



RELEASE NOTES

SolarWinds N-central

Version 2020.1 HF5 (build 2020.1.5.425)

What's New in SolarWinds N-central 2020.1 HF5

⚠️ Please be advised a bug (NCCF-15011) has been identified in this build which may impact the ability for Windows Agents and Probes to update properly. Before installing this hotfix, please review the instructions in this [KB article](#).

Digital Certificate Update

Following our [previous note regarding a digital certificate update](#), we have released HF5 for SolarWinds N-central 2020.1.

Action Required – N-central Server for New Devices, AV Defender

To onboard new devices into your N-central instance, you must upgrade N-central so that you can leverage the new Windows Agent and Windows Probe installers. The macOS and Linux Agents are not affected by the updated digital certificate.

If you are running AV Defender, you must upgrade your existing Windows Agents, or update to the latest version of AV Defender (6.6.20.296) to avoid any interruptions in communications between the Windows Agent and AV Defender. For more details, please see the AV Defender-specific note below.

No Action Required – All Other N-central Services

We are also releasing updates to the following services: Automation Manager, AV Defender, Patch Management, MSP Backup, NetPath, and Take Control. Apart from AV Defender (see the service-specific note below), **no action is required as those services upgrade automatically.**

Service-Specific Notes:

AV Defender

AV Defender 6.6.20.296 is available for Windows Modern Operating Systems, designed for Windows 7/Windows Server 2008 R2 and higher. This will be available as an update, upgrade and fresh install.

The AV Defender update can be scheduled at an appropriate time by adding a maintenance window to your devices. Updating involves an incremental update of components or modules without the need to remove protection. A reboot may be required based on Installation Status. If you do not want updates or reboots to proceed automatically, you can disable them by removing the appropriate maintenance windows from the device or rule.

To determine what version of AV Defender has been installed on a device, refer to the **Settings > Security Manager** tab of the device.

MSP Backup

Existing backup agents will be automatically updated to 20.11.0.20350 with a new digital certificate. However, based on your specific settings/policies/circumstances, the agent may not be automatically updated in time (for example, if the device is offline). In these cases, you may need to update to the new version manually to keep your backups running as expected. If that scenario applies to you, please complete the following steps:

- In N-Central, navigate to **Configuration > Backup Manager > MSP Backup > Dashboard**.
- In the MSP Backup dashboard, click on the **Columns** button and search for the **Client Version** column. Select it and it will be added in the complete right end of your view. Use the arrow to scroll to the right. Once you have identified any devices needing the update (less than 20.11.0.20350) uninstall the MSP Backup software and N-Central Windows Agent will install it back with the latest version, while maintaining your settings.

The screenshot displays the SolarWinds MSP Backup dashboard. The left sidebar shows the navigation menu with 'Configuration' expanded to 'MSP Backup' and 'Dashboard' selected. The main area shows the 'Backup dashboard' for 'Active Servers & Workstations & Microsoft 365' with a '100% Completed' status. A table lists devices with columns for Device name, OS type, Data sources, Selected, Used storage, and Last 28 days. A 'Columns' dropdown menu is open, showing a search for 'Client' and a list of columns including 'Client version' which is selected. Red arrows point to the 'MSP Backup' menu item in the left sidebar and the 'Client version' column in the dropdown.

NetPath

NetPath agent applications updates are taking place; those updates are happening separately from the upgrade of your N-central server and its Windows Agents and Probes. NetPath is being updated to version 1.15.6.12, and you can check what version is installed on a device via the **Asset -> Applications** tab of the device.

Patch Management Engine (PME)

Patch Management Engine (PME) version 1.2.13 was also released with an up-to-date digital certificate. You can check what PME version is installed on a device via the **Patch Status service** or the **Asset > Applications** tab of the device.

The following PME bug fix was included:

- NCPM-4593, Patch installations are timing out after 60 minutes

Take Control

Take Control updates are happening separately from the upgrade of your N-central server. Take Control – both the Windows Agent and the Windows Viewer - are being updated to version 7.00.21, and you can check what version is installed on a device via the **Asset > Applications** tab of the device.

Upgrade paths and notes

To upgrade to 2020.1 HF5, your SolarWinds N-central server must be running one of the following versions:

- SolarWinds N-central 12.2.1.90 – 400
- SolarWinds N-central 12.3.0.241 – 800
- SolarWinds N-central 2020.1.0.202+

Note the following when upgrading SolarWinds N-central.

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

Fixed Issues in SolarWinds N-central

Release 2020.1 HF5

This hotfix updates the digital certificate used by the Windows Agent and Windows Probe. Please see the "[What's New](#)" section for more details.

Release 2020.1 HF4

| CATEGORY | DESCRIPTION | BUG |
|----------|--|------------|
| Core | Unexpected Growth Of N-central Backups Leads To "ERROR: The N-central Backup file creation failed." E-mails | NCCF-14648 |
| Core | Some Recurring PowerShell/VBS/Batch Scheduled Tasks Created Before Upgrading to 2020.1 HF3 Start Failing After N-central is Upgraded to 2020.1 HF3 | NCCF-14743 |

Release 2020.1 HF3

| CATEGORY | DESCRIPTION | BUG |
|----------|--|------------|
| Core | XMPP Module Causes A Memory Leak In The Linux Agent | NCCF-13456 |
| Core | Legacy Security Profile was not Restored with N-central Backup Restore | NCCF-13599 |
| Core | Scheduled Tasks Aren't Reliably Running At The Scheduled Time | NCCF-13714 |
| Core | Audit Trail Shows Incorrect "End Time" Values For Take Control Sessions | NCCF-14048 |
| Core | The "Create Ticket" Button Is Missing from the Overview -> Active Issues Widget | NCCF-14123 |
| Core | Contract ID is temporarily removed for Devices already exported to MSP Manager | NCCF-14235 |
| Core | Choosing "Save and Propagate" For A Custom Organization Property Doesn't Trigger Rule Re-application | NCCF-14321 |
| Core | Performance Issues When Using Custom Properties Together With Rules | NCCF-14334 |
| Core | Hotfix Releases of N-central 2020.x Don't Pull Up the Online Help for 2020.x GA | NCCF-14452 |

| CATEGORY | DESCRIPTION | BUG |
|---------------------------------|---|------------|
| Core | N-central Restore not showing backup names when selecting from Local System | NCCF-14483 |
| Core | SysAudit processing error on Advanced Reporting Usage | NCCF-14506 |
| Core | Add the help doc key for the Network Security page | NCCF-14527 |
| Core | ApplianceRegistrationToken validity does not respect DST | NCCF-14542 |
| Endpoint Detection and Response | All Devices/Active Issues View: The Integration Column Does Not Stay Hidden | KUIP-1729 |
| Endpoint Detection and Response | EDR Status service started getting 201 Failure error. | KUIP-2199 |
| Monitoring | Windows Service Monitoring Causes WMI To Crash | BEAT-1817 |
| Monitoring | Error-Level Entries Seen in the Windows Event Log for the "N-able ShadowProtect Monitoring Service" | NCCF-13729 |
| Remote Control | Launching JNLP-based Remote Control From A macOS Device Prematurely Times Out | NCCF-13193 |
| Remote Control | System Error When Propagating Remote Control Defaults to Existing Sites | NCCF-14070 |
| Remote Control | Launching Multiple RDP Remote Control Sessions From the Same Device Sometimes Conflict | NCCF-14296 |
| Remote Control | N-central Stops Accepting SSH Tunnel Requests After 50 R/C Sessions | NCCF-14472 |
| Remote Control | RDP SSH Tunnel creation fails | NCCF-14475 |
| Remote Control | RDP client (mstsc.exe) and CPH launcher do not work over HTTPS channel | NCCF-14477 |
| Remote Control | "Data Encryption" Error Displayed When RDP Remote Control Falls Back From SSH To HTTPS | NCCF-14517 |
| Security Manager | Improved error handling for Disk Encryption Manager | IAV-1261 |

Release 2020.1 HF2

| CATEGORY | DESCRIPTION | BUG |
|---------------------------------|--|------------|
| Automation Manager | AMP-based Custom Services Fail To Submit Data When The Output Parameter Includes "EndTime" In Its Name | BEAT-1737 |
| Core | Logging in to N-central over HTTP hangs when loading deployJava.js | NCCF-14395 |
| Core | The "License Usage" Report Incorrectly Counts Devices Twice For "Remote Control on Essentials" Licenses | NCCF-14229 |
| Core | The Remote Control Icon Is Unavailable To Users That Only Have Access To Take Control | NCCF-14066 |
| Core | The "Detailed Status" Report Incorrectly Shows A Service As Disconnected Instead Of Failed | NCCF-13956 |
| Core | RDP Remote Control: Fallback to HTTPS Tunneling Doesn't Occur When The Target Device Blocks Outbound Port 22 (SSH) Traffic | NCCF-13859 |
| Core | LSI Physical Drives Aren't Discovered by the Windows Probe When Scanning a VMware ESXi Server | BEAT-1075 |
| Endpoint Detection and Response | Add A "Reboot Required Details" Metric To The EDR Status Services | KUIP-1886 |
| Monitoring | "Scan Now" Isn't Working For Agent-Monitored Services | BEAT-1733 |
| Security | CVE 2020-15909 Session ID anomaly detection has been added, binding the session ID to the client IP address and user agent. This is configurable in N-central, with both protections defaulting to "On". Partners should review the settings under Administration > Mail and Network Settings > Network Security on upgrade and adjust as needed. Please see this KB Article for additional details. | NCCF-13912 |

Release 2020.1 HF1

| CATEGORY | DESCRIPTION | BUG |
|----------|---|------------|
| Core | Remote Control SSH Port-forwarding Allows Access to Internal Backend Services | NCCF-14021 |
| Core | Agent & Probe Settings won't load without Registration Tokens permission | NCCF-13951 |

| CATEGORY | DESCRIPTION | BUG |
|----------|---|------------|
| Core | Corrected a bug impacting server recovery | NCCF-13876 |
| Core | Upgrading N-central Fails If the Azure Agent Had Been Manually Installed | NCCF-13816 |
| Core | Failing To Connect To The Cache Of One Windows Probe Doesn't Cause The Windows Agent To Try Connecting To Other Windows Probes In The Environment | NCCF-13697 |
| Core | XMPP Module Causes A Memory Leak In The Linux Agent | NCCF-13456 |
| Core | Virtual Machines Aren't Displayed Under the "Asset -> Hyper-V Guests" Tab | NCCF-12339 |
| Security | Addresses an Apache Struts vulnerability (CVE-2019-0233) and a Boot Hole GRUB2 vulnerability (CVE-2020-10713) | NCCF-14062 |
| | | NCCF-14068 |

Release 2020.1

| CATEGORY | DESCRIPTION | BUG |
|----------|---|------------|
| Core | RDP Remote Control Times Out Too Quickly | NCCF-13949 |
| Core | RDP Remote Control Doesn't Properly Parse the "Application To Run" Field When it Contains Forward-Slashes | NCCF-13825 |
| Core | Exclude checking primary IP against excluded IP for device match | NCCF-13692 |
| Core | The Datastore (VMware) Service Is Misconfigured, and Reports "201 No data could be retrieved" | NCCF-13658 |
| Core | Error Thrown When Sorting the Recent Tickets Widget by the "Assigned Users" Column | NCCF-13585 |
| Core | The "Settings > Local Agent > Capture Logs" Feature Fails to Retrieve the Agent's Logs | NCCF-13584 |
| Core | Resolve PSA notifications are not being received | NCCF-13523 |
| Core | PSA: Lack of device class mappings can lead to export of unrelated devices | NCCF-13459 |

| CATEGORY | DESCRIPTION | BUG |
|----------|--|------------|
| Core | Dgrid Memory Leak on the Active Issues View | NCCF-13438 |
| Core | Request assistance button no longer linking to startcontrol | NCCF-13420 |
| Core | Submit Queue is held up waiting on notification processing | NCCF-13410 |
| Core | Changing the Font in Custom Branding Throws an "An error was generated when trying to apply custom style" Error Message | NCCF-12739 |
| Core | The Synchronize Button Under "Administration -> Mail and Network Settings -> Network Setup" Is No Longer Needed | NCCF-12179 |
| Core | Inconsistency of error messages in 'Name' fields | NCCF-11694 |
| Core | Discovery Jobs Don't Allow VMware Credentials That Include an Underscore Character | BEAT-1425 |
| Core | Agent Proxy Credentials Not Correctly Transferred To Take Control | NCCF-13512 |
| Core | Erroneous NCSAI Failure in System Health Report when Using the "Regenerate Report" Button | NCCF-13315 |
| Core | The Windows Agent Fails to Log to VeritasModule.log | NCCF-13216 |
| Core | Tools -> Command Prompt Drops Letters During Copy/Paste | NCCF-13097 |
| Core | Possible Denial Of Service Attack Vector in the Password Reset Screen | NCCF-13040 |
| Core | Workstation-Linux Devices Consume a Server License Instead Of A Workstation License | NCCF-13019 |
| Core | Viewing the License Usage Report in Firefox Shows "0NaN-undefined" in the Details Table | NCCF-12949 |
| Core | Agents Ability to Download Their Config From N-central Is Blocked by a Slow PME Thread | NCCF-12946 |
| Core | PSA (Autotask) - In-Product Description of the "Acknowledge Notifications and Suppress All Escalation" Option Is Missing | NCCF-12933 |
| Core | Tools -> Applications Doesn't List Applications When They Have A "ReleaseType" Value In The Registry | NCCF-12901 |

| CATEGORY | DESCRIPTION | BUG |
|----------|--|------------|
| Core | The Job Status Page Shows The Scheduled Time In The Wrong Timezone | NCCF-12891 |
| Core | The {{ConfigurationParameters}} Notification Variable Can Display Passwords In Plain Text | NCCF-12842 |
| Core | API times out when not limiting results from Active issues list | NCCF-12818 |
| Core | System Error When Transferring Tasks Between Probes | NCCF-12805 |
| Core | Agent installer crashes when handling duplicate asset tag error during registration | NCCF-12757 |
| Core | Unrelated Juniper Switches Are Being Flagged As The Same Device | NCCF-12696 |
| Core | Rebooting a Device Clears the Logged in User Column | NCCF-12668 |
| Core | The Device-level Operating System Drop-Down Does Not Contain "Microsoft Windows Storage Server 2012 R2 Standard" and "Microsoft Windows Storage Server 2012 R2 Standard x64" | NCCF-12667 |
| Core | Default SNMP Settings Aren't Applied To Devices If They Are Imported as Essentials Nodes | NCCF-12650 |
| Core | Manually Installing An Agent Can Cause Service Templates To Add More Than The Configured "maxinstances" Of A Service | NCCF-12647 |
| Core | PSA Integration (ConnectWise) - Customer Mapping Page Is Blank Due to Filter Timeouts | NCCF-12643 |
| Core | Automation Manager Policies Are Being Executed More Than Once | NCCF-12542 |
| Core | System Error When A User With Access to "Customer1" Tries to Access a Device That's Been Moved from "Customer2" to "Customer1" | NCCF-12487 |
| Core | System Error When Running The Windows Event Log Report | NCCF-12466 |
| Core | Rules Icon Shows "SO Level" For Customer-level Rules | NCCF-12450 |
| Core | The GUI Installer for the macOS Agent Isn't Usable Dark Mode | NCCF-12400 |
| Core | Sorting Discovery Jobs by the Last Reported column is Alphabetical rather | NCCF- |

| CATEGORY | DESCRIPTION | BUG |
|--------------------|--|------------|
| | than Date | 12229 |
| Core | Notification Profiles Triggered Within 4 Seconds Of Midnight Will Not Generate A Notification | NCCF-12227 |
| Core | Notifications Incorrectly Generated While A Server Is Rebooting During a Maintenance Window | NCCF-12195 |
| Core | Stock filter MSP Backup Devices is configured as custom expression but should be generic | NCCF-11906 |
| Core | Disabling Services from the Active Issues View Logs All Affected Services, for all Selected Devices, in the Device-level Audit Trail | NCCF-11833 |
| Core | Users With Partial Customer Access Are Unable to Run An AVD Scan When Accessing the AV Defender Status Service From The SO Level | NCCF-11795 |
| Core | "Remote Control Defaults" Property Locks Apply To All Device Classes, Not Just The Selected Device Class | NCCF-11756 |
| Core | Some API calls return data when 2FA is enabled | NCCF-11754 |
| Core | Device Not Found When Running Multiple Simultaneous Discovery Jobs Against the Same IP Address | NCCF-11721 |
| Core | XMPP intermittently failing or getting 0% sessions | NCCF-11368 |
| Core | The Agent/Probe Overview Report Doesn't Show Details About Why An Agent Upgrade Failed | NCCF-11156 |
| Core | PSA (Autotask) - Inefficient Fetching of Parent Contracts | NCCF-8528 |
| Core | AMP-based Scheduled Tasks Don't Handle Date-type Custom Properties as Input Parameters | BEAT-1182 |
| Core | HP/Dell/IBM Server Filters Don't Include Linux Devices | BEAT-1118 |
| Core | VMware ESXI Server Serial Number for NEC Server is Not Being Populated | BEAT-1059 |
| Automation Manager | Using a Password-type CDP With an AMP Results in a "The supplied parameters don't match this amp file. The start parameters are not formatted correctly" Error Message | BEAT-1591 |
| Automation Manager | Newly-Created AMPs Unable To Be Opened In Older Versions of Automation Manager | AM-2437 |

| CATEGORY | DESCRIPTION | BUG |
|---------------|---|-----------|
| MSP Backup | MSP Backup Dashboard Failing To Update When the "MaintMSPBackupCloudSync" Script Fails | NSBM-3683 |
| Patch Manager | PME unable to communicate to RPC server over 127.0.0.1 | NCPM-4387 |
| Patch Manager | Automatic patch approvals broken after deleting a customer | NCPM-4324 |
| Patch Manager | Missing Patches report "summary" and "details" inconsistency | NCPM-4272 |
| Patch Manager | Some patch approvals may not take effect | NCPM-4202 |
| Patch Manager | Agent utilizing high CPU due to superseded updates | NCPM-4146 |
| Patch Manager | Patch Status V2 not noting 'last' maintenance windows | NCPM-4122 |
| Monitoring | Upgrade to 2020.1.0.55 Failed Due to Data Type Updates in the Veeam Job Status Service | BEAT-1616 |
| Monitoring | Unable to switch "Enable Field Editing": to "ON" in Custom SNMP Service | BEAT-1497 |
| Monitoring | Remove "WMI" from the Name of the "Active Directory 2012 - DRA (WMI)" Service | BEAT-1154 |
| NetPath | The NetPath Service Isn't Returning to Normal Once The Underlying Issue Has Been Resolved | BEAT-1331 |
| Topology | Topology job specific credentials are lost if the job is changed | BEAT-1139 |
| Topology | IndexOutOfRangeException exception in topology Enrichment service. | BEAT-1041 |

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 " <i>KBA20020: Configuring A Server With Multiple NICs</i> " in the online Help. | 67778 |

Automation Manager

| DESCRIPTION | BUG |
|---|-------|
| Running Automation Manager Policies created using Automation Manager 1.6 or earlier may result in <code>Failed to create an EndDate ... errors</code> if the Policies are run on a computer using a different date format. This issue does not affect Policies created using Automation Manager 1.7 or later. | 65712 |

AV Defender and Backup Manager – D2D

| DESCRIPTION | BUG |
|--|----------|
| Custom Settings option no longer available in 10 for backup profiles. | NSBM-709 |
| 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 |
|---|------------|
| <p>Installing SolarWinds N-central on Servers that have an Nvidia Video Card</p> <p>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.</p> | 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 |
| <p>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.</p> <p>To resolve this issue, perform the following:</p> <ol style="list-style-type: none"> 1. In the Chrome address bar, type <code>chrome://flags/</code>. 2. Under Enable NPAPI, click Enable. 3. Restart Chrome. | 73359 |

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 | <p>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.</p> <p>Server Grade hard drives connected to a RAID controller with a Battery/Capacitor Backed Cache are Required. Examples include 10K+ RPM SCSI or SAS drives, Enterprise Grade SSDs or NVMe for bare metal and virtualized hosts, or a Fibre Channel connected SAN with Enterprise Grade hard drives for virtualized hosts (<i>Fibre Channel cards can be used for bare metal if they are configured in the pre-boot environment and do NOT require vendor-provided drivers</i>).</p> <p>Although Desktop Hard Drives will work with the Operating System, they do not meet the minimum throughput required for the back-end Database of SolarWinds N-central.</p> |

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

System requirements by number of devices managed

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

| NUMBER OF DEVICES | CPU CORES | MEMORY | STORAGE |
|-------------------|-----------|-----------|-------------|
| Up to 1,000 | 2 | 4 GB RAM | 80 GB RAID |
| Up to 3,000 | 4 | 8 GB RAM | 150 GB RAID |
| Up to 6,000 | 8 | 16 GB RAM | 300 GB RAID |
| 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 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 NVMe. SSD and NVMe drives must have an endurance rating of at least 0.2 DWPD (Drive Writes Per Day), and at least 2 physical disks in a redundant RAID array. On Bare Metal servers, the RAID array must appear to the operating system as a single Block or NVMe Device. Currently, many PCIe and NVMe drives do not meet this last requirement and would only work in a virtualized environment.
6. Configure the RAID controller to use the default stripe size and a Read/Write cache of 50%/50%.

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

| SUBSYSTEM | LIMIT |
|-----------------------------------|--|
| Minimum disk space | 80GB |
| Maximum physical disk size (BIOS) | 2TB |
| Maximum physical disk size (UEFI) | 50TB |
| 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 | <p>It is impossible to guarantee the scalability or performance of a SolarWinds N-central server deployed on a Virtual Machine due to:</p> <ul style="list-style-type: none"> ■ variability in field environments resulting from host server configurations, ■ the number of virtual guests run on the host server, and ■ the performance of the underlying host hardware. |
| Supportability | <p>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.</p> <p>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.</p> |
| Virtual Hardware Support | <p>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.</p> <p>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.</p> |

| | |
|-------------------------|---|
| 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 cause memory swapping to disk, and other bottlenecks that can impact guest system performance.
- Ensure that the system has enough RAM and hard drive space to provide permanently allocated resources to the 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 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 LTSC | Windows 10 Enterprise 2016 LTSC |
| Windows 10 Enterprise for Virtual Desktops | Windows 10 Enterprise LTSC 2019 |
| Windows 10 Pro | Windows 10 Pro Education |
| Windows 10 Pro for Workstations | |
| | |
| Windows Server 2008 R2 Enterprise | Windows Server 2008 R2 Datacenter |

| | |
|---|---|
| Windows Server 2008 R2 Standard | Windows Server 2008 R2 Foundation |
| Windows Server 2012 Datacenter | Windows Server 2012 Essentials |
| | |
| Windows Server 2012 Foundation | Windows Server 2012 R2 Datacenter |
| Windows Server 2012 R2 Essentials | Windows Server 2012 R2 Foundation |
| Windows Server 2012 R2 Standard | Windows Server 2012 R2 Standard Evaluation |
| Windows Server 2012 Standard | |
| | |
| Windows Server 2016 Datacenter | Windows Server 2016 Datacenter Evaluation |
| Windows Server 2016 Essentials | Windows Server 2016 Standard |
| Windows Server 2016 Standard Evaluation | |
| | |
| Windows Server 2019 Datacenter | Windows Server 2019 Essentials |
| Windows Server 2019 Standard | Windows Server 2019 Standard Evaluation |
| | |
| Windows Server Datacenter | |
| Windows Small Business Server 2011 Essentials | Windows Small Business Server 2011 Standard |

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 2020.1 HF5 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 |

© 2020 SolarWinds MSP Canada ULC and SolarWinds MSP UK Ltd. All rights reserved.

No part of this document may 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 written consent of SolarWinds MSP Canada ULC ("SolarWinds MSP"). All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds MSP and its respective licensors.

SOLARWINDS MSP DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS MSP, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS MSP HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds MSP and N-CENTRAL marks are the exclusive property of SolarWinds MSP Canada ULC and its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds MSP trademarks, service marks, and logos may be common law marks, registered or pending registration in the United States or in other countries. All other trademarks mentioned herein are used for identification purposes only and may be or are trademarks or registered trademarks of their respective companies.

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.