



# N-central

## Installation and Upgrade Guide

Version 2023.1

Last Updated: Monday, March 6, 2023



# Contents

<b>Contents</b> .....	<b>2</b>
<b>Install N-able N-central</b> .....	<b>4</b>
Prepare installation media .....	5
DVD Creation .....	5
USB Flash Drive .....	5
Linux and MacOS .....	5
Windows .....	5
Install N-able N-central on a physical server .....	6
What's next? .....	7
Install N-able N-central as a guest on an ESX/ESXi 6.0 or newer server .....	8
What's next? .....	9
Install N-able N-central as a guest on Windows Server 2016 or newer Hyper-V server .....	10
What's next? .....	11
Install N-able N-central on Microsoft Azure Managed Disks .....	12
Deployment .....	12
First run .....	13
VM Sizing .....	13
Notes .....	14
What's next? .....	14
Deployment script for Microsoft Azure - Managed Disks .....	15
Azure information .....	15
Azure Region .....	15
Resource naming prefix .....	15
VM size .....	15
Operating system disk size .....	15
Operating system disk storage type .....	15
Data disks sizes .....	16
Number of data disks .....	16
Data disks storage type .....	16
Boot diagnostics storage account .....	16
Boot diagnostics storage account type .....	16
Accelerated networking .....	17



IPv6 Support .....	17
N-central sizing on Azure Managed Disk deployment .....	17
Install N-able N-central on Amazon AWS EC2 .....	18
What's next? .....	18
<b>Upgrading N-able N-central .....</b>	<b>19</b>
Step 1: Back up the N-able N-central server .....	20
Step 2: Install the N-able N-central server upgrade .....	21
Step 3: Post-installation steps .....	22
Rebuild or Reinstall your N-able N-central server .....	24
The server is not working properly or starting successfully .....	24
An upgrade has failed but you can still log in .....	24
Install an existing N-able N-central server on another computer .....	25
<b>Log in to N-able N-central for the first time .....</b>	<b>27</b>
<b>Activating N-able N-central .....</b>	<b>30</b>
Trial .....	30
License limits and configuration settings .....	30
<b>Contacting Technical Support .....</b>	<b>31</b>



## Install N-able N-central

You can install N-able N-central on a physical server or virtual machine. N-able N-central supports the following platforms:

Physical servers:

- A Bare Metal Server with UEFI Firmware enabled (Preferred)
- A Bare Metal Server with Legacy BIOS enabled

Virtual machines:

- 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 2016 or newer Hyper-V (Generation 1)
- Amazon AWS Elastic Cloud Compute (EC2)
- Microsoft Azure Managed Disks

During installation on CentOS and Linux systems, the install performs hardware detection routines. This can cause error messages to appear for undetected devices, like floppy drives, 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 Managed Disks](#)
- [Install on Amazon AWS Elastic Cloud Compute \(EC2\)](#)
- [Activate N-able N-central](#)

## 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:

<b>HP Server</b>	
Cache Options	Set to 50% Read and 50% Write.
Disk RAID 1+0	Configure the RAID controller to use the default stripe size.
<b>Lenovo Server</b>	
Cache Options	Use the default settings.
Disk RAID 1+0	Configure the RAID controller to use the default stripe size.
<b>Dell Server</b>	
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.
<b>Intel Server</b>	
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 be 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
- Set up [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 installed 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) 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**.

**w** 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 be launched. 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
- Set up [Service Organizations](#), [Customers](#) and [Sites](#), and [configure users](#).

## Install N-able N-central as a guest on Windows Server 2016 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 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> . 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**.

 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 be launched. 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
- Set up [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. Only Azure Resource Manager with 1 or more Managed Disks is supported.

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.

You can download the Managed Disks Deployment script from the [N-able N-central release page](#). If you want to deploy a different version of N-central, replace the value for the `$ncentralVersion` setting. You can also edit other 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. See [Azure Managed Disks Deployment Script](#) for details.

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
```



After 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.

**i** If you try to log into 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 are completed.

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



Number of Devices	Recommended Azure Size	CPU Cores	Memory	OS Disk	Data Disks (Total)
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 opposed 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
- Set up [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. You can download the script from [here](#).

The deployment 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

TheN-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://simpledns.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 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, 443, 8443, 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
- Set up [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 Reinstall 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 want to create a Snapshot of the virtual machine. 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 been 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 2023.1 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
a. Select <b>Install upgrade from local repository</b> . b. Select an upgrade version from the list of available options.	a. Select <b>Install upgrade remotely</b> . b. Click <b>Browse</b> and navigate to the .nsp file in the <a href="#">N-able Resource Center</a> .

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 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 installation.

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 N-able 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-2023.1.0.xxx-b1_0_0xxx</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 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 #00a0e3; padding: 5px;"> <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>
	<div style="border: 1px solid #00a0e3; padding: 5px;"> <p><b>i</b> 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> </div>

	Check items as they are completed
	<p>Upgrade your monitoring software automatically for specific SOs, Customers or Sites:</p> <p>Upgrade your monitoring software automatically for specific Customers or Sites:</p> <p>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> <div style="border: 1px solid #0070C0; padding: 5px; margin-top: 10px;"> <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> </div>
	<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 Reinstall your N-able N-central server

There may be circumstances when you want to rebuild or reinstall 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 installing an existing N-able N-central server on another computer.

The following scenarios describe the best way to rebuild or reinstall 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 create 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, along with the associated checksum file,
  - 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 Partners Success 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:** N-able N-central 2021.3 (2021.3.0.83) 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 create 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 your most recent backup before 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.

**i** 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. Reinstall 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:** N-able N-central 2021.3 (2021.3.0.83) ISO

**MD5:** 5bdcc8a6e4e9a11323400061e2ff1fc2

**Size:** 934 MB

**i** 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.

### Install an existing N-able N-central server on 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 create backups but these will be saved to the same local hard drive as the server software itself which may make retrieval more difficult. Some options that may be used to retrieve a backup include:
  - a. Create a new backup in order to minimize data loss.
    - a. Click **Administration > System Backup and Restore > Configure Backups**.
    - b. Click **Save and Run Backup**.

**i** Backing up the 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.

**i** 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:** N-able N-central 2021.3 (2021.3.0.83) ISO

**MD5:** 5bdcc8a6e4e9a11323400061e2ff1fc2

**Size:** 934 MB

**i** 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. Connect to the N-able N-central Web UI on port 8443. For example:  
`https://192.168.1.1:8443/login.`
2. Login using the following credentials:
  - **Email:** `productadmin@n-able.com`
  - **Password:** `ManageAllTheThings0!`

3. The first time you log in, you need 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>	N-central requires a valid TLS Certificate from a publicly trusted root CA. It can also be configured to use a certificate issued by a private CA service, like Active Directory Certificate Service, by uploading the Root CA certificate to the N-central 'CA Certificate' trust store before uploading your N-central TLS certificate.  You can obtain TLS certificates from security vendors such as RapidSSL, Verisign, and Entrust.
<b>Login Name</b>	<b>Login Name</b>	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.
<b>Change Login Password</b>	<b>New Password</b>	Enter a new password that will be used from now on to sign into N-able N-central.  The password must be at least eight (8) characters in length and contain the following: <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> You cannot repeat any of your previous two passwords.
	<b>Confirm New Password</b>	Re-enter the password.
<b>Company Information</b>	<b>Company Name</b>	Name of your company.
	<b>Activation ID</b>	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.  If your Activation ID number is unavailable: <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>

4. 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.

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

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

## Trial

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

## License limits 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. See [Port access requirements](#) for details.

## Support

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

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

Once the 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 Partner Success Manager. You can find their contact information in the [Partner Success Center](#): Click the **Need Assistance?** button. In the **Partner Success Manager** area, click **View Info**. Use the contact information to contact your Partner Success Manager or email [mspsales@n-able.com](mailto:mspsales@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/> and clicking the **Need Assistance** button. You can also call at 1-855-679-0817, or use the [LiveChat](#) feature within N-able N-central.

You can submit a case through the Partner Success Center directly [here](#). You will need to be logged in to the Partner Success Center.

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](#).



© 2023 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).