N-ABLE™

N-central

Release Notes

Version 2022.5 (Build: 2022.5.0.16)

Last Updated: Wednesday, July 6, 2022

What's New in N-able N-central 2022.5

Announcing the GA of N-central 2022.5

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.

New in N-central 2022.5

The 2022.5 version of N-able N-central is jam-packed with new features, continuing previews, and security fixes. Read on for more details!

Support for External Identity Providers!

N-central 2022.5 introduces the preview of support for external identity providers. Any identity provider that supports OpenID Connect will work – most popular among these is Microsoft Azure! This feature can be configured at the System, Service Organization, Customer and Site levels. If you would like to help us field test this new feature, please email ncpreview@n-able.com

Expanded Preview of the New Mac Agent!

The new MacOS agent remains in preview. However, there is additional functionality for it in 2022.5:

- Available for probe and discovery job-based installations
- A generic version of the new MacOS agent remains available to download as it did in 2022.3 while your customer and site levels will show a customer specific version of this agent.
- Previous installations of the new Mac agent will continue to upgrade to the new MacOS agent no matter the feature flag setting.

If you do not request to preview the new Mac agent, you will NOT be able to use the new features or see the new MacOS agent for download. Should you wish to help us out and provide feedback on this new Mac agent, please email ncpreview@n-able.com

Intune Logout

We know that setting up Intune integration in N-central can become a pain point if your credentials need to be changed. N-central 2022.5 now includes a Logout button so you do not need to contact Support if your credentials or tenant model need to be changed!

Continuing the Preview of the Custom UI Port Feature

Several bug fixes related to the Custom UI Port feature are included in N-central 2022.5 – please see the detailed list below. The feature is staying in preview until we have all the fixes included. If you are interested in trying out this feature, please email *ncpreview@n-able.com*.

You can use Safari!

We have adjusted how the login page of N-central works so that you can more easily use Safari to access N-central.

Upgrade paths and notes

Notice to partners

We are advising any partner who sees problems with their probes not upgrading to 2022.5 to perform the following steps to update the credentials used by the probe during the upgrade process.

Perform the following steps at the Customer/Site levels (in most cases, due to different customers or sites using different domains/usernames/passwords):

1. Navigate to **Administration** > **Defaults** > **Agent & Probe Settings**.
2. On the **Credentials** tab, enter the domain/username and password that the probe should be using, and then select both Propagate boxes.
3. Click **Save**.

Please note the following points:

- This credential change should not impact the regular monitoring performed by your agents and probes.
- These new credentials will be used for scheduled tasks that specify Device Credentials in their configuration.
- Keep in mind that the probe credentials need elevated privileges, as laid out in https://documentation.n-able.com/N-central/userguide/Content/Deploying/probe_privilege_levels.htm.
- You should be providing the same credentials here as you would when installing or reinstalling the probe.
- While the credentials are securely stored within N-central for reuse, the credentials are not kept on the upgrading probe.
- If your probe that isn't upgrading also is not checking in, reinstalling the probe using the System/Generic probe installer, and its activation key, is the recommended remediation action.

Important: After the upgrade to N-central 2022.5, 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) is 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 2022.5, 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
- N-able N-central 2022.4.0.6+
- N-able N-central 2022.5.0.6+

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

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 2022.5

Category	Description	Bug
Core	Scheduled task is not retaining the settings for Missed Executions	NCCF-28827
Core	Azure-core dependency failed on legacy version	NCCF-29026
Core	Security Profile Switching Scripts for Modern and Legacy profiles have their UI config profiles reversed.	NCCF-28132
Core	N-central GUI inaccessible after restore despite services running	NCCF-28131
Core	Remote Desktop with Custom UI Port Does Not Work with HTTPS tunnel	NCCF-25585
Core	MDM Connections Being Blocked by Custom UI Port	NCCF-23257
Core	reboot_dialog_logo.png Not Download When Using Custom UI Port	NCCF-23196
Core	Direct Support user actions fail if Custom UI Port is enabled	NCCF-23139
Core	Direct Support disabled on Mac devices after license mode change	CALM-455
Core	Windows Agent not upgrading when file handle is left open	NCCF-25018
Core	The Certificate Chain for Envoy is not Getting Updated when a New Certificate is Uploaded to N-central	NCCF-24464
Core	The "Take Control Is Not Installed" Warning Message Appears Even Though The Take Control Viewer Is Installed, if a Custom UI Port is enabled	NCCF-22915
Core	Custom Protocol Handler is crashing on client PC when WMI service is turned off during RDP connection attempt	NCCF-21702
Core	Unable To Access N-central With The Safari Web Browser	NCCF-19768
Core	Add Missing Security Headers to Static Envoy Pages	NCCF-17521
Core	Version Number Missing from Security Manager Hover-over	IAV-1888

Category	Description	Bug
Core	Further integration and introduction of the new Mac agent	NCCF-20017
Core	Upgrade Openfire to Version 4.7.x	NCCF-9527
Core	Correct Login Flow	NCCF-28828
Core	Login flow with branded URL	NCCF-29182
Core	Misconfigured Automation Manager Services	AM-2885
Core	AM Agent service should be stopped on NC Agent/Probe shutdown for N-central version 2022.3	AM-2893
Core	Probe Upgrade Improvements	NCCF-27733
Core	Release Request: CT2 - Bug fix for Custom UI port not reflected in the password change email URL	NCCF-28192
Core	Java Security configuration update rejects SHA1RSA Root CA certificates	NCCF-29752
Core	Update to Upgrade Paths	NCCF-29601
DNS Filter	The Content F and Block Page entries are not deleted & replaced when assigned to a Profile used to a deployed & running Roaming Client	INT-813
DNS Filtering	Profiles are not replaced after deletion on a Deployment Site	INT-893
DNS Filter	DNS Filter Trial Experience	INT-854
Ecosystem	Intune Logout	KUIP-3171
Patch Management	Auto approval with explicit "No Approval" set on a target looks the same as rule that does nothing to the target.	PMCM-412

Release 2022.4 RC

Category	Description	Bug
Automation Manager	Automation Manager Agent Service unquoted service	AM-2877
Core	Redirect to Azure login page	NCCF-28739
Core	JUnit tests no longer running after merge to main.	NCCF-28592
Core	CVE-2021-4083 Vulnerable kernel` version `3.10.0-	NCCF-28212

Category	Description	Bug
	1127.18.2.el7` was detected in Nable Appliance	
Core	Fix failed unit tests in analytic branch	NCCF-27230
Core	CVE-2021-31805 - Struts2 update	NCCF-25700
Core	cvss 9.8 - CVE-2020-10683 - dom4j-2.1.1.jar requires update or modification	NCCF-24511
Core	cvss 9.8 - CVE-2019-17267 - jackson-mapper-asl-1.9.13.jar requires update	NCCF-24508
Core	Remote Desktop with Custom UI Port Does Not Work (ssh tunnel only)	NCCF-23342
Core	Topology Map Viewer "Go To Device" not working with UI port change	NCCF-22982
Core	Stored XSS via Add Discovery Job	NCCF-14242
Integrations	Ecosystem agent communication / FIPS errors	KUIP-3741,KUIP-3743,KUIP-3575
Integrations	The DNS Filtering Status remains reported as an active issue in N-central after uninstall	INT-849

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

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

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

User Access Management

Description	Bug
Azure/Generic IDP Login Name/Email is CASE SENSITIVE ■ As an admin, when you configure Azure or a Generic (Custom) IDP and then link a user… the user's "Login Name" or "Login Email" (if LDAP enabled), case sensitivity is taken into account when authenticating. If the user enters their email address at login that does not match the exact case of the value contained within either field, the authentication fails. A workaround is to modify the Login Name or Login email to be all lower case, save, unlink and relink then test logging in using all lower case.	NCCF-30422
Bulk User IDP Link and Unlink not working. ℹ This issue pertains to Azure and Generic IDP feature which is a Preview Feature in this release.	NCCF-29040

Description	Bug
■ As an admin, when you select one or more users from the User Management screen (bulk users) and attempt to LINK TO SSO PROVIDER, selecting an provider, nothing happens. It does not prompt me to confirm linking of the user or users. A workaround is to perform the user linking action via Administration›User Management›SSO Providers ›Provider config Link/Unlink. ■ As an admin, when you select one or more users from the User Management screen (bulk users) that have been previously linked to a SSO provider and attempt to Unlink the user or users via LINK TO SSO PROVIDER›Unlink, the Unlink option is greyed out. A workaround is to perform the user unlinking action via Administration›User Management›SSO Providers ›Provider config Link/Unlink.	
Login window reappears when new tab is loaded. When already logged into N-central and a user opens a new tab and browses to N-central from this new tab, the login screen reappears yet the user is already logged in. The left hand navigation is functional.	NCCF-29648

End of support

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

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

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 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

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	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

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.
	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.				
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			√		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. 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

Port Number	Port Location				Description
	N-able N-central Server		Managed Device		
	Inbound	Outbound	Inbound	Outbound	
					■ 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 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.				

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. 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.

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 2022.5 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.