



RELEASE NOTES

SolarWinds N-central

Version 12.2 SP1 HF2 (build 12.2.1.280)



Upgrade paths and notes

To upgrade to 12.2 SP1 HF2, your SolarWinds N-central server must be running one of the following versions:

- SolarWinds N-central 12.1.1.187-450
- SolarWinds N-central 12.2.0.274-350
- SolarWinds N-central 12.2.1.67+

Note the following when upgrading SolarWinds N-central.

Device Auto Import Disabled!

In order to address an information disclosure vulnerability, this hotfix disables the device auto-import feature of SolarWinds N-central. We will reactive this feature in a future release.

Self Signed SSL Certificates!


12.2 no longer supports the ability to use Self-Signed SSL Certificates in conjunction with the LDAP-based SSO module. If you've configured SolarWinds N-central in this manner, upgrading to version 12.2 will remove the self-signed SSL certificate from the SolarWinds N-central certificate store, and as a result you will not be able to login with your LDAP account. We strongly recommend securing your LDAP-based SSO connection with a valid, verified SSL certificate before upgrading to SolarWinds N-central 12.2, so that you do not experience any issues when logging into SolarWinds N-central with your LDAP user account.

Upgrade Agents and Probes!

You will need to upgrade your Agents and Probes to SolarWinds N-central 12.1 SP1 before upgrading to SolarWinds N-central 12.2 SP1 HF2. Without first upgrading to 12.1 SP1, your Agents and Probes won't leverage TLS 1.2 properly, and won't be able to communicate with SolarWinds N-central 12.2 SP1 HF2.

Check your Time Zone Setting!

Before upgrading to SolarWinds N-central 12.2 SP1 HF2, verify your correct Time Zone in the SolarWinds N-central SolarWinds N-central UI and ensure it is a Standard Time Zone, not an Alias. If you are using an Alias Time Zone, an error message will display notifying you to use the Primary (Canonical) IANA time zone name for your location. For more information about Canonical time zone names, please see https://en.wikipedia.org/wiki/List_of_tz_database_time_zones.

-  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 12.2 SP1 HF2

CATEGORY	DESCRIPTION	BUG
Monitoring	Windows Applications and Services Log: Entries in the "Event ID Exclude" Field Are Not Saved.	BEAT-1060
Monitoring	HTTPS Incorrectly Reports a Failed State When Monitoring a Website That Requires Credentials.	NCCF-12492
PSA	The "Recent Tickets" Widget Does Not Work When N-central Is Integrated With Marval.	NCCF-12212
Core	Addresses an information disclosure vulnerability in the Agent self-registration process. Thanks to Justin Oberdorf for bringing this issue to our attention.	NCCF-12687
Core	The "Event Description" Column Isn't Present in the CSV Export of the Windows Event Log Report.	NCCF-11767
Core	Direct Support's TLS Configuration Causes a System Error when attempting to retrieve files with Tools -> File System.	NCCF-11858
Core	Pressing the Backspace Key in Tools -> Command Prompt Deletes The Entire Word, Instead of the Individual Character.	NCCF-12316
Core	Upgrade From 12.2.x to 12.2.y Fails Due to Permission Issues with Jetty.	NCCF-12326
Core	Upgrades to N-central Fail Due to a Logic Issue Related to Modifying the Default Parameters of the Connectivity Service.	NCCF-12504 NCCF-12690
Core	Upgrading an AWS-hosted N-central Instance May Fail Due to a Backup Partition Calculation Error.	NCCF-12530
Core	System Error When Updating The Thresholds Of A Custom Service.	NCCF-12556

Release 12.2 SP1 HF1

CATEGORY	DESCRIPTION	BUG
Monitoring	An Incorrect Timeout Value Causes the Connectivity Service to Transition Between Failed and Stale.	BEAT-906

CATEGORY	DESCRIPTION	BUG
Monitoring	An Error When Monitoring the SSL Certificate Causes The HTTPS Service To Incorrectly Report a Failed State.	NCCF-11622
Monitoring	VMware Services Misconfigured Due to Issue in the Data Retrieval Logic.	NCCF-11805
Core	N-central Performance/Stability Affected by a Process Deadlock.	NCCF-11493
Core	Tools -> Command Prompt Becomes Unresponsive and Consumes CPU Resources.	NCCF-11831
Core	Backup process is not checking for /tmp/initial_install, resulting in backups running during install/OS Upgrade.	NCCF-11875
Core	Bulk editing a Custom Property is limited to 100 characters.	NCCF-11905
Core	Upgrade to 12.2 SP1 Fails Due to Duplicate "Web_Urllp" and "Web_UrllP" Records.	NCCF-12183
Patch Management	Windows Probe Cannot Download Patch Files when TLS 1.0 and TLS 1.1 are Disabled.	NCPM-4115
Patch Management	Message boxes are not suppressed during PME installation.	NCPM-4173
Patch Management	The "Retrieve Recovery Key" Button Returns An Incorrect BitLocker Recovery Key.	NSBM-3641

Known Limitations

The "Known Issues" list 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 Issues 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

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
<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
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	73359

DESCRIPTION	BUG
<p>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. 	

PSA Integration

DESCRIPTION	BUG
<p>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.</p>	65620

UI

DESCRIPTION	BUG
<p>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.</p>	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 7.6 (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 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

NUMBER OF DEVICES	CPU CORES	MEMORY	STORAGE
Up to 16,000	22	48 GB RAM	800 GB HDD
Up to 20,000	28	64 GB RAM	1 TB HDD
Up to 24,000	34	80 GB RAM	1.2 TB HDD

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 7.6 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	<p>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.</p> <p>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.</p>
MAC Addresses	<p>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.</p>

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:

- Java 1.8.162 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

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 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

i 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

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)

Mac Agents

- 10.15 (Catalina)
- 10.14 (Mojave)
- 10.13 (High Sierra)
- 10.12 (Sierra)

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

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)

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 12.2 SP1 HF2 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.solarwindmsp.com
Technical Support Self-Service Portal:	https://support.solarwindmsp.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 solarwindmsp.com.