



INSTALLATION GUIDE

SolarWinds N-central

Version 12.0



Contents


Contents	3
Network Requirements	6
Agent and probe requirements	8
Windows Agents:	8
SolarWinds N-central System Requirements	9
System requirements by number of devices managed	9
Notes	9
Examples of supported servers	10
Optional modem	10
Support for virtualization environments	11
About virtualization	11
Recommended configuration for the virtualization server	12
Supported Software	12
Browsers	12
Remote Control	12
Report Manager	12
Automation Manager	13
SNMP Community String	13
Supported Operating Systems	13
Windows Agents:	13
Windows Server 2016	13
Windows Server 2012	13
Windows Server 2008	13
Microsoft Windows Hyper-V	14
Windows 10	14
Windows 8 and 8.1	14
Windows 7	15

Windows Vista	15
Linux Agents	15
Mac Agents	15
AV Defender	15
Workstation Operating Systems	15
Tablet And Embedded Operating Systems	16
Server Operating Systems	16
Patch Manager	16
Workstation Operating Systems	16
Server Operating Systems	16
Unsupported Operating Systems	16
Windows Update Agent	17
Automation Manager	17
Workstation Operating Systems	17
Server Operating Systems	17
Installing SolarWinds N-central	18
What do you want to do?	18
Install SolarWinds N-central on a physical server	18
Install SolarWinds N-central as a guest on an ESX server	19
Install SolarWinds N-central as a guest on a Hyper-V server	20
Install SolarWinds N-central on Microsoft Azure Resource Manager	20
Prerequisites	21
Before you begin	21
Download and extract the SolarWinds N-central VHD	21
Extract the VHD file	22
Create a Resource Group	22
Create a Storage Account	23
Create a Container	24

Upload the VHD	25
Create a Virtual Network	26
Create a Public IP Address	27
Create a Network Security Group	28
Create a Network Interface	29
Link the Public IP to the NIC	30
Create the Inbound Security Rules for SolarWinds N-central.	31
Install SolarWinds N-central on Amazon AWS EC2	34
Upgrading SolarWinds N-central	35
Step 1: Back up the SolarWinds N-central server	36
Step 2: Install the SolarWinds N-central server upgrade	37
Step 3: Post-installation steps	38
Rebuild or Migrate your SolarWinds N-central server	40
The server is not working properly or starting successfully	40
An upgrade has failed but you can still log in	40
Migrating an existing SolarWinds N-central server to another computer	41
Log in to SolarWinds N-central for the first time	43
Activating SolarWinds N-central	47
Support	47
Contacting Technical Support	49

Network Requirements

SolarWinds N-central requires access to the following ports for regular operation. For a complete list of all ports used by SolarWinds N-central, see the SolarWinds N-central *Security White Paper*.

PORT #	PORT LOCATION				DESCRIPTION
	N-CENTRAL SERVER		MANAGED DEVICE		
	INBOUND	O UTBOUND	INBOUND	O UTBOUND	
20		√			For FTP connections, especially when configured for backups.
21		√			For FTP connections, especially when configured for backups.
22	√			√	SSH for remote control sessions. The firewall must allow access from the Internet to this port on the SolarWinds N-central server.
25		√			SMTP for sending mail.
53		√			For DNS.
80	√	√		√	HTTP to communicate between SolarWinds N-central and agents or probes, (including MSP Connect and MSP Anywhere). The firewall must allow access from the Internet to this port on the SolarWinds N-central server. This port must be open for outbound traffic if the SolarWinds N-central server is monitoring HTTP on a managed device.
<div> Inbound access to port 80 can be blocked if agents are configured to use HTTPS and the SolarWinds N-central server is accessed over port 443 using HTTPS.</div>					
123		√			Used by the NTP Date service to keep the server clock synchronized. Normally using UDP , although some servers can use TCP.
443	√	√		√	HTTPS - used for communication between the SolarWinds N-central UI and Agents or Probes (including MSP Connect and MSP Anywhere).

PORT #	PORT LOCATION				DESCRIPTION
	N-CENTRAL SERVER		MANAGED DEVICE		
	INBOUND	O UTBOUND	INBOUND	O UTBOUND	
					<p>Port 443 is the TCP port needed for SSL (HTTPS) connections. The firewall must be configured to allow access from the Internet to this port on the SolarWinds N-central server.</p> <p>This port must also be open for outbound traffic if the SolarWinds N-central server is monitoring the HTTPS service on a managed device.</p> <p>Backup Manager relies on Port 443 TCP outbound. It is almost always open on workstations but may be closed on servers. This port must be open for outbound traffic on the SolarWinds N-central server.</p>
5280	√			√	<p>Used by Agents and Probes for XMPP traffic.</p> <p>Outbound access to port 5280 for Managed Devices is recommended but not required.</p>
10000	√				<p>HTTPS, used to access the NAC. The firewall must allow access from the Internet to this port on the SolarWinds N-central server.</p>

Agent and probe requirements

To use agents and probes, devices require the following minimum hardware requirements:

- RAM: 512 MB
- Disk space: 500 MB
- Processor: x86 or x64

Windows Agents:

- Microsoft .NET Framework 4.5.2 (or later)


.NET FRAMEWORK ON DEVICE	PROBE	AGENT
Only Microsoft .NET Framework 4.0.x	✗	✗
Both Microsoft .NET Framework 2.0.50727 and Microsoft .NET Framework 4.5.2	✓	✓

i For Windows 2003 devices, installing .NET Framework 4.0.x requires the Windows Imaging Component (see <http://msdn.microsoft.com/en-us/library/8z6watww.aspx>).

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 to install a separate Operating System to run SolarWinds N-central. The SolarWinds N-central ISO includes a modified version of CentOS 6.x, based on the upstream Red Hat Enterprise Linux 6.9.
Physical Hardware	<p>The server (non-virtual) used to install SolarWinds N-central in a bare metal environment must be certified to run Red Hat Enterprise Linux 6.9 (x64) by Red Hat, or the hardware vendor, without any additional drivers. Please check the Red Hat Customer Portal for details.</p> <div>  UEFI (Unified Extensible Firmware Interface) boot support is a technology preview in CentOS 6.x, and not supported. As a result, SolarWinds N-central must be installed using the legacy BIOS boot method. </div>

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
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

 SolarWinds N-central does not support UEFI (Unified Extensible Firmware Interface)–based hardware.

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 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 spindles.
5. If using Solid State Drives (SSDs), SolarWinds MSP requires Enterprise Grade SSDs with a SAS interface. SSDs must have an endurance rating of at least 0.2 DWPD (Drive Writes Per Day), and at least 4 physical disks in a RAID 10 array. The RAID array must appear to the operating system as a Block Device. At this time, many PCIe and NVMe disks do not meet this last requirement.
6. 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).
7. Configure the RAID controller to use the default stripe size and a Read/Write cache of 50%/50%.

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 - ML350 Gen9](#) and [Dell PowerEdge R720](#).

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 6.9 certified, without the need for additional drivers. Physical servers must support legacy BIOS boot, as the newer UEFI boot is a technology preview in CentOS 6.x, and not supported. SolarWinds MSP does not support UEFI boot at this time.

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 is preferred, but RAID 5 is also supported (at the hardware RAID BIOS level).

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.

i 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: <ul style="list-style-type: none"> ■ 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

i 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®

i 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:

- 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

i 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 version 1607 and later

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.

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 2008 (32/64-bit)
- Microsoft Windows Server 2008 R2 (32/64-bit)
- Microsoft Windows Server 2012 (32/64-bit)
- Microsoft Windows Server 2012 R2 (32/64-bit)

Installing SolarWinds N-central

You can install SolarWinds N-central on a physical server, virtual server or in the Microsoft Azure cloud (Resource Manager) or Amazon AWS EC2 computing platform.

What do you want to do?

- [Install on a physical server](#)
- [Install as a guest on an ESX server](#)
- [Install as a guest on a Hyper-V Server](#)
- [Install on Microsoft Azure Resource Manager](#)
- [Install on Amazon AWS EC2](#)

Install SolarWinds N-central on a physical server

1. Configure the server RAID array using the following settings:

HP Server	
Cache Options	Set to 50% Read and 50% Write.
Disk RAID 1+0	HP uses an 8 KB stripe size. Delete and recreate the logical drive to set the stripe size.
IBM Server	
Cache Options	Use the default settings.
Disk RAID 1+0	IBM uses an 8 KB stripe size. Use Express Configuration Controller 2 to enable all settings.
Dell Server	
Cache Options	Set Write Policy to Write-back and Read Policy to Adaptive.
Disk RAID 1+0	Dell uses an 8 KB stripe size.
Intel Server	
Cache Options	Set Write Policy to Write-back and Read Policy to Adaptive.
Disk RAID 1+0	Intel uses an 8 KB stripe size. Use the RAID utility to set the stripe size.

2. Insert the installation CD and restart the server.
3. Type install.

i To install SolarWinds N-central on an HP ML-150G6 server, type `install nodmraid`.

4. Press **Enter**.

i If you are not prompted for network information, SolarWinds N-central was unable to locate a suitable network card. The installation will continue but you will not be able to access SolarWinds N-central.

5. Select a network configuration. SolarWinds MSP recommends **Manual address configuration**.
6. Click **OK** and **Enter**.
7. If you selected **Manual address configuration**, enter the **IP Address** and **Netmask**, click **OK**, and **Enter**.
8. In the **Miscellaneous Network Settings** screen, enter the **Gateway**, **Primary DNS** and **Secondary DNS** addresses.
9. Click **OK** and **Enter**.
10. In the **Hostname Configuration** page, select the hostname configuration and click **OK**.
11. In the **Time Zone Selection** page, select your time zone. UTC is recommended.
12. Save and confirm the procedure.

Install SolarWinds N-central as a guest on an ESX server

1. Create a new virtual machine using the following settings:

OS	Red Hat Enterprise Linux 6 and 7 (32/64-bit) Do not enable paravirtualization.
Virtual Disks	Thick Provision
CPU/Memory/Storage	Size according to tables in the <i>System Requirements</i> .
Network Adapter	VMXNET3

2. Mount a disk or network file system to access the installation CD .ISO image.

i Ensure that the VMware guest is configured to use the mounted disk or network file system as a boot disk.


3. Start the new VM.
4. At the installation prompt, type install and press **Enter**.

i If you are not prompted for network information, SolarWinds N-central was unable to locate a network card. The installation will finish, but you cannot log in. To resolve this issue, verify that the server has a compatible network card.

5. Select the type of network configuration. SolarWinds MSP recommends **Manual address configuration**.
6. Select **OK** and **Enter**.
7. If you selected **Manual address configuration**, enter the **IP Address** and **Netmask**, select **OK** and press **Enter**.
8. In the **Miscellaneous Network Settings** screen, enter the **Gateway**, **Primary DNS** and **Secondary DNS** addresses.
9. Click **OK** and **Enter**.

10. In the **Hostname Configuration** screen, select the hostname configuration.
11. Click **OK** and **Enter**.
12. In the **Time Zone Selection** page, select your time zone. UTC is recommended.
13. Save and confirm the procedure.


Install SolarWinds N-central as a guest on a Hyper-V server

 SolarWinds N-central does not support the use of dynamic memory under Hyper-V.

1. Create a new virtual machine using the settings below.

Generation	Generation 1
CPU/Memory/Storage	Size according to tables in the <i>System Requirements</i> .
Network Adapter	Select a valid network to where the virtual machine can connect.

2. Start the new VM.
3. In the **Virtual Machine Connection** window, type install and **Enter**.
4. Select **Manual address configuration** for the of network configuration type.

 If you are not prompted for network information during the installation, N-central was unable to locate a suitable network card. The installation will continue to conclusion, but you will not be able to log in. To resolve this issue, ensure that the virtual switch settings of the host are configured to the proper network and restart the installation. We recommend that you do not use a Legacy Network Adapter.

5. Select **OK** and **Enter**.
6. Type the **IP Address** and **Netmask**.
7. Select **OK** and **Enter**.
8. In the **Miscellaneous Network Settings** screen, type the **Gateway**, **Primary DNS** and **Secondary DNS** addresses.
9. Select **OK** and **Enter**.
10. In the **Hostname Configuration** screen, select **automatically via DHCP** or **manually**.
11. Select **OK** and press **Enter**.
12. In the **Time Zone Selection** page, select your time zone. UTC is recommended.
13. Save and confirm the procedure.

Install SolarWinds N-central on Microsoft Azure Resource Manager

The instructions below walk you through a new installation of SolarWinds N-central in the Microsoft Azure environment.

SolarWinds N-central is certified to run on Microsoft Azure, sized for up to 9,000 devices. Larger deployments are not currently supported.

SolarWinds MSP recommends that you plan your deployment with SolarWinds MSP Support in advance.

You will need a valid license to be applied before you are able to log in to SolarWinds N-central.

You must have basic knowledge of how to install and configure SolarWinds N-central. SolarWinds N-central deployment to Azure Resource Manager is not designed for technicians who are unfamiliar with Azure Resource Manager and PowerShell.

Prerequisites

Before you begin, ensure that you have:

- An Azure subscription
- A Windows PC with Windows Edge, Internet Explorer 11 or current version of FireFox or Chrome, and PowerShell with Azure Resource Manager extensions.

Set up the PowerShell and Azure environment. PowerShell commands are used to perform the Azure steps required to convert and upload the virtual machine image file and create an Azure Cloud VM based on the image. Each step below requires PowerShell with Azure Resource Manager extensions installed on the working PC.

Background information on the environment setup can be found at <https://azure.microsoft.com/en-us/documentation/articles/powershell-install-configure>.

Before you begin

- You must have Administrator privileges for the Azure Environment.
- PowerShell must be launched as an Administrator by clicking **Start Menu > Search for PowerShell**, Right Click the PowerShell icon and click **Run as Administrator**.
- Clean up any old Azure and Azure Resource Manager PowerShell Modules (as Administrator) - Older versions may not work/upgrade correctly.
- Install the new Azure Resource Manager PowerShell Module (as Administrator).

i All Azure device and resource names must be Cloud, or in some cases, globally unique (no duplicates in the entire cloud location, or in all clouds).

Download and extract the SolarWinds N-central VHD

Download the image file for the version and disk size of SolarWinds N-central you want to install. Extract the .vhd file in your Azure Environment.

i The extraction of the .vhd can take over an hour to complete.

The SolarWinds N-central Virtual Hard Disk (VHD) image is available on the SolarWinds MSP Resource Center. You will need enough free space to extract the full size of the image to the disk. The image size is 100, 200 or 500 GB.


1. Login to the SolarWinds MSP Resource Center (<https://community.solarwindsmsp.com/>).
2. Click the hamburger menu (≡) and click **Support > Software Downloads > N-central**.
3. Click the link for the latest release of SolarWinds N-central.
4. Download the appropriately-sized VHD file for Microsoft Azure.

The web browser downloads the VHD file to the location it has configured for downloaded files from the Internet. Use a decompression tool to extract the VHD file.

Extract the VHD file

Extract the file using a tool such as 7-zip. The extraction of the 100GB VHD image can take over an hour to uncompress. Larger images will take longer.

1. Set up the PowerShell and Azure environment. PowerShell commands are used to perform the Azure steps required to convert and upload the virtual machine image file and create an Azure Cloud VM based on the image. Each step below requires PowerShell with Azure Resource Manager extensions installed on the working PC. For more information on the environment setup, see <https://azure.microsoft.com/en-us/documentation/articles/powershell-install-configure/>.

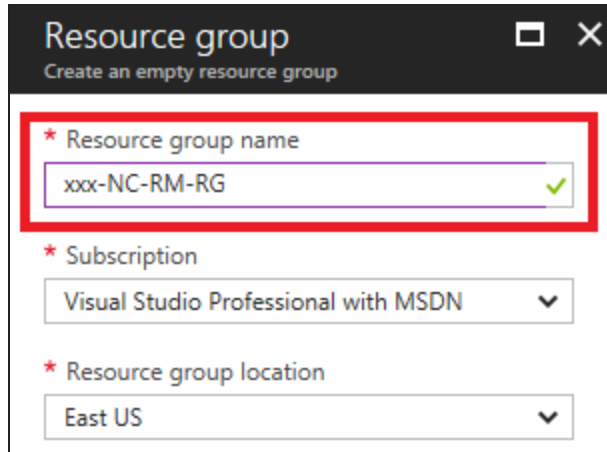
 You need Administrator privileges for the Azure environment.
Launch PowerShell as an Administrator

2. Clean up old Azure and Azure Resource Manager PowerShell modules. Older version may not work or upgrade properly. Run the following commands:
 - Uninstall the AzureRM component modules: `Uninstall-AzureRM`
 - Uninstall the AzureRM module: `Uninstall-Module AzureRM`
 - Uninstall the Azure module: `Uninstall-Module Azure`
3. Close PowerShell and run the **Microsoft Azure PowerShell Uninstaller** from the **Programs and Features** in the **Control Panel**.
4. Reboot the system and install the new Azure Resource Manager PowerShell Module as an Administrator:
`Install-Module AzureRM`
5. From the PowerShell console as Administrator, import the required PowerShell Azure Resource Manager Module previously installed:
`Import-Module AzureRM`
6. Confirm the Azure environment using the command:
`$PSVersionTable.PSVersion.Major and (Get-Module AzureRM).Version.`

Create a Resource Group

Create a Resource Group and give it a name.


1. In Microsoft Azure, click the  icon and click **Add**.
2. Enter a **Resource group name**. For example, xxx-NC-RM-RG.



3. Click **Create**.

Create a Storage Account

Ensure you select Premium storage if you have over 1000 devices.

1. In Microsoft Azure, click the  icon and click **Add**.
2. Enter a **Name**, for example xxxncrmsa.
3. Complete the information as outlined in the image below.

Create storage account

The cost of your storage account depends on the usage and the options you choose below.
[Learn more](#)

* Name ⓘ
xxxncrmsa ✓
.core.windows.net

Deployment model ⓘ
Resource manager Classic

Account kind ⓘ
General purpose

Performance ⓘ
Standard Premium

Replication ⓘ
Locally-redundant storage (LRS)

* Storage service encryption (blobs and files) ⓘ
Disabled Enabled

* Secure transfer required ⓘ
Disabled Enabled

* Subscription
Visual Studio Professional with MSDN

* Resource group ⓘ
☐ Create new ☒ Use existing
xxx-NC-RM-RG

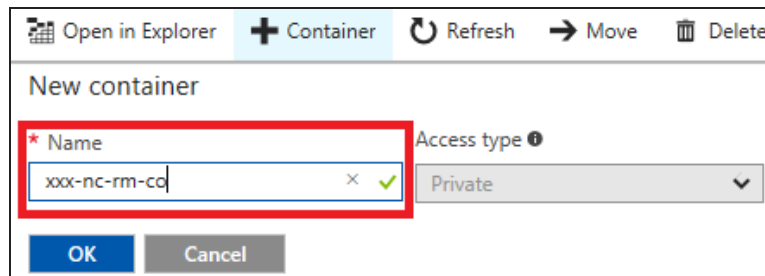
* Location
East US

4. Click **Create**.

Create a Container

Create a Container inside the Storage Account.

1. In the Storage Account, click **Overview** > **Container**.
2. Enter a **Name** for the Container. For example, xxx-nc-rm-co.



- 3.
4. Click **OK**.

Upload the VHD

1. In PowerShell, connect the console to the Azure Subscription:

```
Login-AzureRmAccount
```

An Azure credentials window opens.

```
Get-AzureRmSubscription
```

Displays the Azure Subscriptions.

```
SubscriptionName: Visual Studio Professional with MSDN
```

```
SubscriptionId : ex0fcxxx-b2xx-41xx-86xx-bxx6xxxd1xxx
```

```
TenantId : xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

```
State : Enabled
```

```
Select-AzureRmSubscription -SubscriptionId "ex0fcxxx-b2xx-41xx-86xx-bxx6xxxd1xxx"
```

2. Set the Resource Group PowerShell variable using the name you entered above:

```
$ResourceGroup = "xxx-NC-RM-RG"
```

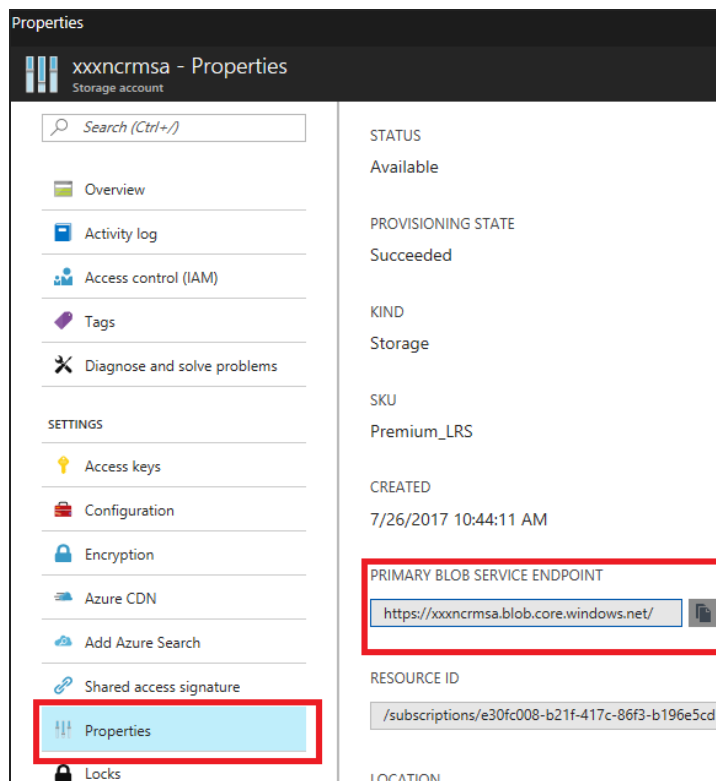
3. Set the Azure Image File name (The file name of the .vhd file you extracted):

```
$ImageFileName = "N-central-xx.x.x.xxxx-x00.vhd"
```

4. Set the Azure Image location (the local folder where the above file is located):

```
$vhdPath = "C:\Some Path\$ImageFileName"
```

5. In Microsoft Azure, copy the URL from the container you created above.



6. Paste the URL to the UploadURL command:


```
$UploadURL = "https://xxx-nc-rm-sa.blob.core.windows.net/xxx-nc-rm-co/$ImageFileName"
```

7. Upload the VHD file to Azure:

```
Add-AzureRmVhd -ResourceGroupName $ResourceGroup -Destination $UploadURL -LocalFilePath $vhdPath
```

Allow the upload to run in the background. The upload will take several hours.

Create a Virtual Network

1. In Microsoft Azure, click the  icon and click **Add**.
2. Enter a **Name** for the virtual network. For example, xxx-NC-RM-VN.
3. Complete the information as outlined in the image below.

Create virtual network

* Name
xxx-NC-RM-VN ✓

* Address space ⓘ
10.2.0.0/24 ✓
10.2.0.0 - 10.2.0.255 (256 addresses)

* Subnet name
xxx-NC-RM-SN ✓

* Subnet address range ⓘ
10.2.0.0/24 ✓
10.2.0.0 - 10.2.0.255 (256 addresses)


* Subscription
Visual Studio Professional with MSDN ▼

* Resource group ⓘ
☐ Create new ☒ Use existing
xxx-NC-RM-RG ▼

* Location
East US ▼

4. Click **Create**.

Create a Public IP Address

1. In Microsoft Azure, click the  icon and click **Add**.
2. Enter a **Name**. For example, xxx-NC-RM-PIP.
3. Complete the information as outlined in the image below.

Create public IP address

* Name
xxx-NC-RM-PIP ✓

* IP Version ⓘ
IPv4 IPv6

* IP address assignment
Dynamic Static

* Idle timeout (minutes) ⓘ
4

DNS name label ⓘ
xxx-nc-rm ✓
.eastus.cloudapp.azure.com

☐ Create an IPv6 address


* Subscription
Visual Studio Professional with MSDN ▼

* Resource group ⓘ
☐ Create new ☒ Use existing
xxx-NC-RM-RG ▼

* Location
East US ▼

4. Click **Create**.

Create a Network Security Group

1. In Microsoft Azure, click the  icon and click **Add**.
2. Enter a **Name**. For example, xxx-NC-RM-SG.
3. Complete the information as outlined in the image below.

Create network security gro... [minimize] [close]

* Name
xxx-NC-RM-SG ✓


* Subscription
Visual Studio Professional with MSDN ▼

* Resource group ⓘ
☐ Create new ☒ Use existing
xxx-NC-RM-RG ▼

* Location
East US ▼

4. Click **Create**.

Create a Network Interface

1. In Microsoft Azure, click the  icon and click **Add**.
2. Enter a **Name** . For example, xxx-NC-RM-NIC.
3. Complete the information as outlined in the image below.

Create network interface

* Name
xxx-NC-RM-NIC ✓

* Virtual network ⓘ
xxx-NC-RM-VN ▼

* Subnet ⓘ
xxx-NC-RM-SN (10.2.0.0/24) ▼

Private IP address assignment
Dynamic Static

Network security group ⓘ
xxx-NC-RM-SG >

☐ Private IP address (IPv6)

* Subscription
Visual Studio Professional with MSDN ▼

* Resource group ⓘ
☐ Create new ☒ Use existing
xxx-NC-RM-RG ▼

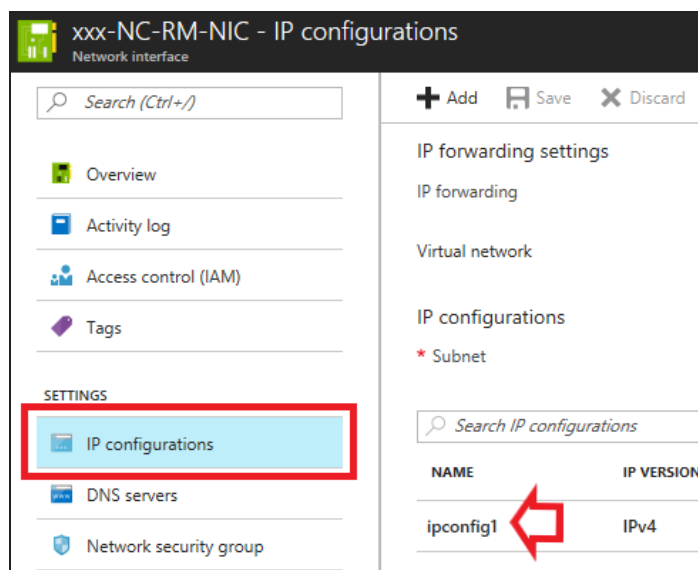
* Location
East US ▼

4. Click **Create**.

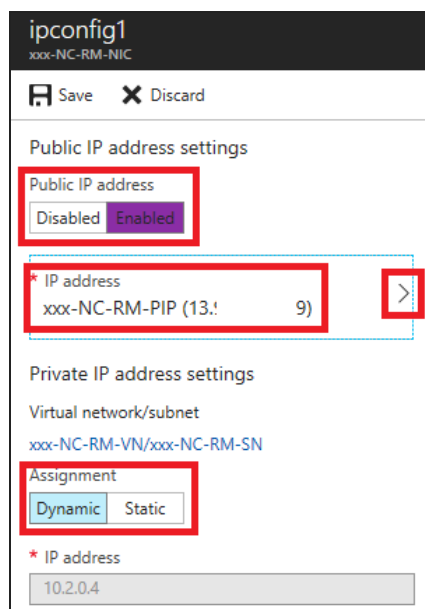
Link the Public IP to the NIC

Enable and attach the Public IP to the NIC created.

1. Go to the IP configuration for the Network Interface you created above.
2. Click IP Configurations in the Settings area and click ipconfig1.




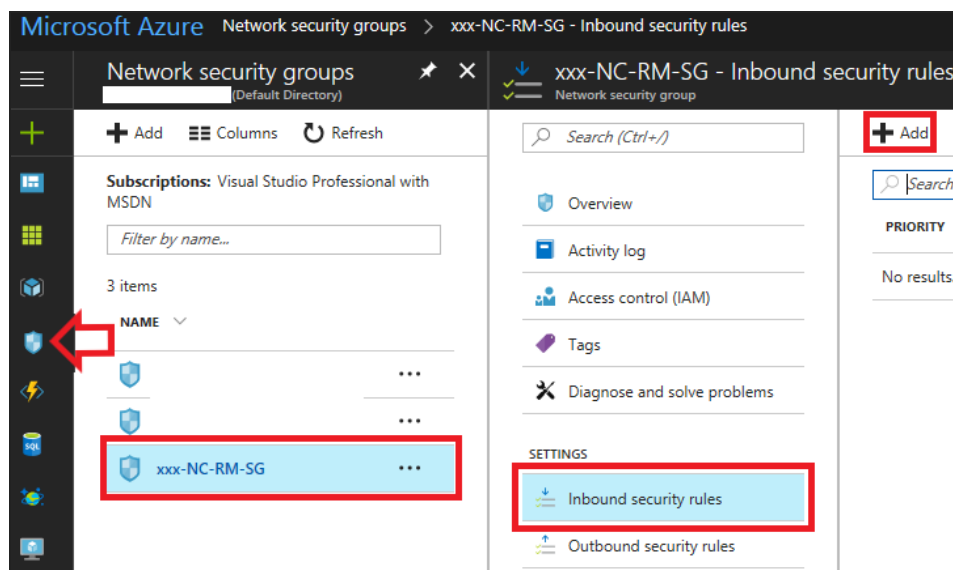
3. Complete the information as shown in the image below.



Create the Inbound Security Rules for SolarWinds N-central.

Create security rules to connect with SolarWinds N-central.

1. In Microsoft Azure, click the icon .
2. Click the **Security Group > Inbound security rules > Add**.



- 3.
4. Add the inbound security rules as outlined in the images below. Create a rule for a Source of Any and Source Port Range of "*" (asterisk) to accept all incoming traffic. Set the destination for ports 22, 80, 443, 10000, and any other ports you may require.

Add inbound security rule

LargeTest-SG

Basic

* Source ⓘ

Any

* Source port ranges ⓘ

*

* Destination ⓘ

Any

* Destination port ranges ⓘ

8080

* Protocol

Any TCP UDP

* Action

Allow Deny

* Priority ⓘ

100

* Name

Port_8080

Description

Add inbound security rule

xxx-NC-RM-SG

Advanced

* Name

xxx-NC-RM-ISR-SSH ✓

* Priority ⓘ

100

* Source ⓘ

Any CIDR block Tag

* Service ⓘ

SSH

* Protocol

Any TCP UDP

* Port range ⓘ

22

* Action

Deny Allow

Security rules					
<div> <div>+ Add</div> <div>Default rules</div> </div>					
<div> <div>Search inbound security rules</div> </div>					
PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
100	xxx-NC-RM-ISR-SSH	Any	Any	SSH (TCP/22)	Allow
110	xxx-NC-RM-ISR-HTTP	Any	Any	HTTP (TCP/80)	Allow
120	xxx-NC-RM-ISR-HTTPS	Any	Any	HTTPS (TCP/443)	Allow
130	xxx-NC-RM-ISR-NAC	Any	Any	Custom (TCP/10000)	Allow

5. Click **OK**.

Complete as many rules as required for communication. For example:

PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
100	xxx-NC-RM-ISR-SSH	Any	Any	SSH (TCP/22)	Allow
110	xxx-NC-RM-ISR-HTTP	Any	Any	HTTP (TCP/80)	Allow
120	xxx-NC-RM-ISR-HTTPS	Any	Any	HTTPS (TCP/443)	Allow
130	xxx-NC-RM-ISR-NAC	Any	Any	Custom (TCP/10000)	Allow

When the upload completes, go to the PowerShell window and Create the VM. Refer to the Number of Devices Managed table in the SolarWinds N-central in the [System Requirements](#) for proper Azure Instance Sizing.

- > 1,000 devices should use Premium Storage.
- > 6,000 devices should also use Compute Optimized Instances.

```
$nic = Get-AzureRmNetworkInterface -Name "xxx-NC-RM-NIC" -ResourceGroupName
$ResourceGroup
$storageAcc = Get-AzureRmStorageAccount -ResourceGroupName $ResourceGroup -Name
"xxxncrmsa"
$location = "Central US" # <- Use the same Azure region used in the user interface
$VMSize = "Standard_DS4_v3" # <- Use an appropriate Azure size based on the MSP N-central Install
Guide and the above considerations.
$vmName = "xxx-NC-RM-VM"
$osDiskName = "xxx-NC-RM-DSK"
$vm = New-AzureRmVMConfig -VMName $vmName -VMSize $VMSize
$vm = Add-AzureRmVMNetworkInterface -VM $vm -Id $nic.Id
$vm = Set-AzureRmVMOSDisk -VM $vm -Name $osDiskName -VhdUri $UploadURL -
CreateOption attach -Linux
New-AzureRmVM -ResourceGroupName $ResourceGroup -Location $location -VM $vm
```

The new SolarWinds N-central server should be accessible through its IP Address or DNS address that was assigned by Microsoft Azure. You can access it using a web browser and the SolarWinds N-central server configuration can continue as outlined the *Install Guide*.

To monitor the state of this VM, the Azure portal can be used.

💡 Be sure to Adjust the Time Zone to match your location or the Time Zone location of the server you are restoring from.

Once your server is deployed to Azure, open a Support Case to have SolarWinds MSP Technical Support apply a finger fix for Bug NCCF-5915. Due to verbose logging being enabled on the Azure Agent, and the default rotate settings in use on the Azure Agent logs, the Azure Agent logs can fill up your SolarWinds N-central disk over several weeks or months. The finger fix prevents this by disabling verbose logging and adjusts the retention settings on the log.

Install SolarWinds N-central on Amazon AWS EC2

1. Login to the Amazon AWS Console, and select the **EC2 Management Console**.
2. Click **Instances** and click **Launch Instance**.
3. Click **Community AMIs** and search for the AMI, or for *N-central*.
4. Click **Select**.
5. Select a suitably sized **General Purpose Instance Type**, based on sizing information from the SolarWinds N-central *System Requirements Guide*.
6. Click **Next: Configure Instance Detail**, then **Click Next: Add Storage**.
7. Set the appropriate storage size for your instance based on sizing information from the SolarWinds N-central *System Requirements Guide*.
8. In the **Volume Type** drop-down list box, select **General Purpose SSD (GP2)**.
9. Click **Review and Launch**.
10. On the Review Page, click **Edit security groups**.
11. Create a security group open the inbound TCP ports 22, 80, 443, and 10000.
12. Click **Review and Launch**, then click **Launch**.
13. Select **Proceed without keypair** from the drop-down list box and click to select the acknowledgement check box.
14. Click **Launch Instances**.

The new instance launches, and you are returned to the Instances page to view the new instance.


Upgrading SolarWinds N-central

This document includes the following upgrade procedures:

- [Step 1: Back up the SolarWinds N-central server](#)
- [Step 2: Install the SolarWinds N-central server upgrade](#)
- [Step 3: Post-installation steps](#)

There may also be circumstances when you want to rebuild or migrate your server.

See [Rebuild or Migrate your SolarWinds N-central server](#).

 Refer to the release notes for compatible upgrade paths before you upgrade from one version to another.

Step 1: Back up the SolarWinds N-central server

Before you upgrade, back up the SolarWinds N-central server in the event of an upgrade failure. Back up the server to a destination FTP server or, if SolarWinds N-central has been installed as a guest on an ESX or Hyper-V server, record a snapshot of the guest.

1. Click **Administration > System Backup and Restore > Configure Backups** and configure the backup properties.
2. Click **Save and Run Backup**.

i During the backup, a backup file and a backup digest file are created. The backup file contains all of the information needed to restore the system. The SHA1 file contains a SHA1 checksum of the backup file and verifies that the backup file is not corrupted.

3. Wait for the system to send you a notification about the backup success or failure.
4. If the backup succeeded and you have not configured it to be uploaded to an FTP server, download the backup image from the SolarWinds N-central server to a safe location:
 - a. Click **Administration > System Backup and Restore > Download Backups**.
 - b. Click **Download Backup** beside the name of the backup file you want to download and save it to a known location.
 - c. (Optional) Click **Download Digest** beside the name of the backup file and save the digest file to a known location.

The downloaded files can now be used to restore the database. To continue the upgrade, proceed to [Step 2: Install the SolarWinds N-central server upgrade](#).

Step 2: Install the SolarWinds N-central server upgrade

You can upgrade to SolarWinds N-central 12.0 by installing the upgrade file downloaded to your SolarWinds N-central server or from the [N-able Resource Center](#).

1. On the **Administrator Console** menu bar, click **Setup**.
2. In the **Central Server** area, click **Version Management** and do one of the following:

N-CENTRAL DIRECT UPGRADE	REMOTE UPGRADE FROM DOWNLOAD LOCATION
<ol style="list-style-type: none">a. Select Install upgrade from local repository.b. Select an upgrade version from the list of available options.	<ol style="list-style-type: none">a. Select Install upgrade remotely.b. Click Browse and navigate to the .nsp file in the N-able Resource Center.

3. Enter an e-mail address in the **Notify this email address when complete** field.
4. Click **Install** and confirm the action.



The server will restart and the upgrade information will be updated.

i The average upgrade takes approximately 30 minutes. However, the upgrade process can take several hours depending on the size of your database. If five hours elapse after the upgrade and you have not received a notification, contact SolarWinds MSP for assistance.

Do not reboot the SolarWinds N-central server during the upgrade process even if it appears unresponsive. To continue the upgrade, proceed to [Step 3: Post-installation steps](#).

Step 3: Post-installation steps

After you have installed SolarWinds N-central, complete the following post-installation checklist.

	CHECK ITEMS AS THEY ARE COMPLETED
<input type="radio"/>	Verify the version of SolarWinds N-central by signing in and click Help > Version Information . The Associated Upgrades displayed must read <code>Applied-update-12.0.0.xxx-b1_0_0xxx</code> , where xxx is a number.
<input type="radio"/>	Verify the network settings and default settings by clicking Administration > Mail Network Settings > Network Setup .
<input type="radio"/>	Verify that the user accounts exist and are accessible.
<input type="radio"/>	Verify that the customer profiles are complete and accurate.
<input type="radio"/>	Verify that the devices are present.
<input type="radio"/>	Verify that the services for each device are reporting correctly.
<input type="radio"/>	Verify that all of the notification profiles are present.
<input type="radio"/>	Verify that the reports generate and display the accurate historical data.
<input type="radio"/>	<p>At the SO level, perform the following to automatically upgrade all Probes and Agents on your customers' remote computers.</p> <ol style="list-style-type: none"> 1. Click Administration > Defaults > Appliance Settings. 2. Select the Upgrade Windows Probes option as either Never (the Probe software will not ever be upgraded) or Always (the Probe software is always upgraded). 3. Click Propagate to distribute this configuration setting to existing devices. 4. Click Reboot device if necessary to automatically restart devices after the Probe software has been upgraded. 5. Click the Upgrade Agents option as either Never (the Agent software will not ever be upgraded) or Always (the Agent software is always upgraded). 6. Click Propagate to distribute this configuration setting to existing devices. 7. Click Reboot device if necessary to automatically restart devices after the Agent software has been upgraded.
	<div>  You can perform the above procedure for specific Customers/Sites by navigating to the Customer/Site level first. You will have to repeat the procedure for each Customer/Site that you want to automatically upgrade their Windows Probes and Windows Agents. </div>
	<p>Once the upgrade procedure has been completed, generate an Agent/Probe Overview report by clicking Reports > Administrative > Agent/Probe Overview in the navigation pane. This will allow you to verify that all probes have been updated.</p>

✓	CHECK ITEMS AS THEY ARE COMPLETED
	<p>i After upgrading an agent that monitors the Asigra Backup service, you will need to stop the Windows agent services, place the Asigra .DLL files to the agent's <code>bin</code> directory and re-start the Windows agent services.</p>
○	<p>Upgrade your monitoring software automatically for specific SOs, Customers or Sites: Upgrade your monitoring software automatically for specific Customers or Sites: Upgrade your monitoring software automatically for specific devices:</p> <ol style="list-style-type: none"> 1. In the navigation pane, click All Devices. 2. Select the Service Organizations, Customers or Sites, or devices to upgrade. 3. Click Update Monitoring Software. 4. In the Upgrade Monitoring Software dialog box, select Now for the monitoring software you want to upgrade from the following: <ul style="list-style-type: none"> ■ Upgrade Agent ■ Upgrade Backup Manager <p>i Upgrading Endpoint Security on devices will cause them to reboot twice: once after the existing software is removed and again when the new software is installed.</p>
○	<p>Once the upgrade procedure has been completed, generate reports by clicking:</p> <ul style="list-style-type: none"> ■ Reports >Status > AV Defender Status

Rebuild or Migrate your SolarWinds N-central server

There may be circumstances when you want to rebuild or migrate your server. For example:

- Your SolarWinds N-central server is not functioning properly or starting successfully;
- An upgrade has failed but you can still log in to SolarWinds N-central;
- You are migrating an existing SolarWinds N-central server to another computer.

The following scenarios describe the best way to rebuild or migrate your SolarWinds N-central server.

The server is not working properly or starting successfully

1. Verify the version of your SolarWinds N-central server. Technical Support can confirm the version of SolarWinds N-central that last communicated with SolarWinds MSP if your server is not working properly or cannot be restarted.
2. Locate the last valid backup of your SolarWinds N-central server. Your SolarWinds N-central server software will automatically record backups but these will be saved to the same local hard drive as the server software, which may make retrieval more difficult. You can retrieve a backup from a:
 - a. previously downloaded backup file in .TAR or .SHA1 format,
 - b. pre-configured SolarWinds N-central that automatically sent backups to an FTP server, or
 - c. snapshot of your SolarWinds N-central server recorded by a virtualized host (Hyper-V or VMWare).
3. Install the version of SolarWinds N-central that you were previously running. You can re-install SolarWinds N-central by downloading the ISO for that build (in an ISO file, not NSP). This image should only be used for new installations, not to upgrade an existing N-central server.

The following is an example of an ISO file available for download at <http://nrc.n-able.com>:

File: N-central 9.5 HF2 (9.5.0.574)

ISOMD5: 4f0ac4baab9146cb0caeb1b63127cc35

Size: 695 MB

4. Restore the backup that you located in Step #2.
5. When the system restore is completed, contact SolarWinds MSP to have your SolarWinds N-central server activated.

An upgrade has failed but you can still log in

Verify the version of your SolarWinds N-central server by clicking **Help > Version Information**.

1. Locate the last valid backup of your SolarWinds N-central server. Your SolarWinds N-central server software will automatically record backups but these will be saved to the same local hard drive as the server software itself which may make retrieval more difficult. Some options that may be used to retrieve a backup in this situation are:

- a. Download the most recent backup that was made prior to the upgrade attempt.
 - a. Click **Administration > System Backup and Restore > Download Backups**.
 - b. Click **Download Backup** beside the name of the backup file that you would like to download.
 - c. Click **Download Digest** beside the name of the backup file.
- b. You had configured SolarWinds N-central to automatically send backups to an FTP server from which they can be obtained.
- c. You have a snapshot of your SolarWinds N-central server recorded by a virtualized host (Hyper-V or VMWare). If this is the case, the following steps will not apply as you can restore your server using the snapshot.

i It is strongly recommended that snapshots of the SolarWinds N-central server should not be taken on a short-term schedule as this can affect system performance (and SolarWinds N-central records its own backups).

2. Install the version of SolarWinds N-central that you were previously running.

You can quickly re-install SolarWinds N-central to the exact version that you were using previously by downloading the ISO for that build (in an ISO file, not NSP). This lets you install the ISO and then restore your backup. Here is an example of an ISO file available for download from <http://nrc.n-able.com>:

File:N-central 9.5 HF2 (9.5.0.574) ISO

MD5:4f0ac4baab9146cb0caeb1b63127cc35

Size:695 MB

i This image should only be used for new installations of SolarWinds N-central. It is not intended for upgrading an existing SolarWinds N-central server.

3. Restore the backup that you located in Step #2.
4. When the system restore is completed, please contact SolarWinds MSP to have your SolarWinds N-central server activated.


Migrating an existing SolarWinds N-central server to another computer

1. Verify the version of your SolarWinds N-central server by clicking **Help > Version Information**.
2. Locate the last valid backup of your SolarWinds N-central server. Your SolarWinds N-central server software will automatically record backups but these will be saved to the same local hard drive as the server software itself which may make retrieval more difficult. Some options that may be used to retrieve a backup include:
 - a. Create a new backup in order to minimize data loss.
 - a. Click **Administration > System Backup and Restore > Configure Backups**.
 - b. Click **Save and Run Backup**.

i Backing up the SolarWinds N-central database will typically take several minutes to an hour.

- b. Download the most recent backup.

- a. Click **Administration > System Backup and Restore > Download Backups**.
- b. Click **Download Backup** beside the name of the backup file that you would like to download.
- c. Click **Download Digest** beside the name of the backup file.
- c. You had configured SolarWinds N-central to automatically send backups to an FTP server from which they can be obtained.
- d. You have a snapshot of your SolarWinds N-central server recorded by a virtualized host (Hyper-V or VMWare). If this is the case, the following steps will not apply as you can restore your server using the snapshot.

 It is strongly recommended that snapshots of the SolarWinds N-central server should not be taken on a short-term schedule. This can affect system performance.


3. Install the version of SolarWinds N-central that you were previously running.

For your convenience, you can quickly re-install SolarWinds N-central to the exact version that you were using previously by downloading the ISO for that build (in an ISO file, not NSP). This lets you install the ISO and then restore your backup. The following is an example of an ISO file available at <http://nrc.able.com>:

File:N-central 9.5 HF2 (9.5.0.574) ISO

MD5:4f0ac4baab9146cb0caeb1b63127cc35

Size:695 MB

 This image should only be used for new installations of SolarWinds N-central. This image is not intended for upgrading an existing SolarWinds N-central server.

4. Restore the backup that you located in Step #2.
5. When the system restore is completed, please contact SolarWinds MSP to activate your SolarWinds N-central.

Log in to SolarWinds N-central for the first time

You can log in to SolarWinds N-central activating SolarWinds N-central for a 30-day trial period. During the trial period, SolarWinds N-central will not display the RSS feed or the **What's New** list. Both are available after activation.

1. From the SolarWinds N-central homepage, log in to `https://192.168.1.1`.
2. Login using the following credentials:
 - **Email:** `productadmin@n-able.com`
 - **Password:** `Password`

3. The first time you log in, you will be prompted to submit information for the following fields:

CATEGORY	FIELD NAME	DESCRIPTION
Security Warning	Your SolarWinds N-central server does not have a valid SSL certificate!	<p>This is not a field that needs to be completed but is a warning that may appear.</p> <p>If this warning is displayed, and you want to properly secure your SolarWinds N-central server, SolarWinds MSP recommends that you purchase a valid, signed SSL certificate and upload it to your SolarWinds N-central server. SSL certificates can be obtained from security vendors such as RapidSSL, Verisign, and Entrust.</p>
Login Name	Login Name	The Login Name must be a valid email address. SolarWinds N-central will prompt you to change the Login Name to an email address other than the default (productadmin@n-able.com). It's important to change the Login Name so that you can receive e-mail notifications when an upgrade to SolarWinds N-central is available, and so that you can reset your password should you forget it.
Change Login Password	New Password	<p>Enter a new password that will be used from now on to sign in to SolarWinds N-central.</p> <p>The password must be at least eight (8) characters in length and contain the following:</p> <ul style="list-style-type: none"> ■ at least one number ■ at least one uppercase character ■ at least one lowercase character ■ at least one special character <p>You can not repeat any of your previous two passwords.</p>
	Confirm New Password	Re-enter the password.
Company Information	Company Name	Name of your company.
	Activation ID	<p>The Activation ID number is a code required to use SolarWinds N-central. This should be sent to you in the initial welcome email.</p> <p>If your Activation ID number is unavailable:</p> <ol style="list-style-type: none"> a. Log in to the NRC. b. Click My Account. c. Copy the SolarWinds N-central Activation ID on the My Account screen.

CATEGORY	FIELD NAME	DESCRIPTION
Email Information	What email address should notifications go to?	Enter the email address that will receive notifications.
	What email address should notifications come from?	Enter the address that will be used as the "sender" for email notifications.
	Mail Relay Server	<p>A mail relay server is required to route email to destination addresses for notifications.</p> <p>The default setting for the mail relay server is the SolarWinds N-central (<code>localhost.localdomain</code>) but you may wish to modify this to conform to your own firewall and mail server configurations.</p> <p>If you modify the mail relay server address, it must be in the format of a valid IP address or a resolvable fully qualified domain name (FQDN).</p>

4. Click **Save and Continue**.

i In the **Getting Started** Wizard, review the instructional videos to learn more before proceeding. Until you activate SolarWinds N-central, the **Getting Started** Wizard is available in the navigation pane under the **Actions** menu and the Help menu. After activation, you can find it under the **Help** menu.

5. Click **Add Customer/Site** to start the **Customer/Site Wizard**.
6. Under **Company Information**, enter the **Customer/Site Name**.
7. Select the **License Type** to use for the devices in this Customer/Site.
8. If necessary, provide the default domain or network credentials that Windows Agents and Windows Probes will use when running scripts, pushing software, and performing other administrative tasks.
9. If **Default Credentials** are provided, select **Show Password** to reveal the password as it is typed.
10. Click **Save and Continue**.
11. On the **Add Devices** page, select the method for adding devices to the Customer/Site. **Install a Windows Probe to Search for Devices** is the default and is recommended. Click **More Options** to select alternate methods.

12. Perform the selected process for adding devices.
 - a. Click **Finish** to launch SolarWinds N-central.
 - b. In the **Introduction** page, review the instructional videos as required and click **Next Step**.
 - c. In the **Discovery Options** page, configure the network discovery properties to discover all the devices on your network.
 - d. In the **Service Templates** page, configure the templates to manage devices and applications. Click **Next Step**.
 - e. In the **Dashboards** page, configure how to display the devices in your network. Click **Next Step**.
 - f. In the **Notifications** page, configure how to notify you about network issues. Click **Next Step**.
 - g. In the **Rules** page, configure the Rules to group devices together and apply settings to them. Click **Finish**.

Activating SolarWinds N-central

Your SolarWinds N-central server includes an initial 30-day activation period. Perform the activation process as soon as possible to take full advantage of your purchased licensing.

During the initial 30-day period, the following limits apply until SolarWinds N-central is activated:

- Branding cannot be customized,
- Custom services cannot be uploaded, and
- The server cannot be integrated with Report Manager

Also note the following limits for licenses and configuration settings:

- 500 Essential licenses
- 500 Professional licenses
- 20 Customers/Sites
- 5 Mobile Devices
- 1 Service Organization
- 50 Probes
- 100 Essential Mode Patch Management licenses
- 100 Third Party Patch Management licenses

i There is no limit on the number of Attended Remote Control licenses available for a server that has not been activated.

Before activating SolarWinds N-central, TCP ports 22, 80, 443, and, 10000 must be accessible to the SolarWinds N-central server over the Internet, and the server has a publicly-accessible IP address.

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

Once the SolarWinds N-central server is activated you will receive an email with your Company ID and instructions.

i To purchase licenses for features, contact your Channel Sales Specialist. You can find their contact information in the [Solarwinds MSP Resource Center](#) under **My Account** or email n-able-salesgroup@solarwinds.com.

Contacting Technical Support

If you require assistance with configuring SolarWinds N-central or have a technical issue, contact Technical Support using the Support web site and knowledge base at <https://support.solarwindmsp.com/kb/> or using the [LiveChat](#) feature within SolarWinds N-central.

In the Knowledge Base is a wide arrange of information including:

- Case management access
- All current SolarWinds MSP products, service packs and hot fixes, along with the appropriate release notes and installation guides
- PDF versions of product documentation, including manuals, system requirements, installation/configurations guides and technical references
- FAQs
- Support definitions, holiday support coverage calendars, and product life-cycle policies.

The LiveChat enables you to communicate directly with a Support representative if online and open and review tickets.

For information on the port and address requirements, see [Required ports and IP addresses for SolarWinds N-central Support](#).

© 2018 SolarWinds MSP Canada ULC. 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 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.