N-ABLE™

N-central

Release Notes

Version: 2022.7 (Build: 2022.7.0.26)

Last Updated: Thursday, November 3, 2022

What's New in N-able N-central 2022.7

What's New in N-central 2022.7 and Automation Manager 2.50

N-central 2022.7 is packed with both fixes and new features! Please see below for more information on our new features, and the fixed items list for a list of bugfixes!

Device Management for Apple

N-central 2022.7 is the first to include N-able's Device Management for Apple solution.

> Note that this is a new service to N-central for Mac workstations only. The existing N-central MDM for iPhones and iPads is similar technology but a different back end. The two services will co-exist for some time.

Here's what Device Management for Apple includes in the 2022.7 release.

- User-approved manual enrollment: To bring Mac workstations under management properly, Apple requires that enrollment into Device Management be approved by the user of the device. This cannot be scripted.
- Enrollment Helper: to assist with manual enrollment, N-central provides an app that presents your brand - or a friendly name of your choosing - to users and asks them to initiate the process of installing the Enrollment Profile. This can be enabled/disabled across your entire fleet, or on a client-by-client basis, or one device at a time.
- Multi-tenant push certificates: To get started with Device Management, N-central admins must send a CSR from N-central to the Apple Push Certificate portal to get a push cert. N-central includes support for creating a push cert for only specific customers, or globally for all devices. Enrollment Helper can be enabled/disabled with each cert. (Note: this is the same technology as the existing APNS cert in N-central's MDM for iPads and iPhones - but it is being setup with a different back-end service.)
- PPPC profiles for N-able products: once a Mac is enrolled in Device Management, our service automatically pushes Configuration Profiles that grant macOS Security & Privacy permissions for the N-central Mac Agent, Take Control, EDR, Backup and more. (The only one we can't push is Screen Recording for Take Control because Apple doesn't allow that permission to be controlled by any MDM, not just ours.) This further streamlines the installation process for new Macs because you don't need to jump through all the hoops to grant Full Disk Access, Notifications, etc.
- Custom Configuration Profiles: Once you have a push cert setup, and devices enrolled, you can upload thousands of configuration profiles - many samples are available in the N-able Automation Cookbook - and push those over the air to your Mac workstations. The configuration possibilities are virtually limitless.
- As powerful as this is, it is a first release. Device Management for Apple has capacity for support for MDM Commands (like lock and wipe), support for iPads, iPhones, AppleTVs in addition to Macs, and support for Apple Business Manager and Apple School Manager automatic zero-touch enrollment. Future builds will round out a complete Device Management service for Apple devices. Those features are on their way to N-central in future releases.
- In addition to Device Management, work continues on surfacing the benefits of our new Mac Agent. N-central 2022.7 includes a real-time Processes widget in the Overview tab of Mac workstations. And for the first time ever, Mac workstations get a Tools tab - it's currently only populated with the same Processes table but will be built out in future N-central releases.

Automation Manager 2.50

Automation Manager 2.50 is now available and included in N-central 2022.7. This version of Automation Manager focuses on bugfixes, including fixes that should help with certain errors in AMP-Based monitoring services in N-central once your agents have upgraded.

In the Designer, we've clarified the help articles to indicate SSHv2 is supported for Network Management objects, and we've adjusted the branding to match N-central's default branding. Prompts from Automation Manager will now always be in the foreground and appear in the center of the screen.

Upgrade paths and notes

After the upgrade to N-centralVersion: 2022.7, 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 2022.7, 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+

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.

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 no longer communicates with external application server since upgrade to 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 2022.7 GA and AM 2.50

Category	Description	Bug
Automation Manager	AM Object: "Backup Registry"Input Parameters mistake in description	AM-2316
Automation Manager	PolicyExecutionEngine logging to agent.log instead of PolicyExecutionEngine.log	AM-2669
Automation Manager	Input Prompt object doesn't allow to link input	AM-2677
Automation Manager	Install Software from FTP doesn't allow SFTP connections	AM-2730
Automation Manager	Add FluentFTP assembly to NC Win Agent and Probe installers	AM-2745
Automation Manager	Pre-Fill The AMP Name When Closing Automation Manager	AM-2749
Automation Manager	Get Events object not returning results for operational logs (e.g Setup)	AM-2808
Automation Manager	Script check failing with error "Exception encountered System.Runtime.Serialization.SerializationException" then automatically resolves itself next check-in	AM-2809
Automation Manager	Make AM able to work when FIPS mode is enabled	AM-2822
Automation Manager	AutomationManager.log displays N-central agent version as 0.0	AM-2826
Automation Manager	Redesign the "Policy List" Window	AM-2830
Automation Manager	Update The Colors In the Automation Manager Designer	AM-2832
Automation Manager	Create AD user module in Automation Manager	AM-2833
Automation Manager	Map network printer	AM-2836

Automation Manager	Get OS Architecture AMP abnormal results	AM-2840
Automation Manager	Set different AM log level from NC dashboard	AM-2843
Automation Manager	Update the "Close Connection" Object To Support SSHv2	AM-2846
Automation Manager	Update the "Command Set" Object To Support SSHv2	AM-2847
Automation Manager	Update the "Enable (Cisco)" Object To Support SSHv2	AM-2848
Automation Manager	Update the "Get Connection Details" Object To Support SSHv2	AM-2849
Automation Manager	Update the "Open Session" Object To Support SSHv2	AM-2850
Automation Manager	Update the "Send Commands and Receive Response" Object To Support SSHv2	AM-2851
Automation Manager	Update the "Set Terminal Length" Object To Support SSHv2	AM-2852
Automation Manager	Large Number of Probe Log Files AutomationManager.ScriptRunner64-p[XXXX].log	AM-2853
Automation Manager	M365 automations Failed execution on remote device	AM-2855
Automation Manager	AM object - Get Environment Variable shows error message but it returns correct info	AM-2858
Automation Manager	AM Run PowerShell Script object throws "Exception: Requested registry access is not allowed"	AM-2859
Automation Manager	Improve AM PolicyExecutionEngine-p[%processid].log	AM-2880
Automation Manager	AM prompts open at the top left of the screen	AM-2883
Automation Manager	Automation Manager Agent Service crash when scheduled task run as logged on user	AM-2890
Automation	Fix AM initialization after Shutdown RPC call	AM-2898

Manager		
Automation Manager	Reboot Prompt Not working when Branding is used	AM-2912
Automation Manager	Prompt improvements: Add check for prompt to always be on foreground	AM-2914
Automation Manager	Script Check failing with Unknown Error (Exception encountered System.InvalidOperationException: There is an error in XML document (0, 0)....)	AM-2915
Automation Manager	Incorrect status for UAC service	AM-2917
Automation Manager	AM RPC server issue: No protocol sequences have been registered	AM-2923
Automation Manager	Automation Manager Object: Reboot Prompt, Exceeded delay time but did not initiate reboot	AM-2927
Automation Manager	Introduce RPC server's fallback address functionality	AM-2960
Automation Manager	Log cleanup: delete empty log files when log level is ERROR or FATAL	AM-2965
Automation Manager	AM assemblies to 2.50 on NC 2022.7	AM-2969
Automation Manager	Fix ConfigurationSettings.xml file for thirdparty dll name	AM-2970
Core	The agent version is displayed instead of the server version	CALM-1419
Integrated AV	Soft-deleted records are not hard-deleted for a long time	IAV-1052
Integrations	The user having 'Read Only' or 'None' permissions over DNS Filtering Integration can still deploy or remove the Roaming Client or select a profile in the deployment process	INT-1005
Integrations	Empty profile name allowed	INT-657
Integrations	The DNS Filtering Status remains reported as an active issue in N-central even after RC's uninstallation (validated after 7 days of RC uninstallation from the client's machine)	INT-849
Integrations	DNS Filter Trial Experience	INT-854

Integrations	Newly created profiles under NC System levels (SO / Customer / Site) cannot be edited (Content Filters / Block Pages selections)	INT-864
Integrations	Add the DNSF service into Monitoring tab when the device is in Essential Mode	INT-941
Ecosystem Framework	MS Intune integration icon shows enabled even when not being used - Dev Work	KUIP-2898
Ecosystem Framework	Sentinel One agent is not being uninstalled when a Device with EDR enabled is being removed from N-Central	KUIP-2985
Core	RemoteControlSSHConfigDataUtil.java references a Nable_ Wrapper.pl option that does not exist	NCCF-14033
Core	[FEATURE] Device Management for Apple	NCCF-14253
Core	System Error When The System Is Out Of Licenses, And A Licensed Feature Is Added To The Device	NCCF-14388
Core	Deprecate Support For Unsupported Versions of Linux and 32-bit Linux Installers	NCCF-14459
Core	The UserAdd API Returns a "-1" When Password That Doesn't Meet The Complexity Requirements Is Specified, Instead Of An Actionable Error Message	NCCF-14470
Core	Domain User Management Re-Did A Global Password Reset For A Customer	NCCF-15022
Core	Large amount of temp file in AM temp location cause agent startup delay	NCCF-15125
Core	Deleting a probe does not delete record from device's "discovering_ wsp"	NCCF-15560
Core	Show caps lock on for login password, instead of sending password in reverse case.	NCCF-15595
Core	Locking the "MFA Not Required" Option Isn't Being Saved	NCCF-15617
Core	Dropdown Custom Property will remain on error state after two empty values	NCCF-16055
Core	The Linux/Mac code sometimes returns 32-bit for 64-bit OSs	NCCF-16219
Core	Incorrect repository capacity is being displayed	NCCF-16323
Core	User cannot create reinstall agent task because probe not assigned	NCCF-16666

Core	Probe HTTPS service: 1. Change X509ChainPolicy.RevocationFlag 2. Change validation logic ignoring error when global error ChainStatus is used for certificate validation	NCCF-17007
Core	Custom Service (SNMP): change Service Identifier and/or Identifier options saves unexpected configuration.	NCCF-17038
Core	Custom Service (SNMP): System Error	NCCF-17040
Core	Settings not retained for Connectivity Service Details when SNMP enabled	NCCF-21344
Core	Improve logging for all Google actions if missing	NCCF-21483
Core	Google IdP Provider: remove the client-id from the error text displayed when NC is accessed by IP	NCCF-22664
Core	Stop Building the Unsupported Agent Installers	NCCF-22822
Core	Remove unsupported Installers From N-central	NCCF-22823
Core	Ensure Existing Deprecated Agent Installers cannot be used to register and activate new appliances	NCCF-22825
Core	Setting Up More than Two Services in a Template, The Service identifier is Not Transferred Correctly	NCCF-24478
Core	Create sysaudit script to collect non-IdP user metrics	NCCF-24846
Core	SSO Providers Google G-Suite - Robot Framework Test Suite Integration: N-central	NCCF-24907
Core	N-Central DMfA Navigation UX	NCCF-26127
Core	Allow sorting by SSO Column	NCCF-27272
Core	64 bit processes not showing DLLs used	NCCF-28092
Core	Default Filter Created on Site Creation Causes System Errors	NCCF-28386
Core	N-central - Send list of clients to Device Management for Apple (DMfA) UI in iframe	NCCF-29749
Core	Update Permission Definitions and UI for DMfA	NCCF-29750
Core	Create Release request for N-central DMfA for 22.7	NCCF-29751
Core	Send permission to DMfA for jwt	NCCF-29997
Core	RF5 Fails on evaluation of python os.gettempdir	NCCF-30087

Core	Add missed statistics for event acknowledgement time	NCCF-30801
Core	N-central - Inconsistent ApplicationDeviceId when requesting an DMfA profile	NCCF-30926
Core	Pending events are not cleared out from queue when system gets into a throttle blocking state and eventing is turned off	NCCF-30977
Core	Fix ROLES page when appledevicemanagement Flag is off	NCCF-31011
Core	Scraping: Records are being dropped due to mandatory date fields that cannot be parsed	NCCF-31201
Core	The assigned Variable in postbuils.sh is causing disruption to the URL	NCCF-31456
Core	Database scraping has an issue where concurrent table processing happens and events overlap	NCCF-31458
Core	Logging I Include protobuf event type	NCCF-31573
Core	XMPP related issues	NCCF-32110
Core	UI I Eventproduction I Only sys admin	NCCF-32195
Core	UI I Analytics Splash Message Removal	NCCF-32474
Core	SessionUtils.refreshExpiryForAppliance Triggering Against Eventing When It Does Not Need To	NCCF-32749
Core	IR Stable Main - Devices - Verify System Warranty Service is Added - Fails	NCCF-32957
Core	IR Stable Main: Devices - Verify Log File Is Not Accessible For User With Low Level Access - Fails	NCCF-32958
Core	ElementClickInterceptedException caused by 'Device Permissions' Dialog warning "You do not have permission to configure devices. Please contact your administrator."	NCCF-32980
Core	Google SSO Provider - Create Google SSO Provider page is broken	NCCF-33150
Core	Event controller should reset pending counts on restart	NCCF-33243
Core	Acknowledgement controller should reset pending counts on restart	NCCF-33244
Core	Catastrophic failure of event buffer termination should resetbuffer state and turn off eventing.	NCCF-33245
Core	Batch sender not started error	NCCF-33483

Core	AdvancedReportingUser is getting dropped due to missing role or customer group	NCCF-33484
Core	Live eventing should not stop when backups occur	NCCF-33536
Core	Records are being removed from bufferingEnabledTables variable and causing events to be permanently dropped	NCCF-33765
Core	EventBufferController Can Cause High Garbage Collection	NCCF-33812
Core	Upgrade certificates with proper clientId for NCOD to support DMfA	NCCF-33990
Core	Left-hand menu for "Analytics" needs to show we are Beta.	NCCF-35263
Core	Memory consumption is too high when buffering events	NCCF-35840
Core	Ensure time series tables are not processed for scraping unless within 24h	NCCF-35851
Core	Interrupt exception can cause event processing and/or acknowledgement processing to stop permanently and needs a watchdog	NCCF-36410
Core	NULL pointer error while saving Device settings	NCCF-37224
Core	Agent download labels incorrect	NCCF-38026
Core	Agent installation fails	NCCF-38236
Core	Parent level view - Permission evaluation is not performed for lower levels	NCCF-39485
Core	ScriptDownloadURI' Version Not Updating After Upgrading of N-central	NCCF-40053
Patch Management CM	Include re-branded PME in the latest N-central	PMCM-715

Known Limitations

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

Agents & Probes

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

Automation Manager

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

Custom Services

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

Core Functionality

Description	Bug
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

Description	Bug
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

Dashboards

Description	Bug
Modifying a Dashboard that is associated with a large number of services may cause performance issues when using the Firefox browser.	70326

PSA Integration

Description	Bug
In some instances, tickets closed in PSAs are not being cleared in N-able N-central. This is likely because the ticketing recipient profile in N-able N-central has **Do not change the Ticket Status** selected (in order to manually configure tickets). Then, when the ticket is removed in the PSA, N-able N-central will not be able to update/resolve the ticket's status and new tickets cannot be created for the same issue. Until a solution is available through the UI for this situation, the work around is to set a Return to Normal status and set a non-used status in the 'updatable statuses' section or set the same status as the return to normal one. This will cause N-able N-central to add a note to the ticket on return to normal but will not alter the ticket's status. This will allow the stale ticket check to remove the ticket from the system.	65620

UI

Description	Bug
After re-naming, the **Names** of files or Registry entries may not be displayed properly in the **File System** window and the **Registry** window of the **Tools** tab when using Internet Explorer.	68149

User Access Management

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

End of support

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

Transport Layer Security (TLS)	N-able N-central now disallows traffic over TLS 1.0 and TLS 1.1. This causes any Windows Agents or Windows Probes that are running on Windows XP and Windows Server 2003, as well as pre-v12.1 versions of the MacOS agent, to lose the ability to communicate with your N-able N-central server. We strongly recommend using a Windows Probe to monitor those devices.
Linux Agent Support	Due to declining usage in the field, N-able N-central Linux agents no longer support CentOS 6, Ubuntu 14.04, and the 32-bit version of Ubuntu 16.04.
Internet Explorer 11	Due to declining usage in the field, a future release of N-able N-central will drop support for the Internet Explorer 11 web browser.
AV Defender 5.x	As of next major release for those of you still utilizing the AV5 Bitdefender Antivirus be advised that monitoring from our AV5 agents will no longer continue. As a result this will leave your environments in a vulnerable state. We encourage you to review your agents to ensure you are now utilizing our latest AV6 agents. Reminder that our online help for Security Manager is available for your reference.

N-able N-central System requirements

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

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

Processor	Server class x86_64 CPUs manufactured by Intel or AMD (i.e. Xeon or EPYC). Please refer to the Red Hat Hardware Ecosystem for further details.
Operating System	You do not need to install a separate Operating System to run N-able N-central. The N-able N-central ISO includes a modified version of CentOS 7, based on the upstream Red Hat Enterprise Linux 7.
Physical Hardware	The physical server used to install N-able N-central in a bare metal environment must be certified to run Red Hat Enterprise Linux 7.7 (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 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 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.
	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.				
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 2022.7 uses the 7-Zip file archiver for installing agents and probes. 7-Zip is free software redistributed under the terms of the GNU Lesser General Public License as published by the Free Software Foundation. For more information, see http://www.7-zip.org.

Customer Support

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

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

About N-able

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