted when assigned to a Profile used in a Deployment Site	INT-1018
Patch Management	Implement Agent renaming and logic for default profile and RC profile	PMCM-2057
Patch Management	Implement N-central Patch Profile changes in order to support RC release of PME	PMCM-919
Patch Management	N-Central Crashes when you attempt to re-add patch classifications or products to an Automatic Patch Approval.	PMCM-415
Patch Management	[FEATURE] Patch Management Engine (PME) Upgrade Options	PMCM-426

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 <i>"KBA20020: Configuring A Server With Multiple NICs"</i> in the online Help.	67778
There is a known issue on the Mac Agent where the CPU and Memory graphs are not being displayed via Direct Support. This issue is being resolved and will become available in an upcoming release.	NCCF-43803

Automation Manager

Description	Bug
Running Automation Manager Policies created using Automation Manager 1.6 or earlier may result in <code>Failed to create an EndDate ... errors</code> 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 <code>c#/l.net</code> 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	NCCF-11842

Description	Bug
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.	
HDM does not work with the "Last 5 Tickets" widget.	NCCF-10855
Warranty information might be inaccurate when determining the warranty expiry dates of devices that are not located in the USA.	NCCF-3649
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
We have recently been made aware of an issue that has existed in N-central since N-central 12.2, where the Asynchronous Restore method will not properly restore historical data. We are actively working on a fix for this, and anticipate this fix being included in a future release of N-central. Until this issue is fixed, we strongly recommend not using the Asynchronous Restore method in production environments or Disaster Recovery situations. Please refer to https://success.n-able.com/kb/nable_n-central/N-central-Asynchronous-Restore-Not-Working for further information.	NCCF-43101

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

End of support

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

Transport Layer Security (TLS)	N-able N-central now disallows traffic over TLS 1.0 and TLS 1.1. This causes any Windows Agents or Windows Probes that are running on Windows XP and Windows Server 2003, as well as pre-v12.1 versions of the MacOS agent, to lose the ability to communicate with your N-able N-central server. We strongly recommend using a Windows Probe to monitor those devices.
Linux Agent Support	Due to declining usage in the field, N-able N-central Linux agents no longer support CentOS 6, Ubuntu 14.04, and the 32-bit version of Ubuntu 16.04.
Internet Explorer 11	Due to declining usage in the field, a future release of N-able N-central will drop support for the Internet Explorer 11 web browser.
AV Defender 5.x	As of next major release for those of you still utilizing the AV5 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	<p>The physical server used to install N-able N-central in a bare metal environment must be certified to run Red Hat Enterprise Linux 7.7 (x64) by Red Hat, or the hardware vendor, without any additional drivers. Please check the Red Hat Hardware Ecosystem for details.</p> <p>Server Grade hard drives connected to a RAID controller with a Battery/Capacitor Backed Cache are Required. Examples include 10K+ RPM SCSI or SAS drives, Enterprise Grade SSDs or NVMeS for bare metal and virtualized hosts, or a Fibre Channel connected SAN with Enterprise Grade hard drives for virtualized hosts (<i>Fibre Channel cards can be used for bare metal if they are configured in the pre-boot environment and do NOT require vendor-provided drivers</i>).</p> <p>Although Desktop Hard Drives will work with the Operating System, they do not meet the minimum throughput required for the back-end Database of N-able N-central.</p>

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

System requirements by number of devices managed

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

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

Number of Devices	CPU Cores	Memory	Storage
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 NVMe. 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



Subsystem	Limit
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 7.7 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	<p>It is impossible to guarantee the scalability or performance of a N-able N-central server deployed on a Virtual Machine due to:</p> <ul style="list-style-type: none"> ▪ variability in field environments resulting from host server configurations, ▪ the number of virtual guests run on the host server, and ▪ the performance of the underlying host hardware.
Supportability	<p>N-able supports N-able N-central software deployed on VMWare ESX/ESXi 6.0 or newer, Windows Server 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.</p>

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

Recommended configuration for the virtualized server

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

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

Supported Software

Browsers

N-able N-central supports the latest 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 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)
- Ubuntu 20.04 LTS (64-bit)
- Ubuntu 18.04 "Bionic Beaver" (x86_64)
- Ubuntu 16.04 "Xenial Xerus" (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 LTSC	Windows 10 Enterprise 2016 LTSC



Windows 10 Enterprise for Virtual Desktops	Windows 10 Enterprise LTSC 2019
Windows 10 Pro	Windows 10 Pro Education
Windows 10 Pro for Workstations	
Windows Server 2008 R2 Enterprise	Windows Server 2008 R2 Datacenter
Windows Server 2008 R2 Standard	Windows Server 2008 R2 Foundation
Windows Server 2012 Datacenter	Windows Server 2012 Essentials
Windows Server 2012 Foundation	Windows Server 2012 R2 Datacenter
Windows Server 2012 R2 Essentials	Windows Server 2012 R2 Foundation
Windows Server 2012 R2 Standard	Windows Server 2012 R2 Standard Evaluation
Windows Server 2012 Standard	
Windows Server 2016 Datacenter	Windows Server 2016 Datacenter Evaluation
Windows Server 2016 Essentials	Windows Server 2016 Standard
Windows Server 2016 Standard Evaluation	
Windows Server 2019 Datacenter	Windows Server 2019 Essentials
Windows Server 2019 Standard	Windows Server 2019 Standard Evaluation
Windows Server Datacenter	
Windows Small Business Server 2011 Essentials	Windows Small Business Server 2011 Standard

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	√	√		√	<p>HTTP - used for communication between the N-able N-central UI and agents or probes (including MSP Connect and MSP Anywhere).</p> <p>The firewall must be configured to allow access from the Internet to this port on the N-able N-central server.</p> <p>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.</p>
<p>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.</p>					
123		√			Used by the NTP Date service which keeps the server clock synchronized. Normally using UDP (although some servers can use TCP).

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
135			√		<p>Used by Agents and Probes for WMI queries to monitor various services.</p> <div style="border: 1px solid #0070C0; padding: 5px;"> <p>i Inbound from the Windows Probe to the Windows Agent.</p> </div>
139			√		<p>Used by Agents and Probes for WMI queries to monitor various services.</p> <div style="border: 1px solid #0070C0; padding: 5px;"> <p>i Inbound from the Windows Probe to the Windows Agent.</p> </div>
443	√	√		√	<p>HTTPS - used for communication between the N-able N-central UI and Agents or Probes (including MSP Connect and MSP Anywhere).</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Used by Agents and Probes for XMPP traffic. Outbound access to port 443 for Managed Devices is recommended but not required.</p> <p>To activate EDR the N-able N-central server needs outbound HTTPS access to port 443 and the following domains:</p> <ul style="list-style-type: none"> ■ *.sentinelone.net ■ sis.n-able.com

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
					<ul style="list-style-type: none"> keybox.solarwindmsp.com <p>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:</p> <ul style="list-style-type: none"> 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		*	*	*	<p>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.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Inbound from the local LAN and not the Internet.</p> </div>
<p>* 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.</p>					

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
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. <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> i Inbound from the local LAN and not the Internet. </div>
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 <code>mtls.api.featureflags.prd.sharedsvcs.system-monitor.com</code> . 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	√				<p>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.</p> <p>N-able recommends excluding all other inbound traffic to port 10000 except from N-able Ports for Support section below.</p>
10004			√	√	<p>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.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Inbound from the local LAN and not the Internet.</p> </div>
15000			√	√	<p>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.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Inbound from the local LAN and not the Internet.</p> </div>

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 2022.8 uses the 7-Zip file archiver for installing agents and probes. 7-Zip is free software redistributed under the terms of the GNU Lesser General Public License as published by the Free Software Foundation. For more information, see <http://www.7-zip.org>.

Customer Support

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

Web Page:	http://www.n-able.com
Technical Support Self-Service Portal:	https://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



© 2022 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.

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

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

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

About N-able

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