



# N-central

## INSTALLATION GUIDE

Version 2021.1

Last Updated: Wednesday, March 24, 2021





# Contents

|  |           |
|--|-----------|
| <b>Contents</b> .....                                      | <b>2</b>  |
| <b>Network Requirements</b> .....                          | <b>6</b>  |
| <b>Agent and probe requirements</b> .....                  | <b>10</b> |
| Windows Agents: .....                                      | 10        |
| <b>N-able N-central System requirements</b> .....          | <b>11</b> |
| System requirements by number of devices managed .....     | 11        |
| Notes .....  | 12        |
| Examples of supported servers .....                        | 13        |
| Support for virtualized environments .....                 | 14        |
| About virtualization .....                                 | 14        |
| Recommended configuration for the virtualized server ..... | 15        |
| Supported Software .....                                   | 15        |
| Browsers .....   | 15        |
| Remote Control .....                                       | 16        |
| Report Manager .....                                       | 16        |
| Automation Manager .....                                   | 16        |
| SNMP Community String .....                                | 16        |
| Supported Operating Systems .....                          | 16        |
| Windows Agents: .....                                      | 16        |
| Windows Server 2019 .....                                  | 16        |
| Windows Server 2016 .....                                  | 17        |
| Windows Server 2012 .....                                  | 17        |
| Windows 10 .....   | 17        |
| Windows 8 and 8.1 .....                                    | 17        |
| Windows 7 .....  | 17        |
| Mac Agents .....   | 18        |



|   |           |
|---|-----------|
| Linux Agents .....  | 18        |
| AV Defender .....   | 18        |
| Workstation Operating Systems .....   | 18        |
| Tablet And Embedded Operating Systems .....   | 18        |
| Server Operating Systems .....  | 18        |
| Patch Manager .....   | 19        |
| Workstation Operating Systems .....   | 19        |
| Server Operating Systems .....  | 19        |
| Windows Update Agent .....  | 19        |
| Automation Manager .....  | 19        |
| Workstation Operating Systems .....   | 19        |
| Server Operating Systems .....  | 19        |
| Disk Encryption Manager .....   | 20        |
| <b>Installing N-able N-central .....</b>  | <b>22</b> |
| What do you want to do? .....   | 22        |
| Prepare installation media .....  | 23        |
| DVD Creation .....  | 23        |
| USB Flash Drive .....   | 23        |
| Linux and MacOS .....   | 23        |
| Windows .....   | 23        |
| Install N-able N-central on a physical server .....   | 25        |
| What's next? .....  | 26        |
| Install N-able N-central as a guest on an ESX/ESXi 6.0 or newer server .....                | 27        |
| What's next? .....  | 28        |
| Install N-able N-central as a guest on Windows Server 2012 R2 or newer Hyper-V server ..... | 29        |
| What's next? .....  | 31        |
| Install N-able N-central on Microsoft Azure Managed Disks .....                             | 32        |



|  |    |
|--|----|
| Deployment .....   | 32 |
| First run .....  | 33 |
| VM Sizing .....  | 33 |
| Notes .....  | 34 |
| What's next? .....   | 35 |
| Deployment script for Microsoft Azure - Managed Disks .....        | 36 |
| Azure information .....  | 36 |
| Azure Region .....   | 36 |
| Resource naming prefix .....                                       | 36 |
| VM size .....  | 36 |
| Operating system disk size .....                                   | 37 |
| Operating system disk storage type .....                           | 37 |
| Data disks sizes .....   | 37 |
| Number of data disks .....   | 37 |
| Data disks storage type .....                                      | 37 |
| Boot diagnostics storage account .....                             | 38 |
| Boot diagnostics storage account type .....                        | 38 |
| Accelerated networking .....                                       | 38 |
| IPv6 Support .....   | 38 |
| N-central sizing on Azure Managed Disk deployment .....            | 39 |
| Install N-able N-central on Microsoft Azure Resource Manager ..... | 40 |
| Prerequisites .....  | 40 |
| Before you begin .....   | 40 |
| Download and extract the N-able N-central VHD .....                | 41 |
| Extract the VHD file .....   | 41 |
| Create a Resource Group .....                                      | 42 |
| Create a Storage Account .....                                     | 42 |



|   |           |
|---|-----------|
| Create a Container .....  | 43        |
| Upload the VHD .....  | 44        |
| Create a Virtual Network .....  | 45        |
| Create a Public IP Address .....  | 46        |
| Create a Network Security Group .....                                   | 47        |
| Create a Network Interface .....  | 48        |
| Link the Public IP to the NIC .....                                     | 49        |
| Create the Inbound Security Rules for N-able N-central. ....            | 50        |
| What's next? .....  | 53        |
| Install N-able N-central on Amazon AWS EC2 .....                        | 54        |
| What's next? .....  | 54        |
| <b>Upgrading N-able N-central .....</b>                                 | <b>55</b> |
| Step 1: Back up the N-able N-central server .....                       | 56        |
| Step 2: Install the N-able N-central server upgrade .....               | 57        |
| Step 3: Post-installation steps .....                                   | 58        |
| Rebuild or Migrate your N-able N-central server .....                   | 60        |
| The server is not working properly or starting successfully .....       | 60        |
| An upgrade has failed but you can still log in .....                    | 60        |
| Migrating an existing N-able N-central server to another computer ..... | 62        |
| <b>Log in to N-able N-central for the first time .....</b>              | <b>64</b> |
| <b>Activating N-able N-central .....</b>                                | <b>68</b> |
| Support .....   | 68        |
| <b>Contacting Technical Support .....</b>                               | <b>69</b> |

## Network Requirements

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

| Port Number   | Port Location           |          |                |          | Description  |
|---|-------------------------|----------|----------------|----------|--|
|   | N-able N-central Server |          | Managed Device |          |  |
|   | Inbound                 | Outbound | Inbound        | Outbound |  |
| 20  |                         | √        |                |          | Used for FTP connections, particularly when configured for backups.  |
| 21  |                         | √        |                |          | Used for FTP connections, particularly when configured for backups.  |
| 22  | √                       |          |                | √        | SSH - used for remote control sessions. The firewall must be configured to allow access from the Internet to this port on the N-able N-central server.   |
| 25  |                         | √        |                |          | SMTP - used for sending mail.  |
| 53  |                         | √        |                |          | Used for DNS.  |
| 80  | √                       | √        |                | √        | <p>HTTP - used for communication between the N-able N-central UI and agents or probes (including MSP Connect and MSP Anywhere).</p> <p>The firewall must be configured to allow access from the Internet to this port on the N-able N-central server.</p> <p>This port must also be open for outbound traffic if the N-able N-central server is monitoring the HTTP service on a managed device.</p> |
| <div style="border: 1px solid #0070C0; padding: 5px;"> <p><span style="color: #0070C0;">i</span> Inbound access to port 80 on the N-able N-central server can be blocked provided that all Agents are configured to use HTTPS and the N-able N-central server is accessed over port 443 using HTTPS.</p> </div> |                         |          |                |          |  |
| 123   |                         | √        |                |          | Used by the NTP Date service which keeps the server clock synchronized. Normally using UDP (although some servers can use TCP).  |

| Port Number | Port Location           |          |                |          | Description  |
|-------------|-------------------------|----------|----------------|----------|--|
|             | N-able N-central Server |          | Managed Device |          |  |
|             | Inbound                 | Outbound | Inbound        | Outbound |  |
| 135         |                         |          | √              |          | <p>Used by Agents and Probes for WMI queries to monitor various services.</p> <div style="border: 1px solid #0070C0; padding: 5px;"> <p> Inbound from the Windows Probe to the Windows Agent.</p> </div>  |
| 139         |                         |          | √              |          | <p>Used by Agents and Probes for WMI queries to monitor various services.</p> <div style="border: 1px solid #0070C0; padding: 5px;"> <p> Inbound from the Windows Probe to the Windows Agent.</p> </div>  |
| 443         | √                       | √        |                | √        | <p>HTTPS - used for communication between the N-able N-central UI and Agents or Probes (including MSP Connect and MSP Anywhere).</p> <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 N-able N-central server.</p> <p>This port must also be open for outbound traffic if the N-able 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 N-able N-central server.</p> <p>Used by Agents and Probes for XMPP traffic. Outbound access to port 443 for Managed Devices is recommended but not required.</p> <p>To activate EDR the N-able N-central server needs outbound HTTPS access to port 443 and the following domains:</p> <ul style="list-style-type: none"> <li>■ *.sentinelone.net</li> <li>■ sis.n-able.com</li> <li>■ keybox.solarwindmsp.com</li> </ul> |

| Port Number  | Port Location           |          |                |          | Description  |
|--|-------------------------|----------|----------------|----------|--|
|  | N-able N-central Server |          | Managed Device |          |  |
|  | Inbound                 | Outbound | Inbound        | Outbound |  |
| 445  |                         |          | √              |          | Used by Agents and Probes for WMI queries to monitor various services.   |
| 1234   |                         | √        |                | √        | Used by MSP Connect in UDP mode.   |
| 1235   |                         | √        |                | √        |  |
| 1433   |                         | *        | *              | *        | <p>Outbound on the N-able N-central server, port 1433 is used by Report Manager for data export. On managed devices, it is also used by Agents (inbound) and Probes (outbound) to monitor Backup Exec jobs.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Inbound from the local LAN and not the Internet.</p> </div> |
| <p>* Port access is only required if you have installed the corresponding product. For example, access to port 1433 is only required if you have installed Report Manager or if you are managing Backup Exec jobs.</p> |                         |          |                |          |  |
| 5000   |                         | √        |                |          | Backup Manager will use local port 5000. If this port is unavailable, Backup Manager will detect a free port automatically (starting from 5001, 5002 and up).  |
| 8014   |                         |          | √              |          | <p>Backup Manager requires access to port 8014. This value cannot be modified.</p> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p> Inbound from the local LAN and not the Internet.</p> </div>  |
| 8800   |                         | √        |                |          | <p>The Feature Flag System in N-able N-central needs to talk to <code>mtls.api.featureflags.prd.sharedsvcs.system-monitor.com</code>.</p> <p>Used by N-able – generally during Early Access Preview and Release Candidate testing – to enable and disable features within N-able N-central.</p>  |



| Port Number | Port Location           |          |                |          | Description  |
|-------------|-------------------------|----------|----------------|----------|--|
|             | N-able N-central Server |          | Managed Device |          |  |
|             | Inbound                 | Outbound | Inbound        | Outbound |  |
| 10000       | √                       |          |                |          | <p>HTTPS - used for access to the N-able N-central Administration Console (NAC). The firewall must be configured to allow access from the Internet to this port on the N-able N-central server.</p> <p>N-able recommends excluding all other inbound traffic to port 10000 except from N-able Ports for Support section below.</p>   |
| 10004       |                         |          | √              | √        | <p>N-able N-central Agents must be able to communicate with a Probe on the network over port 10004 in order for Probe caching of software updates to function properly.</p> <div data-bbox="873 898 1511 1003" style="border: 1px solid #0070C0; padding: 5px;"><p> Inbound from the local LAN and not the Internet.</p></div>                |
| 15000       |                         |          | √              | √        | <p>For downloading software patches, port 15000 must be accessible for inbound traffic on the Probe device while it must be accessible for outbound traffic on devices with Agents.</p> <div data-bbox="873 1213 1511 1318" style="border: 1px solid #0070C0; padding: 5px;"><p> Inbound from the local LAN and not the Internet.</p></div> |



---

## 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)



## N-able N-central System requirements

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

If you have any questions about how your needs affect the system requirements of your N-able N-central server, contact your Channel Sales Specialist or email [n-able-salesgroup@n-able.com](mailto:n-able-salesgroup@n-able.com).

|                          |  |
|--------------------------|--|
| <b>Processor</b>         | Server class x86_64 CPUs manufactured by Intel or AMD (i.e. Xeon or EPYC). Please refer to the <a href="#">Red Hat Hardware Ecosystem</a> for further details.   |
| <b>Operating System</b>  | You do not need to install a separate Operating System to run N-able N-central. The N-able N-central ISO includes a modified version of CentOS 7, based on the upstream Red Hat Enterprise Linux 7.  |
| <b>Physical Hardware</b> | <p>The physical server used to install N-able N-central in a bare metal environment must be certified to run Red Hat Enterprise Linux 7.7 (x64) by Red Hat, or the hardware vendor, without any additional drivers. Please check the <a href="#">Red Hat Hardware Ecosystem</a> 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 N-able N-central.</p> |

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

### System requirements by number of devices managed

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

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

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

#### Notes

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

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

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

| Subsystem            | Limit |
|----------------------|-------|
| Maximum memory       | 12TB  |
| Maximum logical CPUs | 768   |

#### Examples of supported servers

Due to the ecosystem of different hardware, N-able does not certify specific hardware configurations. Instead we rely on the upstream Red Hat Enterprise Linux and hardware vendor testing and certification.

Examples of servers that have been Red Hat certified include [HPE ProLiant DL360 Gen10](#) and [Dell PowerEdge R620](#).

Please consult with your hardware vendor to ensure that any server to be used for a bare metal installation meets the above requirements, and is Red Hat Enterprise Linux 7.7 certified, without the need for additional drivers.

N-able 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

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

### **⚠️ Hyper-V on Windows Desktop Operating Systems not Supported.**

N-able 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 N-able 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 N-able 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.

|                           |  |
|---------------------------|--|
| <b>System Performance</b> | <p>It is impossible to guarantee the scalability or performance of a N-able N-central server deployed on a Virtual Machine due to:</p> <ul style="list-style-type: none"> <li>■ variability in field environments resulting from host server configurations,</li> <li>■ the number of virtual guests run on the host server, and</li> <li>■ the performance of the underlying host hardware.</li> </ul>  |
| <b>Supportability</b>     | <p>N-able supports N-able 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 N-able N-central deployed on Bare Metal. This support is limited to the components (Software and Operating System) shipped with N-able N-central and does not include the troubleshooting of virtualization systems nor of performance issues related to environmental factors.</p> <p>N-able recommends reaching out to your hardware or virtualization vendor for support on the underlying virtualization and hardware components. Any assistance provided by N-able 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 N-able N-central system to a physical hardware deployment.</p> |

|                                 |  |
|---------------------------------|--|
| <b>Virtual Hardware Support</b> | <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 <b>Secure Boot</b>, please select the <b>Microsoft UEFI Certificate Authority</b> template.</p> <p>For VMWare ESX/ESXi deployments, it is recommended to select the <b>Red Hat Enterprise Linux 7</b> guest OS template, then under the <b>Boot Options</b>, select the <b>UEFI Firmware</b>.</p> |
| <b>Network Adapters</b>         | <p>N-able 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, N-able 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>   |
| <b>MAC Addresses</b>            | <p>By default, most virtualization environments use a dynamically assigned MAC address for each virtual network card. As your N-able 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 N-able N-central server.

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

## Supported Software

### Browsers

N-able N-central supports the latest versions of:

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

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

Workaround:

In the Chrome address bar, type `chrome://flags`.

Under **Enable NPAPI**, click **Enable**.

Restart Chrome.

N-able 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:

- .NET Framework 4.5.2 on Windows devices
- Oracle Java 1.8 versions that include Java Web Start

## Report Manager

To use Report Manager with N-able 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 N-able N-central.

## SNMP Community String

On HPE ProLiant Generation 9 or older Physical Servers, when monitoring the N-able N-central server using SNMP, the community string used for SNMP queries to the server must use `N-central_SNMP`, not `public`. SNMP is only enabled on HPE ProLiant Generation 9 or older Physical Servers. All other installs do not enable SNMP on the N-able N-central server.

## Supported Operating Systems

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

### Windows Agents:

- Microsoft .NET Framework 4.5.2 (or later)

### Windows Server 2019

- Windows Server 2019 Datacenter
- Windows Server 2019 Standard

## Windows Server 2016

- Windows Server 2016 Datacenter
- Windows Server 2016 Standard
- Windows Server 2016 Essentials
- Windows Storage Server 2016
- Windows Server 2016 MultiPoint Premium Server
- Microsoft Hyper-V Server 2016

## Windows Server 2012

- R2 Datacenter
- R2 Essentials
- R2 Foundation
- R2 Standard
- Datacenter 64-bit Edition
- Essentials 64-bit Edition
- Foundation 64-bit Edition
- Standard 64-bit Edition
- Microsoft Hyper-V Server 2012
- Microsoft Hyper-V Server 2012 R2
- Storage Server 2012 Enterprise 64-bit Edition
- Storage Server 2012 Express 64-bit Edition
- Storage Server 2012 Standard 64-bit Edition
- Storage Server 2012 Workgroup 64-bit Edition

## Windows 10

- Microsoft Windows 10 Enterprise & Professional
- Microsoft Windows 10 Education editions
- Windows 10 Pro for Workstations

## Windows 8 and 8.1

- 8.1 Enterprise
- 8.1 Professional
- 8 Enterprise
- 8 Professional

## Windows 7

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

## Mac Agents

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

## Linux Agents

Independent Agents are required for 32-bit and 64-bit Linux OS installations.

💡 The probe performs an SSH connection a Linux device. To discover a Ubuntu/Debian OS device, the device must have openssh installed.

- Red Hat Enterprise Linux/CentOS 8 (64-bit)
- Red Hat Enterprise Linux/CentOS 7 (x86\_64 and i686)
- Red Hat Enterprise Linux/CentOS 6 (x86\_64 and i686)
- Ubuntu 18.04 "Bionic Beaver" (x86\_64)
- Ubuntu 16.04 "Xenial Xerus" (x86\_64 and i686)
- Debian 8.7/Ubuntu 14.04 "Trusty Tahr" (x86\_64 and i686)

## AV Defender

### Workstation Operating Systems

- Microsoft Windows 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 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 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

The following operating systems are not supported with N-able N-central patch manager:

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

### Windows Update Agent

The minimum version of the Windows Update Agent (WUA) needs to be greater than 7.6.7600.320. The base NT build version of Windows should be 6.1 or later. Older versions of the base NT build cannot upgrade past version 7.6.7600.256 of the Windows Update Agent.

## Automation Manager

### Workstation Operating Systems

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

### Server Operating Systems

- Microsoft Windows Server 2019
- Microsoft Windows Server 2016 (32/64-bit)
- Microsoft Windows Server 2012 R2 (32/64-bit)
- Microsoft Windows Server 2012 (32/64-bit)

## Disk Encryption Manager

|  |  |
|--|--|
| Hyper-V Server 2012 R2                     | Hyper-V Server 2016                        |
| Windows 7 Enterprise                       | Windows 7 Home Premium                     |
| Windows 7 Professional                     | Windows 7 Ultimate                         |
|  |  |
| Windows 8 Enterprise                       | Windows 8 Pro                              |
| Windows 8 Pro with Media Center            | Windows 8.1 Enterprise                     |
| Windows 8.1 Pro                            | Windows 8.1 Pro with Media Center          |
|  |  |
| Windows 10 Education                       | Windows 10 Enterprise                      |
| Windows 10 Enterprise 2015 LTSC            | Windows 10 Enterprise 2016 LTSC            |
| Windows 10 Enterprise for Virtual Desktops | Windows 10 Enterprise LTSC 2019            |
| Windows 10 Pro                             | Windows 10 Pro Education                   |
| Windows 10 Pro for Workstations            |  |
|  |  |
| Windows Server 2008 R2 Enterprise          | Windows Server 2008 R2 Datacenter          |
| Windows Server 2008 R2 Standard            | Windows Server 2008 R2 Foundation          |
| Windows Server 2012 Datacenter             | Windows Server 2012 Essentials             |
|  |  |
| Windows Server 2012 Foundation             | Windows Server 2012 R2 Datacenter          |
| Windows Server 2012 R2 Essentials          | Windows Server 2012 R2 Foundation          |
| Windows Server 2012 R2 Standard            | Windows Server 2012 R2 Standard Evaluation |
| Windows Server 2012 Standard               |  |
|  |  |
| Windows Server 2016 Datacenter             | Windows Server 2016 Datacenter Evaluation  |
| Windows Server 2016 Essentials             | Windows Server 2016 Standard               |
| Windows Server 2016 Standard Evaluation    |  |



|   |   |
|---|---|
|   |   |
| Windows Server 2019 Datacenter                | Windows Server 2019 Essentials              |
| Windows Server 2019 Standard                  | Windows Server 2019 Standard Evaluation     |
|   |   |
| Windows Server Datacenter                     |   |
| Windows Small Business Server 2011 Essentials | Windows Small Business Server 2011 Standard |

# Installing N-able N-central

You can install N-able N-central on the following platforms:

- A Bare Metal Server with UEFI Firmware enabled (Preferred)
- A Bare Metal Server with Legacy BIOS enabled
- VMWare ESX/ESXi 6.0 or newer with UEFI Firmware enabled (Preferred)
- VMWare ESX/ESXi 6.0 or newer with Legacy BIOS enabled
- Windows Server 2016 or newer Hyper-V Generation 2 (Preferred)
- Windows Server 2012 R2 or newer Hyper-V (Generation 1)
- Microsoft Azure Resource Manager
- Amazon AWS Elastic Cloud Compute (EC2)

**i** Windows Server 2012 R2 Hyper-V Virtualization Server is supported for Generation 1 guest VMs only.

During installation on CentOS and Linux systems, the install performs a hardware detection routines. This can cause error messages to appear on the console at the beginning of the installation. These are normal messages that you will see on any CentOS and Linux during boot, before the splash screen pops up, and does not affect the installation of N-able N-central.

## What do you want to do?

- [Prepare installation media](#)
- [Install on a physical server](#)
- [Install as a guest on VMWare ESX/ESXi 6.0 or newer](#)
- [Install as a guest on Windows Server 2012 R2 or newer Hyper-V](#)
- [Install on Microsoft Azure Resource Manager](#)
- [Install on Microsoft Azure Managed Disks](#)
- [Install on Amazon AWS Elastic Cloud Compute \(EC2\)](#)

## Prepare installation media

To install N-able N-central on a bare metal server, without the option to upload a disk image through iLO, iDRAC or IMM2, you will need to prepare a DVD, or a USB Flash Drive with the N-able N-central installer image.

### DVD Creation

Follow the directions for your DVD creation software to burn the N-able N-central .iso to disk.

### USB Flash Drive

For the USB Flash drive to properly install N-able N-central on both BIOS and UEFI systems, you need to write the .iso image to disk using the “DD” disk writing method. The USB Flash Drive must be at least 2GB in size. You will not be able to use any extra space on the drive until after N-able N-central is installed and you reformat the drive.

 This process is a destructive process for the USB Flash Drive. All data on the USB Flash Drive will be erased.

### Linux and MacOS

1. Elevate to the root user so you can mount the USB Flash Drive.

```
sudo su -
```

2. Identify the USB Flash Drive device name. Be careful to verify the device size so you don't accidentally overwrite another device, like your hard disk.

**Linux:** `lsblk`

**MacOS:** `diskutil list`

3. Write the disk image to the USB Flash Drive. Make sure the device you are writing to is your USB Flash Drive. This step will overwrite all data on the drive. Be sure to specify the device name, not the partition name (`/dev/sdb`, not `/dev/sdb1`).

```
dd if=/path/to/N-central.iso of=/dev/device-name bs=512k
```

### Windows

Use a third-party utility, for example, Rufus, to write the disk image to your USB Flash Drive.

When copying the .iso file, ensure you use the following configuration options:

- **Partition scheme:** “MBR”
- **Target system:** “BIOS or UEFI”
- **Volume label:** Leave it as is. Do NOT change the label!
- **File system:** FAT32
- **Cluster size:** Default

 If you are asked to select the mode used to write the image to disk, use **DD Image mode**. If not selected, N-able N-central may fail to install on certain devices.



## Install N-able N-central on a physical server

Before you begin the install, ensure your install media is set up and ready. For more information, see [Prepare installation media](#).

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 | Configure the RAID controller to use the default stripe size. |
| Lenovo Server |   |
| Cache Options | Use the default settings.                                     |
| Disk RAID 1+0 | Configure the RAID controller to use the default stripe size. |
| Dell Server   |   |
| Cache Options | Set Write Policy to Write-back and Read Policy to Adaptive.   |
| Disk RAID 1+0 | Configure the RAID controller to use the default stripe size. |
| Intel Server  |   |
| Cache Options | Set Write Policy to Write-back and Read Policy to Adaptive.   |
| Disk RAID 1+0 | Configure the RAID controller to use the default stripe size. |

2. Enter the Server Hardware Level Configuration Utility (BIOS) and enable the **UEFI Firmware booting** (Recommended, but Legacy BIOS is also supported).
3. Insert the installation disc or USB Flash drive and restart the server.
4. **If using a USB drive, use the BIOS/UEFI Boot Menu to select the USB Flash Drive as your boot device.**
5. If the **Press the <ENTER> key to install N-central** prompt displays, click **Enter**.

 This will not display if you have Secure Boot enabled.

6. Click **Enter** to Install N-able N-central unless you want to test the physical media or need to install in text only mode (usually if you are using a serial console). Otherwise select the desired boot option and click **Enter**.

 After a few moments, you should be prompted to provide the N-able N-central network settings. If you are not prompted to provide the network settings, N-able N-central was unable to locate a suitable network card. Turn off the server and verify the network card before re-trying the N-able N-central installation.

7. Select which IP stack/s you need to enable (**IPv4 only**, or both **IPv4 and IPv6**). Click **Tab** to highlight **OK** and click **Enter**.

8. Select your IPv4 network configuration. N-able recommends using a **Static IPv4 Address**. Tab to **OK** and click **Enter**.
9. If you selected to use a dual stack configuration, select your IPv6 network configuration. N-able recommends using a **Static IPv6 Address**. Tab to **OK** and click **Enter**.
10. If you selected a **Static IPv4 Address** configuration, enter the **IP Address**, **Netmask**, **Gateway** and **Nameservers** (CloudFlare's 1.1.1.1 has been pre-populated by default). Tab to **OK** and click **Enter**.
11. If you selected a **Static IPv6 Address** configuration, on the next screen enter the **IP Address**, **Prefix Length** (/64 is the most common), **Gateway**, and **Nameservers** (CloudFlare's 1.1.1.1 has been pre-populated by default). Select **OK** and click **Enter**.
12. On the next page, select your desired **Time Zone**. Tab to **OK** and click **Enter**.

 Be sure to Adjust the Time Zone to match your desired location. If you are restoring a N-able N-central Backup, the Time Zone must be an exact match to the server from which you are restoring the Backup.  
If your location is not listed, be sure to select a location that is in the same time zone as you are.

13. The Operating System Installer will now launch. No further input is required on the server console. When the install completes, please go to the indicated web URL to continue configuring N-able N-central.

Ensure you remove the DVD/USB Flash Drive once the Green complete screen appears to ensure that the server does not boot from the DVD/USB Flash Drive at a later time.

 **HPE ProLiant Generation 9** and older servers will have the HPE monitoring drivers installed and SNMP enabled on the N-able N-central server. You must use the Community String `N-CENTRAL_SNMP` to monitor your N-able N-central server.

**HPE ProLiant Generation 10** or newer servers no longer use the Operating System drivers to monitor the hardware. Hardware monitoring is handled through the iLO port.

**Dell PowerEdge** servers may be monitored through the iDRAC port depending on the server feature set and licensing.

**Lenovo** servers may be monitored through the IMM port depending on the server feature set and licensing.

What's next?

With N-able N-central installed:

- review the [Getting Started](#) help topics
- setup [Service Organizations](#), [Customers](#) and [Sites](#), and
- [configure users](#).

## Install N-able N-central as a guest on an ESX/ESXi 6.0 or newer server

**i** VMWare Tools are no longer required to be install on the N-able N-central VM. As per VMware recommendations for Enterprise Linux 7, the OpenVM Tools are included with the Operating System.

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

|                           |  |
|---------------------------|--|
| <b>OS Version</b>         | Red Hat Enterprise Linux 7 (64-bit)<br>Do not enable paravirtualization. |
| <b>Boot Options</b>       | Select UEFI Firmware (Legacy BIOS is also supported).                    |
| <b>Virtual Disks</b>      | Thick Provision  |
| <b>CPU/Memory/Storage</b> | Size according to tables in the <a href="#">System Requirements</a> .    |
| <b>Network Adapter</b>    | VMXNET3 with a static MAC address.                                       |

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. If the **Press the <ENTER> key to install N-central** prompt displays, click **Enter**.
5. Click **Enter** to install N-able N-central unless you want to test the physical media or need to install in text only mode (usually if you are using a serial console). Otherwise select the desired boot option and click **Enter**.

**i** After a few moments, you should be prompted to provide the N-able N-central network settings. If you are not prompted to provide the network settings, N-able N-central was unable to locate a suitable network card. Turn off the server and verify the network card before re-trying the N-able N-central installation.

6. Select which IP stack/s you need to enable (**IPv4 only**, or both **IPv4 and IPv6**). Click **Tab** to highlight **OK** and click **Enter**.
7. Select your IPv4 network configuration. N-able recommends using a **Static IPv4 Address**. Tab to **OK** and click **Enter**.
8. If you selected to use a dual stack configuration, select your IPv6 network configuration. N-able recommends using a **Static IPv6 Address**. Tab to **OK** and click **Enter**.
9. If you selected a **Static IPv4 Address** configuration, enter the **IP Address**, **Netmask**, **Gateway** and **Nameservers** (CloudFlare's 1.1.1.1 has been pre-populated by default). Tab to **OK** and click **Enter**.
10. If you selected a **Static IPv6 Address** configuration, on the next screen enter the **IP Address**, **Prefix Length** (/64 is the most common), **Gateway**, and **Nameservers** (CloudFlare's 1.1.1.1 has been pre-populated by default). Select **OK** and click **Enter**.

11. On the next page, select your desired **Time Zone**. Tab to **OK** and click **Enter**.

 Be sure to Adjust the Time Zone to match your desired location. If you are restoring a N-able N-central Backup, the Time Zone must be an exact match to the server from which you are restoring the Backup.

If your location is not listed, be sure to select a location that is in the same time zone as you are.

12. The Operating System Installer will now launch. No further input is required on the server console. When the install completes, please go to the indicated web URL to continue configuring N-able N-central.

What's next?

With N-able N-central installed:

- review the [Getting Started](#) help topics
- setup [Service Organizations](#), [Customers](#) and [Sites](#), and
- [configure users](#).

## Install N-able N-central as a guest on Windows Server 2012 R2 or newer Hyper-V server

### **Hyper-V on Windows Desktop Operating Systems not Supported.**

Desktop versions of Microsoft Windows, with the Hyper-V feature enabled are **not supported as a host for N-able N-central**. The Hyper-V feature must be enabled on a supported version of the Windows Server 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 N-able 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 N-able N-central.

### **Dynamic Memory is not supported.**

N-able N-central does not support the use of Dynamic Memory under Hyper-V. Enabling Dynamic Memory can lead to Kernel Panics, Service crashes, and Database corruption.

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

|                             |   |
|-----------------------------|---|
| <b>Generation</b>           | Generation 2 (preferred).   |
| <b>Firmware</b>             | Move the DVD Drive to the top of the boot order.  |
| <b>Security</b>             | Under the <b>Secure Boot</b> section, select the <b>Microsoft UEFI Certificate Authority</b> from the <b>Template</b> drop-down menu.   |
| <b>Memory</b>               | Size according to tables in <a href="#">System Requirements</a> .<br>Disable "Dynamic Memory".  |
| <b>Processor</b>            | Size according to the table in <a href="#">System Requirements</a> . Expand the <b>Processor</b> options (+). In the <b>NUMA</b> subsection, click <b>Use Hardware Topology</b> .   |
| <b>Hard Drive</b>           | Size according to table in the <a href="#">System Requirements</a> .  |
| <b>DVD Drive</b>            | Mount the N-able N-central ISO disk image.  |
| <b>Network Adapter</b>      | Set a static MAC address.   |
| <b>Integration Services</b> | Enable <b>Guest Services</b> .  |
| <b>Checkpoints</b>          | Checkpoints should be disabled except for when you create a cold checkpoint immediately before a N-able N-central upgrade. The Checkpoint should be removed as soon as the upgrade has been successful in order to reduce the performance impact of the Checkpoint Differencing Disk. |

2. Start the new VM.
3. If the **Press the <ENTER> key to install N-central** prompt displays, click **Enter**.
4. Click **Enter** to Install N-able N-central unless you want to test the physical media or need to install in text only mode (usually if you are using a serial console). Otherwise select the desired boot option and click **Enter**.

**i** After a few moments, you should be prompted to provide the N-able N-central network settings. If you are not prompted to provide the network settings, N-able N-central was unable to locate a suitable network card. Turn off the server and verify the network card before re-trying the N-able N-central installation.

5. Select which IP stack/s you need to enable (**IPv4 only**, or both **IPv4 and IPv6**). Click **Tab** to highlight **OK** and click **Enter**.
6. Select your IPv4 network configuration. N-able recommends using a **Static IPv4 Address**. Tab to **OK** and click **Enter**.
7. If you selected to use a dual stack configuration, select your IPv6 network configuration. N-able recommends using a **Static IPv6 Address**. Tab to **OK** and click **Enter**.

8. If you selected a **Static IPv4 Address** configuration, enter the **IP Address**, **Netmask**, **Gateway** and **Nameservers** (CloudFlare's 1.1.1.1 has been pre-populated by default). Tab to **OK** and click **Enter**.
9. If you selected a **Static IPv6 Address** configuration, on the next screen enter the **IP Address**, **Prefix Length** (/64 is the most common), **Gateway**, and **Nameservers** (CloudFlare's 1.1.1.1 has been pre-populated by default). Select **OK** and click **Enter**.
10. On the next page, select your desired **Time Zone**. Tab to **OK** and click **Enter**.

 Be sure to Adjust the Time Zone to match your desired location. If you are restoring a N-able N-central Backup, the Time Zone must be an exact match to the server from which you are restoring the Backup.  
If your location is not listed, be sure to select a location that is in the same time zone as you are.

11. The Operating System Installer will now launch. No further input is required on the server console. When the install completes, please go to the indicated web URL to continue configuring N-able N-central.

What's next?

With N-able N-central installed:

- review the [Getting Started](#) help topics
- setup [Service Organizations](#), [Customers](#) and [Sites](#), and
- [configure users](#).

## Install N-able N-central on Microsoft Azure Managed Disks

The instructions below walk you through a new installation of N-able N-central in the Microsoft Azure Managed Disks environment. Microsoft Azure Classic deployment is no longer supported, however, Azure Resource Manager without Managed Disks is still supported.

While we recommend new deployments use this Azure Managed Disk deployment method, the 100GB, 200GB, 500GB and 1TB VHD images are still available for Azure Resource Manager without Managed Disks, and is available and supported for reinstalling and restoring N-able N-central from a backup.

Unlike all other N-able N-central deployments, Azure Managed Disks (MD) deployments support/require at least one Data disk in addition to the Operating System Disk. When you use the deployment script and assign one Data disk, Azure creates a RAID 0 array of the one disk. If you assign  $X$  data disks, Azure creates a RAID 0 of those  $X$  disks. N-able N-central uses a RAID 0 to combine multiple Data disks into a single mount point, while writing to all disks in parallel. This increases the IOPS throughput by  $X$  times.

Additionally, Azure MD deployments have no SWAP Volume, as N-able N-central uses the Resource Disk for the SWAP Volume. The Azure MD OS Disk image is 8 GB, as the install dynamically expands the image to match the deployed Managed Disk size on first boot.

Azure MD images are published to each Public Azure Region, so you no longer need to upload the VHD. It is important to know that there are some Azure Regions that are restricted to certain Azure users. These are a second, geographically separated Azure Region in the same country, or in the case of the EU, another nearby country that is reserved for customers needing in-country disaster recovery. For information on Azure regions, see <https://azure.microsoft.com/en-us/global-infrastructure/geographies/#overview>.

### Deployment

Deploying N-able N-central to Azure with Managed Disks is simplified by using a Deployment PowerShell script. The script requires [PowerShell 7](#) (formerly PowerShell Core) and the [Azure PowerShell Module](#). You can run the script on any operating system that supports the cross platform PowerShell 7.

 You must have basic knowledge of how to use Microsoft Azure, Windows PowerShell and how to install and configure N-able - N-Central.

The script is available for download on the N-able N-central Release page of the [N-able Customer Success Center](#).

After downloading the PowerShell Script, you need to edit the settings at the top of the script to meet your requirements. Some items are required, while others can be left with the defaults unless they need to use specific values, such as the virtual network settings. The script contains full documentation explaining all included options.

For more information, see [Deployment script for Microsoft Azure - Managed Disks](#).

 Ultra\_SSD Data Disks are not supported.

🔔 Before you deploy a dual stack application in Azure, you must configure your subscription for this preview feature using the following Azure PowerShell.

Register as follows:

```
Register-AzProviderFeature -FeatureName AllowIPv6VirtualNetwork -
ProviderNamespace Microsoft.Network
```

It takes up to 30 minutes for feature registration to complete.

You can check your registration status by running the following Azure PowerShell command:

```
Get-AzProviderFeature -FeatureName AllowIPv6VirtualNetwork -
ProviderNamespace Microsoft.Network
```

After the registration is complete, run the following command:

```
Register-AzResourceProvider -ProviderNamespace Microsoft.Network
```

Once you have modified the PowerShell Install Script with your settings, you only need to launch it in a PowerShell console and it will complete the deployment for you. If you have not already logged into your Azure account from PowerShell, the script will prompt you to log in.

If you are using Windows, you may need to complete the following steps to run the script. For more information see the Microsoft article, [Set-Execution Policy](#).

1. Ensure your PowerShell Execution Policy is set to "Remote-Signed".

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Scope LocalMachine
```

2. Un-Block the Install Script.

```
Unblock-File -Path .\AzureMD.ps1
```

## First run

After the PowerShell Script has completed successfully, wait a few minutes before logging into the Web UI. On first run, N-able N-central will expand the OS disk, create a software RAID from the data disks, and move the database to it, then reset the trial license. This process can take 10 - 15 minutes to complete.

🔔 If you try to log in to the web UI right after they VM is deployed, you will be kicked out, and the web UI will be unresponsive for a few minutes while the first run tasks complete.

If you deploy the VM more than 15 days after the Azure image was generated, you will be able to tell the first run activities have not been completed by the expired license warning on the login page. Once the first run tasks complete, the license error will no longer be present.

## VM Sizing

⚠️ Always size N-able N-central for your expected number of devices in the future. Try to plan for at least 2 - 3 years in the future.

The maximum number of supported Data Disks is defined by the Azure VM size. You will need to consult the Azure Documentation for their VM size before deciding on the number of Data Disks. Azure VM sizing can be a little tricky, and may require some trial and error to determine the best VM size for any particular deployment.

💡 VM sizing must support Generation 2 VMs.

Rough guidelines are as follows:

| Number of Devices | Recommended Azure Size | CPU Cores | Memory | OS Disk | Data Disks (Total) |
|-------------------|------------------------|-----------|--------|---------|--------------------|
| Up to 1,000       | Standard_DS2_v2        | 2         | 4 GB   | 80 GB   | 20 GB              |
| Up to 3,000       | Standard_DS3_v2        | 4         | 8 GB   | 110 GB  | 60 GB              |
| Up to 6,000       | Standard_DS4_v2        | 8         | 16 GB  | 200 GB  | 125 GB             |
| Up to 9,000       | Standard_DS5_v2        | 12        | 24 GB  | 300 GB  | 200 GB             |
| Up to 12,000      | Standard_DS5_v2        | 16        | 32 GB  | 400 GB  | 275 GB             |
| Up to 16,000      | Standard_DS32s_v3      | 22        | 48 GB  | 550 GB  | 375 GB             |
| Up to 20,000      | Standard_F32s_v2       | 28        | 64 GB  | 700 GB  | 500 GB             |
| Up to 24,000      | Standard_F48s_v2       | 34        | 80 GB  | 875 GB  | 650 GB             |

#### Notes

- The recommendations are based on N-able N-central requirements balanced with Azure Maximum IOPS. For example, N-able recommends "Standard\_DS5\_v2" as apposed to the newer generation "Standard\_D16s\_v3", because the "Standard\_DS5\_v2" has a maximum IOPS of 51200 as compared to 25600 for the "Standard\_D16s\_v3".
- For best performance, we recommend using the maximum number of Data disks your VM size permits. More small disks will provide better IOPS performance than fewer larger disks.
- The OS disk is still used for temporary storage during the nightly backup to reduce IOPS on the data disks, as well as for the Backup Volume. Therefore there needs to be at least the size of the Data disk, plus OS files, Repository and 15% for the Backup Volume. As a result, the total disk utilization is slightly more than for non-Azure deployments.
- N-able N-central is only supported on Instance types that provide local SSD storage. For Azure based N-able N-central deployments, the Local SSD Resource Disk is used for the swap-file, in place of the swap volume on all other N-able N-central deployments. An example of an unsupported instance type without local SSD storage would be the Dsv4 Series (not to be confused with the supported Ddsv4 Series).
- N-able N-central is only currently supported on Instance types that provide Intel Processors. The newer AMD EPYC Processor instances have not been tested and verified. An example of an unsupported AMD EPYC instance type would be the Dasv4 Series.



---

What's next?

With N-able N-central installed:

- review the [Getting Started](#) help topics
- setup [Service Organizations](#), [Customers](#) and [Sites](#), and
- [configure users](#).

## Deployment script for Microsoft Azure - Managed Disks

Deploying N-able N-central to Azure with Managed Disks is simplified by using a Deployment PowerShell script.

The script is available for download on the N-able N-central **Release** page of the [N-able Customer Success Center](#).

This script requires PowerShell 7.0 or higher. PowerShell 7 is a cross platform version of PowerShell (Formerly called PowerShell Core) that has installers for Windows, MacOS and Linux. You can download the latest version of Powershell on [GitHub](#).

The script is pre-populated with the version of N-able N-central you downloaded it for. If you want to install a different version, replace this value with the full Version number. The version is on the **N-central Download Page** for the version you want to deploy.

Note that Azure Managed Disks are only supported for N-able N-central 2020.2 and higher releases.

For more information on the installation process, see [Install N-able N-central on Microsoft Azure Managed Disks](#).

### Azure information

You can retrieve your Azure subscription ID from the Subscriptions Blade in the Azure Portal.

[https://portal.azure.com/#blade/Microsoft\\_Azure\\_Billing/SubscriptionsBlade](https://portal.azure.com/#blade/Microsoft_Azure_Billing/SubscriptionsBlade)

### Azure Region

Select the Azure region, for example, `eastus` where N-able N-central will be located. Not all features are available in all regions. Check with Microsoft Azure for availability. You can get all the Azure locations using the Azure PowerShell command:

```
Get-AzLocation
```

### Resource naming prefix

The script is designed to use a naming prefix for naming all resources it creates. With the default script configuration, keep this value between 1 - 18 characters, excluding any symbols to avoid exceeding other resource name length limits.

For more information, see [Develop your naming and tagging strategy for Azure resources](#).

### VM size

You will need to define the size of the N-able N-central, Azure, Generation 2, VM Instance, for example, 'Standard\_DS3\_v2'. You can get all the VM sizes in the US East region using the Azure PowerShell command. Use the region where you plan to install N-able N-central:

```
Get-AzVMSize -Location 'eastus'
```

For more information, see [Support for generation 2 VMs on Azure](#).

## Operating system disk size

You will need to define the size of the new OS Managed Disk in GB. It should be greater than 80GB. For more information, see [What disk types are available in Azure?](#)

## Operating system disk storage type

Select the storage type for the Operating System Managed Disk. The valid options are:

- Premium\_LRS,
- StandardSSD\_LRS, and
- Standard\_LRS.

Azure does not support using the UltraSSD\_LRS storage type for Operating System Disks. For more information, see

- [What disk types are available in Azure?](#)
- [Azure Storage redundancy](#)

## Data disks sizes

You will need to set the size of the new Data Managed Disks in GB (each). All the Data Disks will be combined into a software RAID to take advantage of parallel disk writes, spreading the IOPs load across the total number of disks you select.

## Number of data disks

Define the number of Data Managed Disks in the Software RAID array. This value can be between 1 - 99, but the maximum number of Data Disks is defined by the Azure VM Size.

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/generation-2#generation-2-vm-sizes>

## Data disks storage type

Select the storage type for the Data Managed Disk. The valid options are:

- Premium\_LRS,
- StandardSSD\_LRS, and
- Standard\_LRS.

UltraSSD\_LRS is unsupported at this time, but is planned to be added once the Azure PowerShell Modules provide better deployment support.

For more information, see

- [What disk types are available in Azure?](#)
- [Azure Storage redundancy](#)

## Boot diagnostics storage account

Select the storage type for the Boot Diagnostics Storage Account. The valid options are:

- Premium\_LRS,
- StandardSSD\_LRS, and
- Standard\_LRS.

This storage account is used for the Azure VM boot diagnostic logs. It is also used during deployment to temporarily host the VHD image before it is imported to a Managed Disk. This is a seldom used storage account, so it does not have to be on the fasted storage types.

## Boot diagnostics storage account type

Select the type of boot storage account you want to use for the VM Boot Diagnostics storage. N-able N-central requires either **Storage** or **StorageV2**.

- **Storage**: General purpose Storage account that supports storage of Blobs, Tables, Queues, Files and Disks.
- **StorageV2**: General Purpose Version 2 (GPv2) Storage account that supports Blobs, Tables, Queues, Files, and Disks, with advanced features like data tiering.

## Accelerated networking

The N-able N-central image for Azure Managed Disks has been configured to support Accelerated Networking, if desired. For more information, see [Create a Linux virtual machine with Accelerated Networking using Azure CLI](#).

## IPv6 Support

N-able N-central does not yet support IPv6 for monitoring, however the underlying operating system and services are ready to support it in the future. To future proof your deployment, you can configure the Azure deployment with IPv6 support.

Before you deploy a dual stack application in Azure, you must configure your subscription for this preview feature using the following Azure PowerShell commands:

```
Register-AzProviderFeature -FeatureName AllowIPv6VirtualNetwork -  
ProviderNamespace Microsoft.Network
```

It takes up to 30 minutes for feature registration to complete. You can check your registration status by running the following Azure PowerShell command:

```
Get-AzProviderFeature -FeatureName AllowIPv6VirtualNetwork -ProviderNamespace  
Microsoft.Network
```

After the registration is complete, run the following command:

```
Register-AzResourceProvider -ProviderNamespace Microsoft.Network
```

You can generate a random Private IPv6 Network Prefix by going to <https://simplifiedns.com/private-ipv6>.



## N-central sizing on Azure Managed Disk deployment

| Number of Devices | Recommended Azure Size | CPU Cores | Memory | OS Disk | Data Disks (Total) |
|-------------------|------------------------|-----------|--------|---------|--------------------|
| Up to 1,000       | Standard_DS2_v2        | 2         | 4 GB   | 80 GB   | 20 GB              |
| Up to 3,000       | Standard_DS3_v2        | 4         | 8 GB   | 110 GB  | 60 GB              |
| Up to 6,000       | Standard_DS4_v2        | 8         | 16 GB  | 200 GB  | 125 GB             |
| Up to 9,000       | Standard_DS5_v2        | 12        | 24 GB  | 300 GB  | 200 GB             |
| Up to 12,000      | Standard_DS5_v2        | 16        | 32 GB  | 400 GB  | 275 GB             |
| Up to 16,000      | Standard_DS32s_v3      | 22        | 48 GB  | 550 GB  | 375 GB             |
| Up to 20,000      | Standard_F32s_v2       | 28        | 64 GB  | 700 GB  | 500 GB             |
| Up to 24,000      | Standard_F48s_v2       | 34        | 80 GB  | 875 GB  | 650 GB             |

## Install N-able N-central on Microsoft Azure Resource Manager

The instructions below walk you through a new installation of N-able N-central in the Microsoft Azure Resource Manager environment. Microsoft Azure Classic deployment is no longer supported.

 New installs should use [Azure Managed Disks deployment](#). The Azure Resource Manager Install has been deprecated. These instructions are being retained should an existing server needs to be rebuilt, and cannot be rebuilt using the newer Azure Managed Disk deployment.

N-able N-central VHD images for Microsoft Azure are available sized for up to 20,000 devices. Larger deployments are not currently supported. Performance of N-able - N-Central above 9,000 devices cannot be guaranteed on Microsoft Azure.

N-able recommends that you plan your deployment with N-able Support in advance.

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

 Creating snapshots for backups is not supported with N-able N-central with Azure.

### 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.
- Windows 10, or [Windows Management Framework 5.1](#).

Set up the PowerShell and Azure environment. PowerShell commands are used to perform the Azure steps required to upload the virtual machine image file and create an Azure 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://docs.microsoft.com/en-us/powershell/azure/install-az-ps?view=azps-2.0.0>.

### 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 N-able N-central VHD

**⚠** Azure Resource Manager VHD images will no longer be built in future releases. A limited subset of the image sizes *may* be released between 2020.2 and the eventual end of support for the older Azure Resource Manager VHD images.

Download the image file for the version and disk size of N-able N-central you want to install. Extract the .VHD file on your local workstation. To reduce the size of the Azure Image files, they are compressed using XZ compression in the 7-Zip format. Use a compatible utility to decompress the image.

**i** The extraction of even the 100 GB .VHD file can take over an hour to complete.

The N-able N-central Virtual Hard Disk (VHD) image is available on the N-able Resource Center. You will need enough free space to extract the full size of the image to the local disk. The images are 100GB, 200GB, 500GB or 1TB in size when fully expanded.

1. Login to the N-able Resource Center (<https://nrc.n-able.com/>).
2. Click the hamburger menu (☰) and click **Support > Software Downloads > N-central**.
3. Click the link for the latest release of N-able 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 .VHD file using a tool such as 7-zip. The extraction of the 100GB VHD image can take over an hour to complete. 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://docs.microsoft.com/en-us/powershell/azure/install-az-ps?view=azps-2.0.0>.

**i** 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:

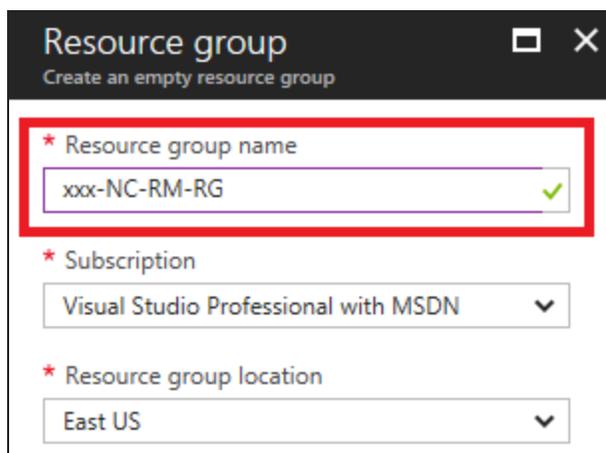
- Uninstall the AzureRM component modules: `Uninstall-AzureRM`
  - Uninstall the AzureRM module: `Uninstall-Module AzureRM`
  - Uninstall the Azure module: `Uninstall-Module Azure`
3. Close PowerShell and run the **Microsoft Azure PowerShell Uninstaller** from the **Programs and Features** in the **Control Panel**.
  4. Reboot the system and install the new Azure Resource Manager PowerShell Module as an Administrator:  
`Install-Module -Name Az -AllowClobber`
  5. From the PowerShell console as Administrator, import the required PowerShell Azure Resource Manager Module previously installed:  
`Import-Module Az`

## Create a Resource Group

Microsoft Azure is continually improving the user interface. As a result, the screen captures in these procedures may already be out of date. You may need to adjust your steps accordingly.

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**

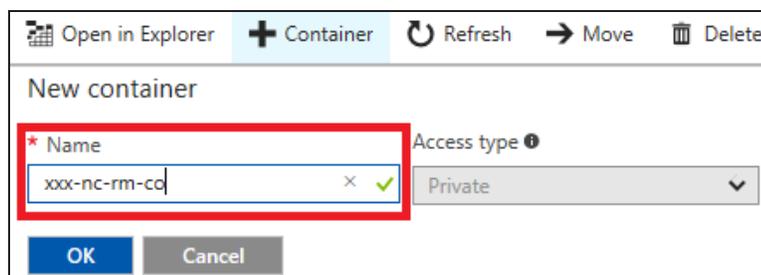
East US ▾

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. Click **OK**.

## Upload the VHD

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

```
Login-Az
```

An Azure credentials window opens.

Typing `Get-AzSubscription` displays the Azure Subscriptions.

```
PS C:\WINDOWS\system32> Get-AzSubscription
Name                               Id                               TenantId                           State
----                               -
Visual Studio Professional         xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx Enabled
ACME Corp. Azure Cloud              xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx 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"
```

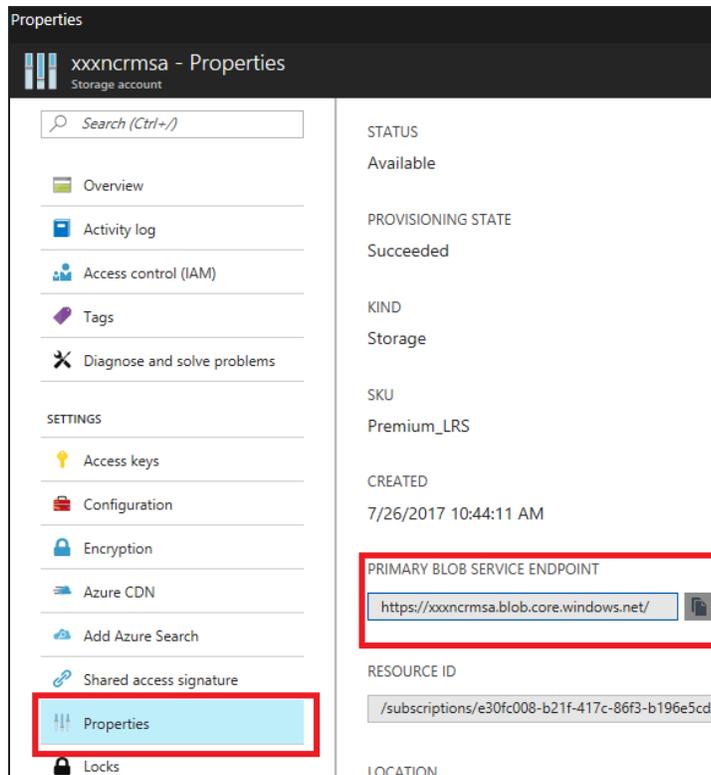
3. Set the Azure Image File name (The file name of the .vhd file you extracted):

```
$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"
```

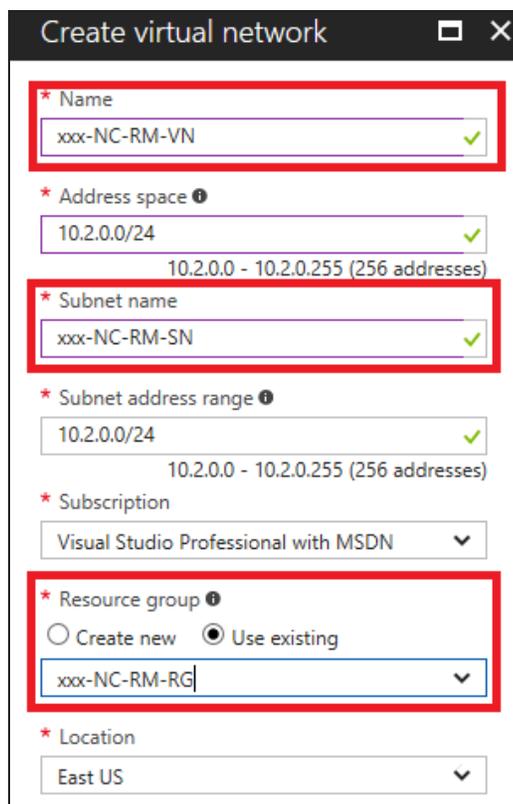
7. Upload the VHD file to Azure:

```
Add-AzVhd -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... ✕

\* Name  
xxx-NC-RM-SG ✓

\* Subscription  
Visual Studio Professional with MSDN ▾

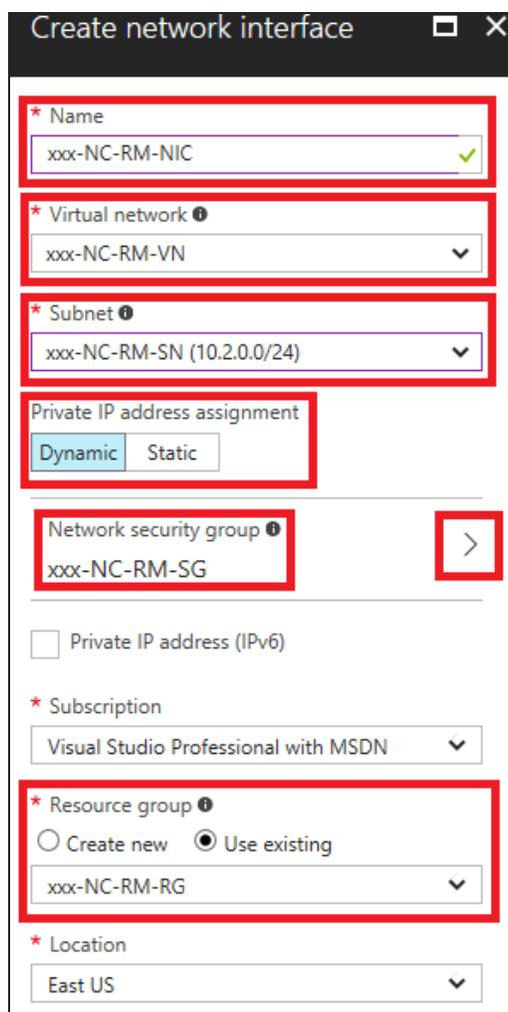
\* Resource group ⓘ  
 Create new  Use existing  
xxx-NC-RM-RG ▾

\* 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

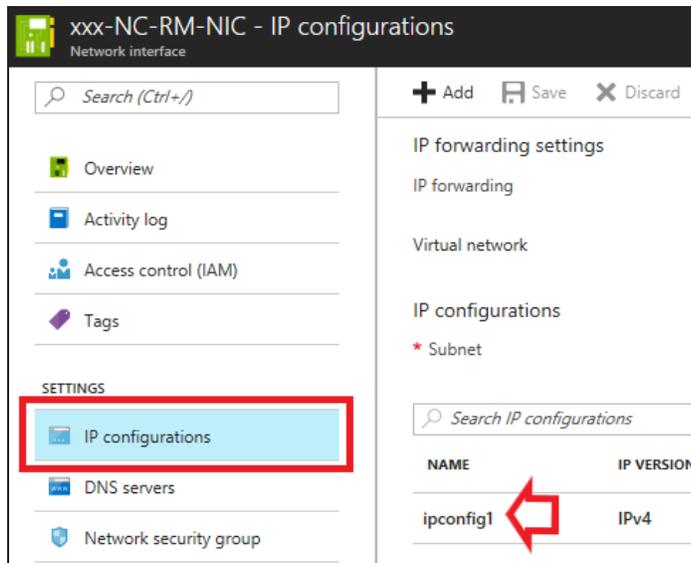
\* Location  
East US

4. Click **Create**.

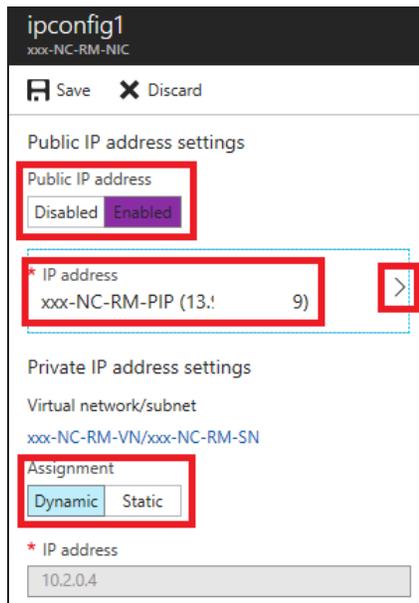
Link the Public IP to the NIC

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.



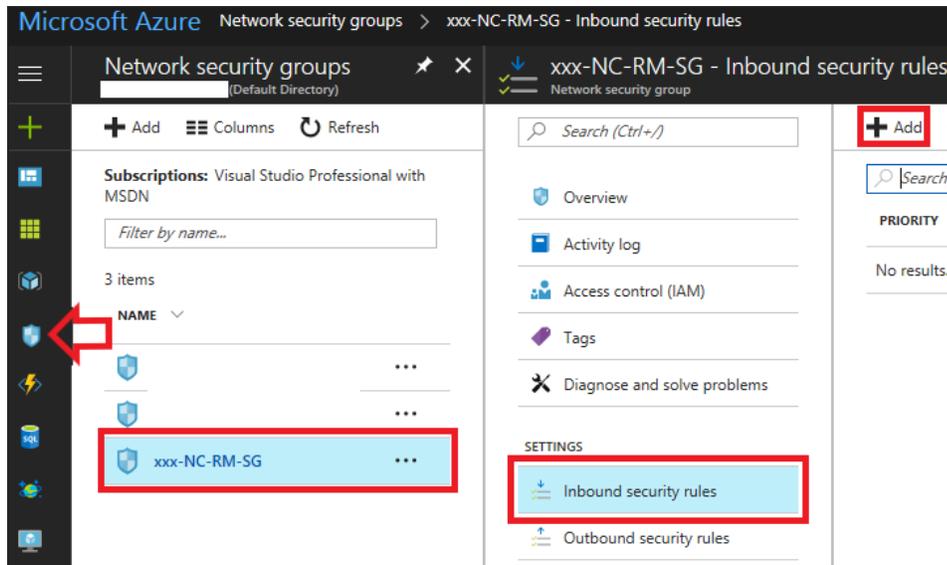
3. Complete the information as shown in the image below.



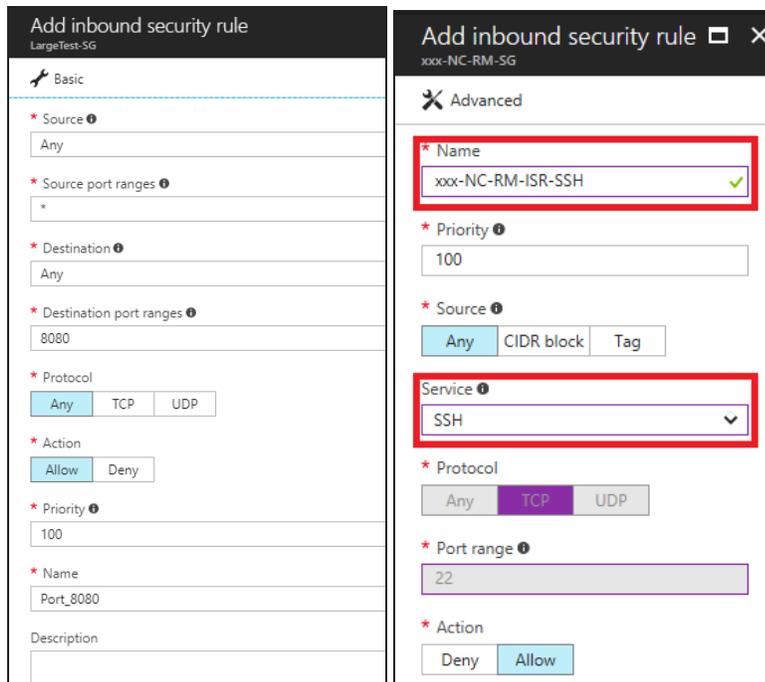
Create the Inbound Security Rules for N-able N-central.

Create security rules to connect with N-able N-central.

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



3. 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, 5280, 10000, and any other ports you may require.



Security rules

+ Add Default rules

Search inbound security rules

| 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  |

4. 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 N-able 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-AzNetworkInterface -Name "xxx-NC-RM-NIC" -ResourceGroupName
$ResourceGroup
$storageAcc = Get-AzStorageAccount -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 N-able N-
central Install Guide and the above considerations.
$vmName = "xxx-NC-RM-VM"
$osDiskName = "xxx-NC-RM-DSK"
$vm = New-AzVMConfig -VMName $vmName -VMSize $VMSize
$vm = Add-AzVMNetworkInterface -VM $vm -Id $nic.Id
$vm = Set-AzVMOSDisk -VM $vm -Name $osDiskName -VhdUri $UploadURL -CreateOption
attach -Linux
New-AzVM -ResourceGroupName $ResourceGroup -Location $location -VM $vm
```

The new N-able 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 N-able N-central server configuration can continue as outlined the *Install Guide*.

To monitor the state of this VM, you can use the Azure portal.

💡 Be sure to adjust the time zone to match your desired location. If you are restoring a N-able N-central backup, the time zone must be an exact match to the server from which you are restoring the backup. If your location is not listed, be sure to select a location that is in the same time zone as you are.

What's next?

With N-able N-central installed:

- review the [Getting Started](#) help topics
- setup [Service Organizations](#), [Customers](#) and [Sites](#), and
- [configure users](#).

## Install N-able 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 the sizing information table in the [System Requirements](#).
6. Click **Next: Configure Instance Detail**, then **Click Next: Add Storage**.
7. Set the appropriate storage size for your instance based on the sizing information table in the [System Requirements](#).

 N-able N-central AWS EC2 Instances have a maximum useable storage size of 2TB.

8. In the **Volume Type** drop-down list box, select **General Purpose SSD (GP2)** (Provisioned IOPS can provide better disk performance, but at a higher cost).
9. Click **Review and Launch**.
10. On the Review Page, click **Edit security groups**.
11. Create a security group, and open the inbound TCP ports 22, 80, 443, 5280, 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 (If you provide a keypair, it will be ignored and not installed).
14. Click **Launch Instances**.

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

 Be sure to Adjust the Time Zone to match your desired location. If you are restoring a N-able N-central Backup, the Time Zone must be an exact match to the server you are restoring the Backup from.

What's next?

With N-able N-central installed:

- review the [Getting Started](#) help topics
- setup [Service Organizations](#), [Customers](#) and [Sites](#), and
- [configure users](#).

# Upgrading N-able N-central

This document includes the following upgrade procedures:

- [Step 1: Back up the N-able N-central server](#)
- [Step 2: Install the N-able 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 N-able 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 N-able N-central server

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

### Pre-Backup Snapshot.

If you are running N-able N-central as a virtual machine, before upgrading, you may wish to create a Snapshot of the virtual machine. In order to avoid corruption of the Snapshot due to database tables being cached in memory, you will need to **shut down** the N-able N-central virtual machine before creating the Snapshot.

N-able recommends shutting down the virtual machine and **deleting the Snapshot** after the upgrade has completed successfully. Deleting the Snapshot will prevent increased disk write latency associated with the differencing disks used by Snapshot technologies.

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

 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 N-able 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 N-able N-central server upgrade](#).

## Step 2: Install the N-able N-central server upgrade

You can upgrade to N-able N-central 2021.1 by installing the upgrade file downloaded to your N-able N-central server or from the [N-able Resource Center](#).

1. Log into the N-able N-central Administration Console using one of the following URLs:
  - <https://<Your Server Address>/admin>
  - <https://<Your Server Address>:10000/>
2. On the Administrator Console under the **Setup** section, click **Version Management**.
3. Choose one of the following:

| N-central Direct upgrade  | Remote upgrade from download location   |
|---|---|
| <ol style="list-style-type: none"> <li>a. Select <b>Install upgrade from local repository</b>.</li> <li>b. Select an upgrade version from the list of available options.</li> </ol> | <ol style="list-style-type: none"> <li>a. Select <b>Install upgrade remotely</b>.</li> <li>b. Click <b>Browse</b> and navigate to the .nsp file in the <a href="#">N-able Resource Center</a>.</li> </ol> |

4. Enter an e-mail address in the **Notify this email address when complete** field.
5. Click **Install**.

If you selected the Remote Upgrade option, the .nsp file will now be uploaded to the N-able N-central server.

Please upload the .nsp upgrade file from a machine local to the N-able N-central server in order to avoid a file upload timeout on a slow internet connection.

Once the .nsp file is uploaded, or if you are installing from the local repository, the upgrade file will now be extracted to the N-able N-central server. This can take a few moments.

6. Click **Confirm** to begin the install.

The N-able N-central Web UI and services will be stopped and the upgrade will be applied.

You can monitor the progress of the SolarWinds N-central upgrade from the server console.

Do not reboot the N-able N-central server during the upgrade process even if it appears unresponsive.

To continue, proceed to [Step 3: Post-installation steps](#).

## Step 3: Post-installation steps

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

| <input checked="" type="checkbox"/>   | Check items as they are completed  |
|---|--|
| <input type="checkbox"/>  | Verify the version of N-able N-central by signing in and click <b>Help &gt; Version Information</b> . The Associated Upgrades displayed must read <code>Applied-update-2021.1.0.xxx-b1_0_xxx</code> , where xxx is a number.   |
| <input type="checkbox"/>  | Verify the network settings and default settings by clicking <b>Administration &gt; Mail Network Settings &gt; Network Setup</b> .   |
| <input type="checkbox"/>  | Verify that the user accounts exist and are accessible.  |
| <input type="checkbox"/>  | Verify that the customer profiles are complete and accurate.   |
| <input type="checkbox"/>  | Verify that the devices are present.   |
| <input type="checkbox"/>  | Verify that the services for each device are reporting correctly.  |
| <input type="checkbox"/>  | Verify that all of the notification profiles are present.  |
| <input type="checkbox"/>  | Verify that the reports generate and display the accurate historical data.   |
| <input type="checkbox"/>  | <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"> <li>1. Click <b>Administration &gt; Defaults &gt; Appliance Settings</b>.</li> <li>2. Select the <b>Upgrade Windows Probes</b> option as either <b>Never</b> (the Probe software will not ever be upgraded) or <b>Always</b> (the Probe software is always upgraded).</li> <li>3. Click <b>Propagate</b> to distribute this configuration setting to existing devices.</li> <li>4. Click <b>Reboot device if necessary</b> to automatically restart devices after the Probe software has been upgraded.</li> <li>5. Click the <b>Upgrade Agents</b> option as either <b>Never</b> (the Agent software will not ever be upgraded) or <b>Always</b> (the Agent software is always upgraded).</li> <li>6. Click <b>Propagate</b> to distribute this configuration setting to existing devices.</li> <li>7. Click <b>Reboot device if necessary</b> to automatically restart devices after the Agent software has been upgraded.</li> </ol> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <p><b>i</b> 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.</p> </div> |
| <p>Once the upgrade procedure has been completed, generate an Agent/Probe Overview report by clicking <b>Reports &gt; Administrative &gt; Agent/Probe Overview</b> in the navigation pane. This will allow you to verify that all probes have been updated.</p> |  |

|    | Check items as they are completed   |
|---|---|
|   | <p> 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:<br/>Upgrade your monitoring software automatically for specific Customers or Sites:<br/>Upgrade your monitoring software automatically for specific devices:</p> <ol style="list-style-type: none"><li>1. In the navigation pane, click <b>All Devices</b>.</li><li>2. Select the Service Organizations, Customers or Sites, or devices to upgrade.</li><li>3. Click <b>Update Monitoring Software</b>.</li><li>4. In the <b>Upgrade Monitoring Software</b> dialog box, select <b>Now</b> for the monitoring software you want to upgrade from the following:<ul style="list-style-type: none"><li>■ <b>Upgrade Agent</b></li><li>■ <b>Upgrade Backup Manager</b></li></ul></li></ol> <p> 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 a report by clicking:</p> <ul style="list-style-type: none"><li>■ <b>Reports &gt; Status &gt; AV Defender Status</b></li></ul>   |

## Rebuild or Migrate your N-able N-central server

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

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

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

### The server is not working properly or starting successfully

1. Verify the version of your N-able N-central server. Technical Support can confirm the version of N-able N-central that last communicated with N-able if your server is not working properly or cannot be restarted.
2. Locate the last valid backup of your N-able N-central server. Your N-able 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 N-able N-central that automatically sent backups to an FTP server, or
  - c. snapshot of your N-able N-central server recorded by a virtualized host (Hyper-V or VMWare).

 **Possible incomplete restore from backup.**

Before recording a snapshot on an ESX or Hyper-V server, shut down the virtual machine upon which N-able N-central is installed.

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

You can re-install N-able 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-able N-central server.

- a. Login to the [N-able Resource Center](#).
- b. Click **Downloads**.
- c. Click the release you want to re-install.
- d. Select the checkbox to agree to having reviewed the known issues.
- e. Click **Enable Download**.
- f. Click the ISO for the release.

Here is an example of an ISO file available for download:

**File:** SolarWinds N-central 12.1 SP1 (12.1.1.191) ISO

**MD5:** 5bdcc8a6e4e9a11323400061e2ff1fc2

**Size:** 934 MB

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

### An upgrade has failed but you can still log in

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

1. Locate the last valid backup of your N-able N-central server. Your N-able 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 N-able N-central to automatically send backups to an FTP server from which they can be obtained.
  - c. You have a snapshot of your N-able 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.

 **Possible incomplete restore from backup.**

Before recording a snapshot on an ESX or Hyper-V server, shut down the virtual machine upon which N-able N-central is installed.

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

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

You can quickly re-install N-able 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.

- a. Login to the [N-able Resource Center](#).
- b. Click **Downloads**.
- c. Click the release you want to re-install.
- d. Select the checkbox to agree to having reviewed the known issues.
- e. Click **Enable Download**.
- f. Click the ISO for the release.

Here is an example of an ISO file available for download:

**File:** SolarWinds N-central 12.1 SP1 (12.1.1.191) ISO

**MD5:** 5bdcc8a6e4e9a11323400061e2ff1fc2

**Size:** 934 MB

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

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

## Migrating an existing N-able N-central server to another computer

1. Verify the version of your N-able N-central server by clicking **Help** > **Version Information**.
2. Locate the last valid backup of your N-able N-central server. Your N-able 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**.

 Backing up the N-able 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 N-able N-central to automatically send backups to an FTP server from which they can be obtained.
  - d. You have a snapshot of your N-able 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.

 **Possible incomplete restore from backup.**

Before recording a snapshot on an ESX or Hyper-V server, shut down the virtual machine upon which is installed.

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

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

For your convenience, you can quickly re-install N-able 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.

- a. Login to the [N-able Resource Center](#).
- b. Click **Downloads**.
- c. Click the release you want to re-install.
- d. Select the checkbox to agree to having reviewed the known issues.
- e. Click **Enable Download**.
- f. Click the ISO for the release.

Here is an example of an ISO file available for download:

**File:** SolarWinds N-central 12.1 SP1 (12.1.1.191) ISO

**MD5:** 5bdcc8a6e4e9a11323400061e2ff1fc2

**Size:** 934 MB

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

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



## Log in to N-able N-central for the first time

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

1. From the N-able N-central homepage, log in to `https://192.168.1.1`.
2. Login using the following credentials:
  - **Email:** `productadmin@solarwinds.com`
  - **Password:** `ManageAllTheThings0!`

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

| Category                     | Field Name   | Description  |
|------------------------------|--|--|
| <b>Security Warning</b>      | <b>Your N-able N-central server does not have a valid SSL certificate!</b> | <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 N-able N-central server, N-able recommends that you purchase a valid, signed SSL certificate and upload it to your N-able N-central server. SSL certificates can be obtained from security vendors such as RapidSSL, Verisign, and Entrust.</p>  |
| <b>Login Name</b>            | <b>Login Name</b>  | <p>The Login Name must be a valid email address. N-able 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 N-able N-central is available, and so that you can reset your password should you forget it.</p>  |
| <b>Change Login Password</b> | <b>New Password</b>  | <p>Enter a new password that will be used from now on to sign in to N-able 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"> <li>■ at least one number</li> <li>■ at least one uppercase character</li> <li>■ at least one lowercase character</li> <li>■ at least one special character</li> </ul> <p>You can not repeat any of your previous two passwords.</p> |
|                              | <b>Confirm New Password</b>  | <p>Re-enter the password.</p>  |
| <b>Company Information</b>   | <b>Company Name</b>  | <p>Name of your company.</p>   |
|                              | <b>Activation ID</b>   | <p>The Activation ID number is a code required to use N-able 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"> <li>a. Log in to the <a href="#">NRC</a>.</li> <li>b. Click <b>My Account</b>.</li> <li>c. Copy the <b>N-able N-central Activation ID</b> on the <b>My Account</b> screen.</li> </ol>  |

| 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 N-able 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> |

- Click **Save and Continue**.

In the **Getting Started** Wizard, review the instructional videos to learn more before proceeding. Until you activate N-able 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.

- Click **Add Customer/Site** to start the **Customer/Site Wizard**.
- Under **Company Information**, enter the **Customer/Site Name**.
- Select the **License Type** to use for the devices in this Customer/Site.
- 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.
- If **Default Credentials** are provided, select **Show Password** to reveal the password as it is typed.
- Click **Save and Continue**.
- 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 N-able 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 N-able N-central

Your N-able 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 N-able 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

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

### Support

Contact N-able to activate your N-able N-central server.

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

Once the N-able 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 [N-able Resource Center](#) under **My Account** or email [n-able-salesgroup@n-able.com](mailto:n-able-salesgroup@n-able.com).



## Contacting Technical Support

If you require assistance with configuring N-able N-central or have a technical issue, contact Technical Support using the N-able Partner Success Center at <https://success.n-able.com/> or using the [LiveChat](#) feature within N-able N-central.

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

- Case management access
- All current N-able products, service packs and hot fixes, along with the appropriate release notes and installation guides
- product documentation, including online help, 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 N-able N-central Support](#).



© 2021 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.

This document may not 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 prior written consent of N-able. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of N-able, its affiliates, and/or its respective licensors.

N-ABLE DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL N-ABLE, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF N-ABLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The N-ABLE, N-CENTRAL, and other N-able trademarks and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. and may be common law marks, are registered, or are pending registration with the U.S. Patent and Trademark Office and with other countries. All other trademarks mentioned herein are used for identification purposes only and are trademarks (and may be registered trademarks) of their respective companies.

### **About N-able**

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale. For more information, visit [www.n-able.com](http://www.n-able.com).