RELEASE NOTES

Solarwinds N-central

Version 11.1 SP1 HF1

solarwinds msp

Last Updated: Monday, April 16, 2018

Upgrade paths and notes

To upgrade to 11.1 SP1 HF1, your Solarwinds N-central server must be running one of the following versions:

- Solarwinds N-central 11.0.0.1079-1150
- Solarwinds N-central 11.0.1.985-1237
- Solarwinds N-central 11.1.0.647-1350
- Solarwinds N-central 11.1.1.166+

Note the following when upgrading Solarwinds N-central.

Agents currently on unsupported Operating Systems such as XP and 2003, will not upgrade but will remain functional.
Scheduled Tasks may expire if the Agent on an associated device is being upgraded when the task is scheduled to be completed. Agent upgrades are normally short in duration but may be delayed if a restart of the device is pending.

Fixed Issues in Solarwinds N-central 11.1 SP1 HF1

CATEGORY	DESCRIPTION	BUG
MSP Backup	An issue causing a System Error to be displayed in MSP Backup Profiles on expired trials has now been resolved.	NSBM-1897
MSP Backup	An issue impacting cloned MSP Backup Profiles from populating as well as blocking the ability to access has now been resolved.	NSBM-1882
PSA	An issue blocking Autotask integration has now been resolved.	NPSA-1830
PSA	ANTS for services which were not touched during trigger modifications will no longer be deleted.	NPSA-1814
Patch Manager	The API call to Windows Update Agent patch detection exhausting allocated memory resources, causing a `Generic WUA error (0x80240FFF)` has now been resolved.	NCPM-3110
Core	Struts Vulnerability CVE-2017-15707.	NCCF-6897
Core	Corrected the behavior involving the Agent reinstall not working if a device is in Unscheduled Downtime.	NCCF-6878
Core	The behavior involving DirectSupport calls timing out due to common locks on both send and receive threads has now been corrected.	NCCF-6866
Core	Resolved the issue causing the Active Issues view to not load.	NCCF-6857
Core	An issue if the HP Warranty soap call fails causing the failover method to run into a Null Pointer Exception, has been corrected.	NCCF-6771

Fixed Issues in Solarwinds N-central 11.1 SP1

CATEGORY	DESCRIPTION	BUG
MSP Backup	Backup Profiles now support using apostrophe's in the profile name.	NSBM-1880
MSP Backup	Improved behavior involving deactivated MSP Backup account receiving system errors and preventing user from moving devices.	NSBM-1884
Solarwinds N-central Backup and Recovery	Improved behavior surrounding integration connections between MSP Backup and N-central that were causing socket timeouts.	NSBM-1769
AV Defender	An issue causing USB scan run to reset the Days since last successful scan to zero has been corrected and will no longer reset the [days since last scan] detail in AV Defender Status Service.	NSBM-1879
AV Defender	Changes have been made to improve the server performance when impacted by large amounts of quarantined items.	NSBM-1875
AV Defender	An issue blocking an upgrade as a result of Third party Antivirus product being detected has now been resolved.	NSBM-1846
AV Defender	Corrected behavior involving proxy settings which was causing updates to fail.	NSBM-1760
AV Defender	Improved behavior surrounding reboot handling during device hibernation events ensuring reboot will be picked up in the next available maintenance window.	NSBM-1739
PSA	We have resolved the inconsistencies when using Run Now in AutoTask affecting AutoTask Billing.	NPSA-1785
PSA	Improved performance impact on the UI when PSA Export is in process.	NPSA-1739
PSA	A problem resulting in a system error when attempting to create tickets in MSP Manager as a result of permission handling, will now yield the message; "You do not have permission to view the notification schedule".	NPSA-1734
PSA	We have implemented connection pooling to address servers becoming unresponsive and requiring reboot.	NPSA-1721
PSA	Resolved an issue where the ConnectWise REST will be able to display tickets that do not have a due date.	NPSA-1805

Category	Description	Bug
PSA	A problem causing MSP Manager status to not update when only custom status is sent has now been resolved.	NPSA-1690
PSA	An issue that prevented MSP Manager ticket creation for N-central has been fixed.	NPSA-1674
PSA	An issue causing notifications to randomly not be sent after incident detection has now been resolved.	NPSA-1665
PSA	Improved performance handling for ConnectWise requests involving long customer lists.	NPSA-1663
PSA	An issue preventing the Notification bell functionality to work has now been addressed.	NPSA-1649
PSA	Improved ConnectWise customer mapping to handle scenarios when mapped customers no longer exists.	NPSA-1646
PSA	An issue with ConnectWise Rest API failing to create ticket emails correctly has now been resolved.	NPSA-1641
PSA	An issue preventing MSP Manager Time entries from being attached has now been resolved.	NPSA-1632
PSA	Improved performance handling for ConnectWise request for companies when the 'Annual Revenue' is too big, which was causing issues with Customer mapping.	NPSA-1628
PSA	An issue causing global notifications at the customer level setting to be ignored has now been resolved.	NPSA-1617
PSA	An issue causing Ticket status to stop working as a result of a ticket being moved to a different board has now been corrected.	NPSA-1596
PSA	Corrected display issue involving the Incident Summary CVS report which was causing all columns to shift if there was no connection between Incident and device.	NPSA-1537
PSA	An issue causing MSP Manager Device Exports to deselect the Remote Control option has now been resolved.	NPSA-1521
PSA	Improved the behavior surrounding invalid entries in Customer Mapping to no longer cause System Error when amending customers.	NPSA-1514
PSA	Restored Billing profile display when creating a new site via Action -> New Site or Administration for the given Service Organization	NPSA-1416

CATEGORY	DESCRIPTION	BUG
Patch Manager	An issue where meta data for 3rd party patches may become out of date has been resolved.	NCPM-3096
Patch Manager	Optimizations surrounding agent resource utilization have been applied to improve performance.	NCPM-3080
Patch Manager	Corrected the behavior when filtering for Patch by KB Article ID which would result in no results or may have resulted in a system error.	NCPM-3029
Patch Manager	An issue that can cause the possibility of creating wrong supersedence relationships between patches has been corrected.	NCPM-2963
Patch Management	Restored display of Install Date for Security only Updates.	NCPM-3037
Patch Management	An issue causing Firefox updates to install the wrong language version has been corrected.	NCPM-3012
Patch Management	An issue causing Agent install pop up to show all patches when it should only be displaying missing patches has now been corrected.	NCPM-2976
Patch Management	An issue causing the Agent to send incomplete patch scans has been corrected.	NCPM-2975
Patch Management	Corrected behavior to ensure FileDownloader to use the correct WebProxy settings.	NCPM-2948
Core	An unmanaged asset cannot be shown in Active Issues.	NCCF-6765
Core	Automation Manager temp folder will now be maintained to delete expired temp files regularly.	NCCF-6738
Core	Resolved the System Error displayed when you select a Discovery job after adding a default SNMP profile to the customer.	NCCF-6714
Core	Resolved the issue causing a System Error on new AMP based custom service.	NCCF-6678
Core	Restored the ability to allow AWS installs to reset passwords when something goes wrong.	NCCF-6664
Core	An issue preventing the ability to locate datastores on vCenter has now been resolved.	NCCF-6609
Core	Self-Healing task output directory has been moved from Root.	NCCF-6731

CATEGORY	DESCRIPTION	BUG
Core	Improvements to address agent/probe upgrade failures have been added such as added logging and changing the windows start up order.	NCCF-6726
Core	Corrected error handling when changing Default Thresholds for a service with a Boolean metric.	NCCF-6715
Core	An issue prohibiting remote control due to Azure WA Agent verbose logging has now been corrected.	NCCF-6673
Core	An issue causing remotely executed Automation Policies to show all devices as potential targets has now been resolved.	NCCF-6658
Core	An issue causing Shadowprotect SPX to go misconfigured has now been resolved.	NCCF-6646
Core	Restored the AV defender custom scan functionality.	NCCF-6627
Core	An issue with two-step verification causing the backup code to fail at login and resulting in a System Error has now been corrected.	NCCF-6619
Core	An issue causing the agent monitoring services to go stale has now been resolved.	NCCF-6593
Core	A problem where the asset scan causes the MSI Installer to refresh all packages, resulting in numerous log entries, has now been resolved.	NCCF-6574
Core	The device-level Audit Trail will now sort properly by User column.	NCCF-6517
Core	An issue resulting in a system error when modifying Customer-level ExternalIDs due to permission handling has now been resolved.	NCCF-6515
Core	A pre-11.1 agent with an ODBC Query service will now work without having to upgrade agent after server upgrade to Solarwinds N-central11.1.	NCCF-6504
Core	An issue causing the Domain User Management to show duplicate domains has been corrected.	NCCF-6496
Core	If a service is configured for Self Healing, opening up the Service Details will now navigate to the Status tab.	NCCF-6484
Core	Various help links from the agent/probe no longer showing a 404 link.	NCCF-6468
Core	The RAID controller status monitoring has been corrected ensuring mapping VMware native health value statuses corrected.	NCCF-6461

CATEGORY	DESCRIPTION	BUG
Core	Improvements have been made to reduce bloat on the Security Audit Log table for those using the API call to create an automated wallboard.	NCCF-6459
Core	The Raw Monitored Data report will now show all applicable metrics when run against the HTTP or HTTPS services.	NCCF-6455
Core	License Limit calculations have been corrected for Site Level devices.	NCCF-6394
Core	We have resolved the scenario where manually adding an Ubuntu device with automatic agent installation would revert to manual agent installation.	NCCF-6350
Core	XMPP send() messages will no longer be significantly delayed causing Remote Execution Tasks to not be retrieved until after they're expired.	NCCF-6203
Core	An issue causing Solarwinds N-central to crash the Windows WMI service has been resolved.	NCCF-6185
Core	VMware DIMM memory status will now return the correct value.	NCCF-6178
Core	A Service Template used in a rule will no longer be allowed to be modified while the rule is processing.	NCCF-6134
Core	An issue of multiple devices reporting failed logins has been resolved using portscan to verify the existance of the device/port.	NCCF-6109
Core	An issue causing adverse behavior with AV Defender such as displaying errors, profile not applying, protection status not displaying has been resolved.	NCCF-6091
Core	Enhancements have been made to reduce verbose logging for Azure WA Agent.	NCCF-5915
Core	An issue caused by trailing spaces in ShadowProtect job names resulting in ShadowProtect SPX service misconfigured with an Error: 201 Get SPX job data failed. This has now been addressed by trimming the spaces.	NSBM-1734
Core	An issue causing the Ubuntu agent monitoring to go into a stale state has now been resolved.	NCCF-6506
Core	An issue causing integral pieces of N-central software to be reported as a virus has now been corrected.	NCCF-6471
Core	Restored the ability to save Notification Recipients in asset jobs.	NCCF-6424
Core	An N-central deadlock preventing task changes from being saved has now been	NCCF-

CATEGORY	DESCRIPTION	BUG
	corrected.	6399
Core	An issue causing Veeam and Windows backup Discovery to fail due to special characters has been corrected.	NCCF-6380
Core	An issue preventing SMS Registration functionality has been corrected.	NCCF-6362
Core	An issue causing ESX or VMWare services to go stale preventing the ability to login, or lock as a result of the Base64 to plain text conversion on upgrade has now been corrected.	NCCF-6349
Core	An issue causing Built-in policy Veeam Job Monitor fails when jobs are in process on Veeam 8 & 9 has been corrected.	NCCF-6343
Core	An issue causing Cron based export for non-RM export to fail due to incorrect file owner has now been corrected.	NCCF-6339
Core	Backup Manager (UDP) has been added to Maintenance Windows.	NCCF-6337
Core	An issue causing upgrade failure when Agent/Probe failure notification profiles' default trigger has been deleted has been corrected.	NCCF-6322
Core	The Solarwinds N-central SNMP v3 library has been updated, which resolves a problem where the SNMP v3 handshake was failing.	NCCF-6315
Core	ActiveIssuesList API call will no longer return a "5000 Query Failed" error if a probe with a failed probe status service, the behavior has been improved to return as a failed service.	NCCF-6311
Core	Restored behavior populating the Anti-phishing table in the ODS and the warehouse DBS.	NCCF-6246
Core	Site/Customer name is now shown at the Customer Level for the Scheduled Tasks page to easily distinquish Site/Customer.	NCCF-6191
Core	An issue with NKO stopping and preventing upgrade failures has been corrected.	NCCF-6187
Core	Occasionally the ability to filter for "Customer Name" would return no results or system errors has now been corrected.	NCCF-6177
Core	An issue preventing the ability to delete system backups through UI as a result of files being owned by root has now been corrected.	NCCF-6148
Core	An issue exists when using Service template to manually add the Reboot	NCCF-

CATEGORY	DESCRIPTION	BUG
	Required service to a device causing a System Error, this has now been corrected.	6147
Core	Improved behavior involving the ability to edit a cloned rule while it's running.	NCCF-6131
Core	Refined permission handling surrounding the ability to add/edit Scheduled Task scripts.	NCCF-6121
Core	Performance improvements applied to Service template to improve handling for large templates	NCCF-6110
Core	An issue causing patch approval to display last updated dates predating the device creation has now been corrected.	NCCF-6108
Core	An issue causing the Agent account status to incorrectly flip to Account Enabled or Account Disabled has been corrected	NCCF-6104
Core	Corrected behavior which was causing a system error when changing own user password.	NCCF-6093
Core	An issue preventing AV Defender to upgrade has now been corrected.	NCCF-6091
Core	An issue causing the Linux agent monitoring to go stale on receiving second agent upgrade request has been corrected.	NCCF-6080
Core	Performance improvements applied in response to a random occurrence of the N-central Monitor Server Maxing CPU.	NCCF-6076
Core	Generating a Certificate Signing Request (CSR) will now succeed when using spaces in the available fields.	NCCF-6063
Core	Updated the help tool tip to be consistent with documentation for Connectivity Packet Interval.	NCCF-6053
Core	A random issue causing the server to become unresponsive or causing a system error when modifying the Service Template has been corrected.	NCCF-6050
Core	Reference for cdyne link has been updated.	NCCF-6047
Core	Improved behavior involving the ability to move a device linked to a probe with multiple identically named discovery jobs at different sites to ensure a system error is not returned.	NCCF-6046
Core	Behavior corrected for Service metrics exported csv file to display min/max/avg	NCCF-

CATEGORY	DESCRIPTION	BUG
	instead of raw data.	6045
Core	An issue blocking a remote execution task to succeed when no remote share parameters are specified as this is an optional parameter has now been corrected.	NCCF-6043
Core	An issue causing Dashboard Service filter from returning correct results has been resolved.	NCCF-6036
Core	An incorrect service status of 'None' was causing filtering issues on the Dashboard. This option has now been removed.	NCCF-6033
Core	An issue with discovery MAC Address Exclusion list malfunctioning due to white space on MAC Addresses has now been corrected.	NCCF-6019
Core	An issue with the "Windows Server Performance Counters" service reporting a Misconfigured state due to a missing threshold has been corrected.	NCCF-6017
Core	We have updated the Solarwinds N-central kernel to prevent the CVE-2017-1000364 exploit.	NCCF-6016
Core	Direct Support Domain User Management has been optimized to prevent timeouts.	NCCF-6001
Core	Optimized Agent logging to processing "resume"- type Power events to avoid logs from filling up and preventing the Agent from starting.	NCCF-5999
Core	A random issue causing the server to become unresponsive or causing a system error when scheduling tasks due to a deadlock has now been corrected.	NCCF-5980
Core	An issue resulting in "unknown" displayed in Audit trail when using the scan now feature on any service has now been corrected to provide action and details in the Audit trail.	NCCF-5979
Core	Improved behavior to ensure Agent will succeed in updating when Windows Installer services are running at the same time.	NCCF-5972
Core	An issue causing Process (SNMP) service thresholds from not displaying correctly has been corrected.	NCCF-5969
Core	An issue causing remote control and upgrades to fail due to Log partition being full has been corrected.	NCCF-5915
Core	An issue with 64 bit Firefox on Windows 8.1 closing the window when user selects the status drop down on any probe (Administration -> Probes) when it should be expanded has now been corrected.	NCCF-5891

CATEGORY	DESCRIPTION	BUG
Core	An issue with uploading an AMP with fewer parameters not updating Service Template Service Parameters has been corrected.	NCCF-5697
Core	Improved behavior during probes upgrade when credentials are not valid.	NCCF-5684
Core	An issue where the Ethernet Errors service was mashing together both the interface name and it's alias has been resolved.	NCCF-5671
Core	Corrected sorting for "CPU Usage (%)" in Service Details.	NCCF-5648
Core	An issue with Mac Agent memory service reporting No Data or Stale on OSX device has now been corrected.	NCCF-5502
Core	An issue causing Scheduled Tasks status to display differently when viewed by SO level has now been corrected.	NCCF-4656
Core	Changed behavior when modifying customer to ensure UI remains res.	NCCF-3604
Automation Manager	Fixed an issue where a path exception error occurred when running a custom policy to create mapped drives.	AM-1890
Automation Manager	Fixed an issue where AMP services based on Power Shell script object switched to misconfigured state.	AM-1885
Automation Manager	Fixed an issue where the "Get Desktop Monitor Information" object, on some versions of Windows, does not provide complete information for multiple monitors .	AM-1821
Automation Manager	Fixed an issue where NCentralLauncherService.exe process was conflicting with the Mimecast Outlook plugin process causing the Mimecast plugin to fail.	AM-1804
Automation Manager	Fixed an issue where the "*" wildcard was not working on the "Is Application Installed" object.	AM-1789
Automation Manager	Fixed an issue where an application specified inside the "Run Program" object would not run when using custom credentials.	AM-1766
Automation Manager	An issue where the NCentralLauncherService.exe process was conflicting with the Mimecast plugin for Microsoft Outlook has been resolved.	AM-1804
Automation Manager	An issue where the Automation Manager policy that underpins the "UAC Enabled" service was querying an incorrect registry key has been resolved.	AM-1793
Automation	The "Is Application Installed" object now properly handles the * character as a	AM-

CATEGORY	DESCRIPTION	BUG
Manager	wildcard.	1789
Automation Manager	The "Run Program" object now properly supports the use of custom credentials.	AM-1766
ArcServe UDP	An issue where the monitoring of ArcServe backups would erroneously show a Warning for "days since last recovery" message has been resolved.	NSBM-1802
ArcServe UDP	Fixed an issue where 3 failed upgrade attempts would result in the backup manager status losing reporting information surrounding backups running. Data will now show up in the backup status service in the event of an upgrade failure.	NSBM-1797

Known Limitations

Known limitations for the current version of the Solarwinds N-central software is composed of issues that may significantly impact performance whose cause has been replicated by SolarWinds MSP, and where a fix has not yet been released. Any of the limitations listed below may not impact every customer environment.

CATEGORY	DESCRIPTION	BUG
Active Issues	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	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	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
Backup Manager – ArcServe	The ability to customize ArcServe UDP backup profiles at the device level has been removed.	NSBM-709
Backup Manager – ArcServe	ShadowProtect Data Reader service is using high CPU due to large amount of historical data as part of the backup.	74971
Backup Manager – ArcServe	The **About Backup Manager** dialog box no longer indicates whether or not the Backup Manager software is licensed.	68226
Custom Services	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	Modifying a Dashboard that is associated with a large number of services may cause performance issues when using the Firefox browser.	70326
Core	Warranty information might be inaccurate when determining the warranty expiry dates of devices that are not located in the USA.	NCCF-3649
Core	Chrome 42.x does not support NPAPI plugins which means that Java and Direct	73359

CATEGORY	DESCRIPTION	BUG
	Connect will not function with that browser version. When attempting to open remote control connections in Chrome 42.x, users will be repeatedly prompted to install either Java or the NTRglobal plugin with no successful connections made. To resolve this issue, perform the following: 1. In the Chrome address bar, type `chrome://flags/`. 2. Under **Enable NPAPI**, click Enable. 3. Restart Chrome.	
Patch Management	Microsoft Security Bulletin MS14-045 announced the withdrawal of four individual Windows updates due to security issues. This security bulletin applies to: • Windows RT and Windows RT 8.1 • Windows Server 2012 and Windows Server 2012 R2 • Windows 8 and Windows 8.1 • Windows Server 2008 and Windows Server 2008 R2 • Windows 7 • Windows Vista • Windows Server 2003 The following updates were withdrawn: •2982791 •2970228 •2975719 •2975331 If any of these updates have been installed on managed devices, refer to the security bulletin about how to resolve security risks.	67830
Patch Management	It is strongly recommended that your Update Server not be a device that requires uninterrupted disk access (for example, an Exchange server or a web server) as update functionality can be disk-intensive.	n/a
PSA Integration	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.	65620

CATEGORY	DESCRIPTION	BUG
	This will allow the stale ticket check to remove the ticket from the system.	
UI	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

Known Issues

Known issues for the current version of the Solarwinds N-central software is composed of issues that may significantly impact performance whose cause has been replicated by SolarWinds MSP, and where a fix has not yet been released. The latest list of known issues can be found at the following location:

https://community.solarwindsmsp.com/Support/Known-Issues

Any of the known issues may not impact every customer environment.

End of Support

Solarwinds N-central 11.1 SP1 HF1 no longer supports the following technologies.

Linux	The Linux agent will no longer support CentOS 5.x. The Linux agent will no longer support CentOS 6.6 and earlier.
Autotask Integration	The legacy method of configuring integration between Solarwinds N-central and Autotask (Autotask Built-in Integration) is deprecated.
Windows	Windows XP and Windows 2003 Support for Windows XP and Windows 2003 has been deprecated. As a result, the Windows Agent and Windows Probe will no longer install on machines running those operating systems. The Windows Probe can continue to monitor those machines though, and existing Agents and Probes running on those machines will continue to function.
Web Browsers	Older versions of Chrome, Firefox, Edge and Internet Explorer. Solarwinds N-central only supports the latest versions of these browsers.
Remote Support Manager (RSM)	Upon upgrading to Solarwinds N-central 11.1 SP1 HF1, any installed RSM will be removed and a reboot may occur during your maintenance window. IIS Express will remain installed if it needs to be used by additional applications.

The following services will be deprecated in a future release.

AV Monitoring	All AV monitoring will now be done with the AV Status script/service. As a results all AV Activity and Av Def services will be removed, with the exception of AVDefender.
Generic SQL Server	Generic SQL Server service has been replaced by SQL TCP Availability service.
Service Groups	Service Groups will be deprecated.
Reports	The following reports will be deprecated: ▪ Security Incident Summary ▪ Security Incidents by Service ▪ Security Incidents by Device
Intel	Intel vPro & Intel AMT services will be removed.

<table>
<tr><td rowspan="14">Cisco Call Manager 4.x</td><td colspan="2">Support for <i>Cisco Call Manager 4.x</i> has been deprecated; as a result, the following WMI-based services will be removed from Solarwinds N-central:</td></tr>
<tr><td>CUCM ccmGateways (Cisco)</td><td>CUCM ccmGroupName (Cisco)</td></tr>
<tr><td>CUCM ccmPhone (Cisco</td><td>CUCM ccmStatus (Cisco)</td></tr>
<tr><td>All of the CUCM Critical Processes" services</td><td>CUCM CTIDevices (Cisco)</td></tr>
<tr><td>CUCM MediaDevices (Cisco)</td><td>CCM ISDN - Primary Rate Interface</td></tr>
<tr><td>CUCM VoiceMailDevice (Cisco)</td><td>CCM Server</td></tr>
<tr><td>CCM Music on Hold</td><td>CCM Call Activity</td></tr>
<tr><td>CCM Annunciator</td><td>CCM Analog Gateway FXS Port</td></tr>
<tr><td>CCM Performance</td><td>CCM MTP - Transcoder</td></tr>
<tr><td>CCM Analog Gateway</td><td>CCM ISDN - T1 Trunk</td></tr>
<tr><td>CCM CTI Activity</td><td>CCM Conf Activity</td></tr>
<tr><td>CCM ISDN - Basic Rate Interface</td><td>CCM ISDN - T1 Trunks</td></tr>
<tr><td>CCM Analog Gateway FXO Port</td><td></td></tr>
</table>

Solarwinds N-central System Requirements

The following requirements are for typical usage patterns, acknowledging that some patterns may require greater system resources from an 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	Intel Xeon E5-2600 series or similar.
Operating System	You do not need an OS to run Solarwinds N-central. The Solarwinds N-central ISO includes a modified version of CentOS 6.x.
Physical Hardware	The hardware used for a physical Solarwinds N-central server (non-virtual machine) must be certified to run Red Hat Enterprise Linux 6.7 (x64) by Red Hat or the hardware vendor. Login to your Red Hat Customer Portal for more details.

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	75 GB HDD
Up to 3,000	4	8 GB RAM	150 GB HDD
Up to 6,000	8	16 GB RAM	300 GB HDD
Up to 9,000	12	24 GB RAM	450 GB HDD
Up to 12,000	16	32 GB RAM	600 GB HDD
Recommendation: When managing 15,000+ devices, install Solarwinds N-central in a bare metal environment.			
Up to 16,000	22	48 GB RAM	800 GB HDD
Up to 20,000	28	64 GB RAM	1,000 GB HDD
Up to 24,000	34	80 GB RAM	1,200 GB HDD

Notes

1. Server-grade hard drives (such as SAS, SCSI, or Fibre Channel) are required to ensure performance and power-loss data protection.
2. Hard drives on the Solarwinds N-central server should not be shared with other applications that have significant I/O workloads. For example, Report Manager should not be installed on the same drive as Solarwinds N-central.
3. SolarWinds MSP recommends two or more hard drives be placed in a RAID to improve redundancy. With two drives, RAID 1 must be used. With more than two drives, RAID 1+0 is preferred, but RAID 5 is also an option.
4. Solarwinds N-central must be run on a server with a RAID controller that includes a Flash-Backed Write Cache (FBWC) or Battery-Backed Write Cache (BBWC).
5. Configure the RAID controller to use the default stripe size and a Read/Write cache of 50%/50%.

Examples of supported servers

HP ProLiant DL360 G8 and Dell PowerEdge R720 are examples of servers that are supported if they meet the system requirements. SolarWinds MSP recommends that for either server, two or more hard drives be placed in a RAID to improve redundancy. RAID 1+0 is preferred (RAID 5 is supported).

Optional modem

A US Robotics USR5610C or a serial modem is required to use paging or SMS notification features.

Support for virtualization environments

Solarwinds N-central supports those versions of VMware ESX Server and Windows Server Hyper-V that are compatible with Red Hat Enterprise Linux 6 (x64). Use the latest stable versions of VMware or Hyper-V are used in order to ensure the best performance and compatibility with Solarwinds N-central.

SolarWinds MSP is committed to providing support to customers using virtualization environments as we do with other Solarwinds N-central certified hardware.

ⓘ If you need to deploy Solarwinds N-central in a Hyper-V environment with more than seven virtual processors or more than 30GB of allocated RAM, contact Technical Support for assistance.

About virtualization

Virtualization provides an abstraction layer between the hardware and the OS 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 an Solarwinds N-central server deployed on a Virtual Machine due to: ▪ variability in field environments resulting from virtualization server configurations, ▪ number of guests run on the virtualization server, and ▪ performance of the underlying VMware system.
Supportability	SolarWinds MSP supports the Solarwinds N-central software deployed in VMware and Hyper-V in the same way that we support Solarwinds N-central deployed in other environments. This support is limited to the components (software and OS) shipped with Solarwinds N-central and does not include troubleshooting of virtualization systems or performance issues related to environmental factors. These are supported on a best-effort basis. In the event of serious performance problems, we might ask you to move the system to a physical hardware deployment.
Generation	Installing Solarwinds N-central as a guest on a Hyper-V server requires that the Virtual Machine is Generation 1. Attempting to install Solarwinds N-central on a Generation 2 Virtual Machine will fail.
Network Adapters (VMware only)	N-central supports both E1000 and VMXNET3. When the VM is configured as Red Hat 6, it will use VMXNET3 by default (which is preferred).
MAC Addresses	Solarwinds N-central does not support dynamic MAC addresses. Static MAC addresses must be configured for the virtual machine where you install Solarwinds N-central.

Recommended configuration for the virtualization server

Provisioning virtual disks as "thin" or "thick" results in nearly-identical performance. Thick provisioning is recommended.

- Assign higher resource access priority to Solarwinds N-central than competing systems.
- Do no over-provision memory on the host system. Over-provisioning causes disk based swapping that impacts system performance.
- Ensure that the system has sufficient RAM and hard drive space to provide permanently allocated resources.

Supported Software

Browsers

Solarwinds N-central supports the latest versions of:

- Internet Explorer®
- Microsoft Edge®
- Mozilla Firefox®
- Google Chrome®

Chrome 42.x does not support NPAPI plugins (including Java and Direct Connect). When you attempt to launch a remote control connection in Chrome 42.x, you will be repeatedly prompted to install Java or the NTRglobal plugin without success.

Workaround:
In the Chrome address bar, type `chrome://flags`.
Under Enable NPAPI, click Enable.
Restart Chrome.

Solarwinds N-central is not supported on Internet Explorer in Compatibility View mode.

Attended Remote Control and Direct Connect remote control connections are not supported on 64-bit browsers.

Remote Control

Remote control connections require the following software on the computers that initiate connections:

- Java 6 Update 20 or greater

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

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`.

Supported Operating Systems

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

Windows Agents require:

- Microsoft .NET Framework 4.5.2 (or later)

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
- 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

- Windows 2008
- Datacenter Server
- Datacenter Server without Hyper-V
- Enterprise Server
- Enterprise Server without Hyper-V
- Essential Business Server
- Foundation Server
- R2 Datacenter Server
- R2 Enterprise Server
- R2 Foundation Server
- R2 Standard Server
- R2 Web Server
- Small Business Server
- Standard Server
- Standard Server without Hyper-V
- Standard Server 64-bit Edition
- Web Server

ⓘ The following are required to install Windows Agents on a server using Windows Server 2008 R2 Server 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.

Microsoft Windows Hyper-V

- Server 2012 64-bit Edition
- Server 2008 R2
- Server 2008

Windows 10

- Microsoft Windows 10 Enterprise & Professional
- Education editions

Windows 8 and 8.1

- 8.1 Enterprise
- 8.1 Enterprise 64-bit Edition
- 8.1 Professional
- 8.1 Professional 64-bit Edition
- 8 Enterprise
- 8 Enterprise 64-bit Edition
- 8 Professional
- 8 Professional 64-bit Edition
- 8 64-bit Edition

Windows 7

- Microsoft Windows 7 Enterprise & Professional
- Microsoft Windows 7 Ultimate

Windows Vista

- Vista Business
- Vista Enterprise
- Vista Ultimate

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.

- CentOS 6.7 and higher (32/64-bit)
- Red Hat Enterprise Linux 6.6 and 7 (32/64-bit)
- Ubuntu 14.04 (LTS build of "Trusty Tahr")
- Ubuntu 16.04 (LTS build of "Xenial Xerus")
- Debian 8.7 32-bit (using Ubuntu Agent DEB version 14 x86)
- Debian 8.7 64-bit (using Ubuntu Agent DEB 14 x64)

Mac Agents

- 10.13 (High Sierra)
- 10.12 (Sierra)
- 10.11 (El Capitan)

- 10.10 (Yosemite)
- 10.9 (Mavericks)

AV Defender

Workstation Operating Systems

- Microsoft Windows Vista SP1
- Microsoft Windows 7
- Microsoft Windows 8, 8.1
- Microsoft Windows 10
- Microsoft Windows 10 TH2
- Microsoft Windows 10 Anniversary Update "Redstone"

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

> 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

Server Operating Systems

- Microsoft Windows Server 2008 R2 SP1
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2 SP1
- Microsoft Windows Server 2016

Unsupported Operating Systems

- Windows XP
- Windows Vista
- 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.

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	✓	✓	✓	✓	✓	✓
MSP Connect	✓	✓	✗	✗	✓	✓
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 11.1 SP1 HF1 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

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.

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 MSP empowers IT service providers with technologies that fuel their success. Solutions that integrate layered security, collective intelligence, and smart automation—both on-premises and in the cloud, backed by actionable data insights, help IT service providers get the job done easier and faster. SolarWinds MSP helps our customers focus on what matters most—meeting their SLAs and delivering services efficiently and effectively. For more information, visit solarwindsmsp.com.