RELEASE NOTES

SolarWinds N-central

Version 12.3 HF7 (build 12.3.0.765)

solarwinds msp

Last Updated: Thursday, October 29, 2020

What's New in SolarWinds N-central 12.3 HF7

Security Vulnerabilities

The following vulnerabilities were addressed in N-central 12.3 HF7 (released on October 26, 2020):

- CVE-2020-25617—Could allow for remote code execution to the N-central Administrative Console (NAC); however, to be executed, the user must be authenticated as an administrator.
- CVE-2020-25618—Could allow a compromised account to run a set of whitelisted commands that if improperly used could allow for unintended escalation of privilege; however additional protections are in place to minimize access to the local machine.
- CVE-2020-25619—Under certain circumstances, could enable “remote control SSH port forwarding” to connect to local ports on the N-central server.

Upgrade paths and notes

To upgrade to 12.3 HF7, your SolarWinds N-central server must be running one of the following versions:

- SolarWinds N-central 12.2.0.274-350
- SolarWinds N-central 12.2.1.90-400
- SolarWinds N-central 12.3.0.241+

Note the following when upgrading SolarWinds 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 SolarWinds N-central

Release 12.3 HF7

Category	Description	Bug
Mobile Device Manager	N-central's MDM module has been updated to use Apple's newer HTTP/2-based APNs (Apple Push Notification service) provider API.	NCCF-11243
Core	Legacy Security Profile was not Restored with N-central Backup Restore.	NCCF-13599

Release 12.3 HF6

Category	Description	Bug
Core	Logging in to N-central over HTTP hangs when loading deployJava.js	NCCF-14395

Release 12.3 HF5

Category	Description	Bug
Security	Addresses an Apache Struts vulnerability (CVE-2019-0233).	NCCF-14068
Core	Corrected a bug impacting server recovery.	NCCF-13876

Release 12.3 HF4

Category	Description	Bug
Patch Manager	PME unable to communicate to RPC server over 127.0.0.1.	NCPM-4387
Patch Manager	Automatic patch approvals don't work after deleting a customer.	NCPM-4324
Patch Manager	Latest PMESetup.exe now downloads from the SIS server rather than bundled with the N-central agent.	NCPM-4422

CATEGORY	DESCRIPTION	BUG
Patch Manager	Better handling of "RPC Server is unavailable" issue in Patch Manager engine.	NCPM-4398
Patch Manager	Patch Manager engine auto-update more robust.	NCPM-4397
Core	Exclude checking primary IP against excluded IP for device match.	NCCF-13692
Core	PSA: Lack of device class mappings can lead to export of unrelated devices.	NCCF-13459
Core	Submit Queue is held up waiting on notification processing.	NCCF-13410
EDR	EDR Monitoring Status in 12.3 HF3 not showing all metrics.	KUIP-1624

Release 12.3 HF3

CATEGORY	DESCRIPTION	BUG
Core	Tools > Command Prompt Isn't Accepting UTF-8 Special Characters.	NCCF-13481
Core	Software Update Notification Notice from suspicious sender to all customers.	NCCF-13458
Core	The Patch Status Service and the "Patch Summary" Widget on the Overview Tab Temporarily Show a System Error.	NCCF-13386
Core	Thread Blocks Occurring Due to Missing JAR File.	NCCF-13360
Core	N-central Thinks that the NSP for 12.3 HF1 is Corrupt.	NCCF-13274
Core	Loading a Service Within a Service Template Takes > 30 Seconds.	NCCF-13243
Core	N-central upgrade failed on Azure; errors related to getty@ttyS0.	NCCF-13238
Core	Incorrect Thread Pool Settings Causes Jetty to Stop Responding Under High Load.	NCCF-13187

CATEGORY	DESCRIPTION	BUG
Core	Device Does Not Perform An AV scan After Missing Its Scheduled Time.	NCCF-11364
Core	XMPP Policy Violations Cause Poor Performance/Stability In The Tools Menu.	NCCF-7790
EDR	Logic Issue In EDR Caching Code Caused All EDR Agents To Be Uninstalled.	KUIP-1405
EDR	Typo in the EDR Status Service.	KUIP-1260
EDR	System Error when creating new Rule to Uninstall Integrations.	KUIP-1242
Monitoring	Incorrect TLS Settings Causes The Windows Probe To Fail To Discover Physical Drives on ESXi Hosts.	BEAT-1522

Release 12.3 HF2

CATEGORY	DESCRIPTION	BUG
Core	Analytics Data Export Causes Increased CPU Usage.	NCCF-13213
Core	macOS Agent Fails to Upgrade As It Stores The New Installer In /tmp.	NCCF-13207
Core	NcentralAssetTag can be ignored on discovery, creating duplicate device.	NCCF-13182
Core	macOS Agent and S1 Removed When macOS Agent Upgrades Itself.	NCCF-13178
Core	Upgrade from 12.1 to 12.3 Was Allowed To Proceed, Even Though It's An Unsupported Upgrade Path.	NCCF-13164
Core	Mobile Devices Tab Crashes Browser Tab at System Level.	NCCF-13102
Core	Unable to View or Add Notification Triggers Due to Devices With Duplicate Names and URIs.	NCCF-13018
Core	Hovering Over a Service in the All Devices View Shows All Services.	NCCF-12815

CATEGORY	DESCRIPTION	BUG
Core	N-central Stability Affected by Under-Optimized Filter Code.	NCCF-12758
Core	Improve The Security Of The JSESSONID Cookie By Utilizing The HttpOnly Flag.	NCCF-10415
Core	Upgrades of N-central Don't Give The Default Administrator Role "Manage" Permissions to the Integrations Menu.	KUIP-1246
Core	Upgrade to 12.3 Fails When the Default Administrator Role Isn't Present.	KUIP-962
PSA	Autotask Tickets Created by N-central Aren't Being Closed When The Service Returns To Normal.	NCCF-12511
EDR	Logic Flaw In Discovery Could Cause EDR To Become Misconfigured Or Unintentionally Removed.	KUIP-1257
EDR	N-central Fails to "Take Over" Standalone Installs Of EDR.	KUIP-1215
EDR	The Initial Install Of EDR Gets Cancelled If The Device Is Offline Overnight.	KUIP-1191
EDR	The License Usage Report Generates a System Error when N-central Cannot Retrieve EDR Licensing Information.	KUIP-1025
EDR	Integrated EDR Deployments Aren't Upgrading from v3.6.x to v3.7.x.	KUIP-1021
EDR	Integrations -> Integration Management Incorrectly Shows EDR as Trial Instead of Active.	KUIP-1005
EDR	Integrations -> EDR -> Dashboard Fails To Load At The SO Level.	KUIP-986

Release 12.3 HF1

CATEGORY	DESCRIPTION	BUG
Core	Submit Queue Causes Devices to Fail to Come Out of Downtime.	NCCF-13022

CATEGORY	DESCRIPTION	BUG
Core	Exporting the All Devices View as a CSV Doesn't Include All Devices.	NCCF-13002
Core	Jetty Stability Issues Caused By Incorrect "MetaspaceSize" Value.	NCCF-12799
Core	Can't save Organization/Device level Custom Properties entries.	NCCF-12798
Core	Notifications Aren't Generated Due to Maint Timer 1 Hanging.	NCCF-12746
Core	Service import failure during upgrade.	NCCF-12744
Core	N-central backup does not store Network Security settings.	NCCF-12719
Core	Server Offline Caused By Duplicate activenotificationtriggerticketdetail and notifonnormalticketdetail Entries.	NCCF-12607
Core	All Device View Loads Unacceptably Slowly On Busy Systems.	NCCF-12564
Core	All Agents use a fixed password to talk to XMPP on n-central.	NCCF-12394
Core	N-central Backup Does Not Properly Clean Up if FTP Transfer Fails in Active Mode.	NCCF-12305
Monitoring	Unable to Configure a Discovery Job to Use VMware Credentials that end in ".local".	BEAT-1333
NetPath	After Rebuilding/Restoring N-central, NetPath Shows a "An Unknown Error Has Occurred Try Again" Error Message.	BEAT-1137

Release 12.3

CATEGORY	DESCRIPTION	BUG
Core	System Error When Attempting to Delete a Mobile Device.	IAV-625
Core	JETTY request logs are rolling over by day not size, this is filling up the /var/log folder.	NCCF-12755

CATEGORY	DESCRIPTION	BUG
Core	N-Central Upgrade Fails, and reports "Error installing database".	NCCF-12690
Core	CVE-2020-7984 - Authentication Vulnerability in N-central Agent Registration (public PoC).	NCCF-12687
Core	Azure VM Agent Doesn't Get Installed on N-central.	NCCF-12591
Core	Autotask PSA Integration - Setting Devices to "Inactive" Does Not Work.	NCCF-12559
Core	System Error When Updating The Thresholds Of A Custom Service.	NCCF-12556
Core	Upgrades to N-central Fail Due to a Logic Issue Related to Modifying the Default Parameters of the Connectivity Service.	NCCF-12504
Core	HTTPS Incorrectly Reports a Failed State When Monitoring a Website That Requires Credentials.	NCCF-12492
Core	Tools -> Applications Isn't Updating Due to an Unhandled Exception.	NCCF-12465
Core	Filtering the Administration > User Management > Users Page With Certain Characters Generates a System Error.	NCCF-12340
Core	Hovering Over a Service in Dashboards Isn't Displaying Misconfigured Service Instances.	NCCF-12333
Core	Upgrade From 12.2.x to 12.2.y Fails Due to Permission Issues with Jetty.	NCCF-12326
Core	Security Update: Creating a new Customer now has enhanced checks around access groups.	NCCF-11652
Core	Security Update: Address the logging of Self-healing custom credentials in specific situations.	NCCF-11450
Core	Security Update: Use HTTPS for download of the third party software provided by SIS server.	NSBM-3281
Core	Security Update: Enhance session security mechanisms, strengthening protections against session brute-forcing attacks.	NCCF-6924
Core	NCSAI Lost Track of it's PID and Lock Files When the Service Startup Was	NCCF-

CATEGORY	DESCRIPTION	BUG
	Cancelled..	12304
Core	Unable to Save/Propagate Site-Level, Organization Custom Property.	NCCF-12282
Core	The "Recent Tickets" Widget Does Not Work When N-central Is Integrated With Marval.	NCCF-12212
Core	System Error in Netpath When Clicking on the "License Usage" Link.	NCCF-11807
Core	Service Metric scan detail chart X axis legend will vary from JavaScript to PDF.	NCCF-11582
Core	Windows Agent Crashes and Erroneously Uninstalls the Take Control Agent.	NCCF-12230
Core	Unable to use the @ symbol When Entering VMware Credentials in a Discovery Job.	NCCF-12228
Core	System Error When you Turn off PSA Integration and Subsequently Create a New Customer.	NCCF-12210
Core	Upgrade to 12.2 SP1 Fails Due to Duplicate "Web_UrlIp" and "Web_UrlIP" Records.	NCCF-12183
Core	N-central's loginLoginAction.action Page Throws a 500 Error.	NCCF-12177
Core	Improper PID and OS Signal Handling in NKO Causing Intermittent NOS Start/Stop Failures and Upgrade Failures.	NCCF-12169
Core	Installing a New Windows Agent or Windows Probe Fails, and Logs an "Unable to Communicate with Server" Error.	NCCF-12130
Core	Scheduled Tasks Fail Due to the Windows Agent Changing the Filename To Short-Filename.	NCCF-11921
Core	Bulk editing a Custom Property is limited to 100 characters.	NCCF-11905
Core	Backup process is not checking for /tmp/initial_install, resulting in backups running during install/OS Upgrade.	NCCF-11875
Core	Direct Support's TLS Configuration Causes a System Error when attempting to retrieve files with Tools -> File System.	NCCF-11858

CATEGORY	DESCRIPTION	BUG
Core	Upgrade of N-central Failed Due To The NOS Initscript Performing Invalid Return Code Comparisons.	NCCF-11851
Core	NableCommandPromptManager64.exe crashing.	NCCF-11831
Core	N-central Fails To Generate a CSR If The "Division or Business Unit" Field Is Empty.	NCCF-11822
Core	Device-Level Audit Trail Erroneously Shows Two "Service Monitoring" Entries.	NCCF-11816
Core	VMware Services Misconfigured Due to Issue in the Data Retrieval Logic.	NCCF-11805
Core	Downtime from "Unscheduled Downtime" will resume service scanning if you disable/enable the service.	NCCF-11785
Core	Unable to View Long Instance Names When Configuring the Service Metrics Report.	NCCF-11771
Core	The "Event Description" Column Isn't Present in the CSV Export of the Windows Event Log Report.	NCCF-11767
Core	Connectivity Service fails when increasing packet size.	NCCF-11761
Core	System Error when accessing domain in Domin User Management.	NCCF-11759
Core	Device Export to PSA Not Occurring When The Export Profile Targets Unlinked Customers.	NCCF-11725
Core	Custom Branding Allows for Disallowed File Types (BMP and ICO) to be Uploaded.	NCCF-11712
Core	Edge not listed as one of the supported browsers.	NCCF-11711
Core	Filtering for Scheduled Downtime Does Not Consider Customer/Site Downtime.	NCCF-11708
Core	The Associations Tab of Scheduled Task Profiles Takes Unnecessarily Long To Load.	NCCF-11707
Core	Deleting a Printer from the Tools > Printers Menu Fails.	NCCF-

CATEGORY	DESCRIPTION	BUG
		11697
Core	N-central Sends Out Notifications About "Attended Remote Control Trial Period Expiring".	NCCF-11695
Core	Serial Number Isn't Being Discovered on HP iLO Cards.	NCCF-11684
Core	The ShadowProtect Service Shows An Incorrect "Last Successful Backup Date".	NCCF-11673
Core	'Replace or auto-rename' pop-up window doesn't appear for the second try.	NCCF-11670
Core	New Customer creation does not trigger access group check for restrictions.	NCCF-11652
Core	Services Monitored By the N-central Server Report a Stale Status.	NCCF-11623
Core	HTTPS services are failing after upgrading to 12.1.1.241.	NCCF-11622
Core	Exception Thrown When The macOS Agent Submits Asset Data to N-central.	NCCF-11620
Core	Add URL redirect logic to Probe when using Connectivity service monitoring.	NCCF-11610
Core	Unable to Configure a Service Metrics Report for the NetPath Service.	NCCF-11535
Core	Dashboards Sorted Differently In The Dashboard Menu vs. The "Manage Dashboards" Page.	NCCF-11530
Core	Missing Input Validation on the "Server Address" Field for CSR Generation.	NCCF-11517
Core	N-central Performance/Stability Affected by a Process Deadlock.	NCCF-11493
Core	Self-Healing On the HTTPS Service Reports An "Invalid Credentials" Error.	NCCF-11479
Core	Self Healing for Hyper-V Guests Doesn't Work When Guest Name Contains Quotes.	NCCF-11449

CATEGORY	DESCRIPTION	BUG
Core	N-central Doesn't Update the Manufacturer Field for Cisco Devices.	NCCF-11420
Core	AMP-Based Monitoring Services Reporting Stale Due to An Artificially Low Thread Limit.	NCCF-11393
Core	Device Does Not Perform An AV scan After Missing Its Scheduled Time.	NCCF-11364
Core	Custom PSA: Ticket is reopened if previous resolution has not been acknowledged.	NCCF-11362
Core	The "Move Device" Wizard Takes Too Long to Load the Probe Selection Menu.	NCCF-11306
Core	Fan Status (VMware) Service Goes Misconfigured, Due To An Unhandled Exception When The Hardware Sensors Are Not Available For Fans.	NCCF-11276
Core	An Active Notification Trigger Isn't Re-activated When Devices Come Out of Downtime.	NCCF-11164
Core	Agent/probe upgrade MSIExec check is susceptible to internationalization errors.	NCCF-11154
Core	N-central Imports iDRAC Cards as "Servers - Linux" Devices Instead of "Servers - Management Interface".	NCCF-11092
Core	Unable to launch Automation manager logged with Google SSO.	NCCF-8731
Core	When Generating a New CSR, The Jetty Timeout Is Too Short.	NCCF-7488
Monitoring	Windows Application and Services Log Fails to Detect Events Due To a Null Pointer Exception.	NCCF-12258
Monitoring	System Error on Interface Health Service.	BEAT-1138
Monitoring	Windows Applications and Services Log: Entries in the "Event ID Exclude" Field Are Not Saved.	BEAT-1060
Monitoring	Veeam Job Monitor often reads 0kb backup size.	BEAT-985
Monitoring	The HTTPS Service Reports a Failed Status on Websites That Do Not	BEAT-

CATEGORY	DESCRIPTION	BUG
	Support TLS 1.2.	921
Monitoring	An Incorrect Timeout Value Causes the Connectivity Service to Transition Between Failed and Stale.	BEAT-906
Monitoring	The APC PDU Service Isn't Getting Auto-Applied Through Service Templates.	BEAT-855
Monitoring	By Default The DNS Service Tries To Resolve "www.n-able.com".	BEAT-429
Monitoring	The WSFC Monitoring Services Don't Use the "Run PS Script" Object.	AM-2204
Topology Maps	500 (Server Error) Displayed When Trying to Access a Topology Map.	BEAT-1107
Topology Maps	Map Showing Unnecessary Additional Devices and Not Honoring the "Ignore ICMP" Setting	BEAT-1068
Topology Maps	Incorrect Customer Name In Topology Map	BEAT-953
Topology Maps	Unable to Switch Between "Recurring" Topology Maps	BEAT-904
Topology Maps	When Configuring a Subnet Range, The Topology Job Wizard Doesn't Accept .0 as the Last Octet of the IP Address.	BEAT-903
Automation Manager	Global Variables Returning Empty Values.	AM-2222
Automation Manager	Numerical results in Automation Manager showing incorrectly in some OS locales.	AM-2007
Automation Manager	"Set Default Browser" object removing .html associations.	AM-2001
MSP Backup	MSP Backup Status is intermittently failing on multiple devices due to an error parsing the StatusReport.xml.	NSBM-3742
Patch Manager	Devices Not Displayed in the All Devices View Due to Unnecessary Instances of the "Old" Patch Status Service.	NCPM-4224
Patch Manager	Message boxes are not suppressed during PME installation.	NCPM-4173

CATEGORY	DESCRIPTION	BUG
Patch Manager	Clean up PME log files.	NCPM-4148
Patch Manager	Windows Probe Cannot Download Patch Files when TLS 1.0 and TLS 1.1 are Disabled.	NCPM-4115
Patch Manager	Unhandled Exception In Patch Management Can Cause The Windows Agent To Crash.	NCPM-4078
Patch Manager	System Error When Moving Devices Between Customers.	NCPM-4057
EDR	Profiles are duplicated in the drop down of device config/rules etc.	KUIP-920
Security Manager	System Error When Clicking Into the "Security Events" Service.	IAV-731
Security Manager	The Device Selection Widget in the Recovery Key Report Isn't Sorted Alphabetically.	IAV-531
Security Manager	The Disk Encryption Status Service Considers "Unencrypted" To Be a Failure Instead of a Warning.	IAV-530
Security Manager	The Disk Encryption Report Doesn't Have Pagination.	IAV-528
Security Manager	The "Retrieve Recovery Key" Button Returns An Incorrect BitLocker Recovery Key.	NSBM-3641
Security Manager	License Usage Report Shows Incorrect Values for the Number of Consumed Disk Encryption Licenses.	NSBM-3634

Known Limitations

These items for the current version of the SolarWinds N-central software is composed of material issues significantly impacting performance whose cause has been replicated by SolarWinds MSP 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 SolarWinds 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 SolarWinds 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 SolarWinds 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
Custom Settings option no longer available in 10 for backup profiles.	NSBM-709

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 SolarWinds N-able Technical Support.	65288

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

Core Functionality

DESCRIPTION	BUG
Installing SolarWinds N-central on Servers that have an Nvidia Video Card Due to a bug in CentOS 7 with Nvidia's "Nouveau" driver, installing SolarWinds N-central on servers that have an Nvidia video card may result in the SolarWinds N-central console showing a black/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	73359

DESCRIPTION	BUG
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.	

PSA Integration

DESCRIPTION	BUG
In some instances, tickets closed in PSAs are not being cleared in SolarWinds N-central. This is likely because the ticketing recipient profile in SolarWinds 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, SolarWinds 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 SolarWinds 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

End of support

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

Internet Explorer 11	Due to declining usage in the field, a future release of SolarWinds N-central will drop support for the Internet Explorer 11 web browser.
Agents	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 on the NRC.

SolarWinds N-central System Requirements

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

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

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

System requirements by number of devices managed

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

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

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

Notes

1. Server Grade hard drives connected to a RAID controller with a Battery/Capacitor Backed Cache, are **required** to ensure performance and unexpected power-loss data protection.
2. In a virtualized environment, hard drives for the SolarWinds 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 SolarWinds N-central.
3. SolarWinds MSP 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. SolarWinds MSP recommends more, smaller disks in a RAID array, as opposed to fewer larger disks. Database-backed applications, like SolarWinds N-central, have better write performance with an increased number of parallel writes (hard drives).
5. If using Solid State Drives (SSDs), SolarWinds MSP requires Enterprise Grade, SLC based (or better) SSDs with a SAS interface, or Enterprise Grade NVMes. SSD and NVMe drives must have an endurance rating of at least 0.2 DWPD (Drive Writes Per Day), and at least 2 physical disks in a redundant RAID array. On Bare Metal servers, the RAID array must appear to the operating system as a single Block or NVMe Device. Currently, many PCIe and NVMe drives do not meet this last requirement and would only work in a virtualized environment.
6. Configure the RAID controller to use the default stripe size and a Read/Write cache of 50%/50%.

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

Subsystem	Limit
Minimum disk space	80GB
Maximum physical disk size (BIOS)	2TB
Maximum physical disk size (UEFI)	50TB
Required minimum memory	4GB for 4 or fewer logical CPUs
	1GB per logical CPU for more than 4 logical CPUs
Maximum memory	12TB
Maximum logical CPUs	768

Examples of supported servers

Due to the ecosystem of different hardware, SolarWinds MSP 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.

SolarWinds MSP 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

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

Hyper-V on Windows Desktop Operating Systems not Supported.

SolarWinds 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 SolarWinds 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 SolarWinds 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 SolarWinds 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	SolarWinds MSP supports SolarWinds 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 SolarWinds N-central deployed on Bare Metal. This support is limited to the components (Software and Operating System) shipped with SolarWinds N-central and does not include the troubleshooting of virtualization systems nor of performance issues related to environmental factors. SolarWinds MSP recommends reaching out to your hardware or virtualization vendor for support on the underlying virtualization and hardware components. Any assistance provided by SolarWinds MSP 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 SolarWinds 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	SolarWinds MSP 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, SolarWinds 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 SolarWinds 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 SolarWinds N-central server.

- Assign the highest resource access priority to SolarWinds 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 SolarWinds N-central guest.

Supported Software

Browsers

SolarWinds N-central supports the latest versions of:

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

SolarWinds 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:

- Oracle Java 1.8 versions that include Java Web Start

Report Manager

To use Report Manager with SolarWinds 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 SolarWinds N-central.

SNMP Community String

On HPE ProLiant Generation 9 or older Physical Servers, when monitoring the SolarWinds 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 SolarWinds N-central server.

Supported Operating Systems

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

Windows Agents:

- Microsoft .NET Framework 4.5.2 (or later)

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 Server 2008 R2

- Windows 2008
- Windows 2008 SP2
- Microsoft Hyper-V Server 2008 R2
- R2 Datacenter Server
- R2 Enterprise Server
- R2 Foundation Server
- R2 Standard Server
- R2 Web Server

The following are required to install Windows Agents on a server using Windows Server 2008 R2 Server and Windows Hyper-V Server 2008 R2 Core 64-bit:

- The operating system must be Windows Server 2008 R2 Server Core 64-bit SP1 or later.
- .NET Framework 4 for Server Core (64-bit) must be installed.

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

Mac Agents

- 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 7 (x86_64 and i686)
- Red Hat Enterprise Linux/CentOS 6 (x86_64 and i686)
- 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 Vista SP1
- Microsoft Windows 7 SP1
- Microsoft Windows 8, 8.1
- Microsoft Windows 10

Tablet And Embedded Operating Systems

- Windows Embedded Standard 2009
- Windows Embedded POSReady 2009
- Windows Embedded Enterprise 7
- Windows Embedded POSReady 7
- Windows Embedded Standard 7

Server Operating Systems

- Microsoft Windows 2008
- Microsoft Windows 2008 Server
- Microsoft Windows 2008 R2

- Microsoft Windows Small Business Server 2011
- Microsoft Windows Home Server 2011
- Microsoft Windows 2012 Server
- Microsoft Windows 2012 Server R2
- Microsoft Windows 2016 Server
- Microsoft Windows 2019 Server

For Microsoft Windows Embedded Standard 7, TCP/IP, Filter Manager, and Windows Installer must all be enabled.

Patch Manager

Workstation Operating Systems

- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 8.1
- Microsoft Windows 10 version 1607 and later

Server Operating Systems

- Microsoft Windows Server 2008 R2 SP1
- 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 SolarWinds N-central patch manager:

- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 10 Home Edition
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

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 7 (32/64-bit)
- Microsoft Windows 8 (32/64-bit)
- Microsoft Windows 8.1 (32/64-bit)
- Microsoft Windows 10 (32/64-bit)

Server Operating Systems

- 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)
- Microsoft Windows Server 2008 R2 (32/64-bit)
- Microsoft Windows Server 2008 (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

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		Mac OS X	
	Remote System	Technician	Remote System	Technician	Remote System	Technician
Custom	✓	✓	✓	✓	✓	✓
Take Control	✓	✓	✗	✗	✓	✓
Remote Desktop	✓	✓	✗	✓	✗	✗[1]
SSH	✓	✓	✓	✓	✓	✓
TeamViewer	✓	✓	✗	✗	✓	✓
Telnet	✓	✓	✓	✓	✓	✓
Web	✓	✓	✓	✓	✓	✓

1. Requires a remote third-party desktop viewer compatible with Mac.

Licensing and Customer Support

Agent/Probe Installation Software

SolarWinds N-central 12.3 HF7 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 SolarWinds MSP to activate your SolarWinds N-central server.

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

Feedback

SolarWinds MSP is a market driven organization that places importance on customer, partner and alliance feedback. All feedback is welcome at the following email address: n-ablefeedback@solarwinds.com.

About SolarWinds MSP

SolarWinds is a leading provider of powerful and affordable IT infrastructure management software. Our products give organizations worldwide, regardless of type, size, or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-premises, in the cloud, or in hybrid models. We continuously engage with all types of technology professionals—IT operations professionals, DevOps professionals, and managed service providers (MSPs)—to understand the challenges they face maintaining high-performing and highly available IT infrastructures. Targeted for MSPs, the SolarWinds MSP product portfolio delivers broad, scalable IT service management solutions that integrate layered security, collective intelligence, and smart automation. Our products are designed to enable MSPs to provide highly effective outsourced IT services for their SMB end customers and more efficiently manage their own businesses. Learn more today at solarwindsmsp.com.