Citrix SD-WAN Center 11.4

Contents

System requirements and installation 4

Install and configure Citrix SD-WAN Center on ESXi Server 8

Install and configure Citrix SD-WAN Center on XenServer 20

Install and configure Citrix SD-WAN Center on Microsoft Hyper-V 27

Citrix SD-WAN Center on Azure Marketplace using solution template 35

Citrix SD-WAN Center on AWS in VM importable image format 41

Two factor authentication 47

Primary authentication 48

Secondary authentication 52

Single-region network deployment 56

Multi-region network deployment 58

Configuration 63

Configure the management interface settings 63

Install the SD-WAN Center SSL certificate 64

Install the Citrix SD-WAN SSL certificate 65

Switch the active storage to new data storage 67

Deploy Citrix SD-WAN appliance 68

Configure Citrix SD-WAN appliances 68

Configuration Editor 69

Change Management Wizard 71

Appliance settings 73

Remote LTE site management 75

Citrix SD-WAN Center as a license server 80

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Deploy Citrix SD-WAN on Azure from Citrix SD-WAN Center **83**

Zero Touch Deployment **91**

On-prem zero touch **113**

AWS **113**

Azure **124**

Proxy Server Settings for zero touch deployment **143**

Palo Alto Network Integration **145**

Microsoft Azure Virtual WAN **151**

Using Citrix SD-WAN to connect to Microsoft Azure Virtual WAN **163**

Cloud Direct Service **195**

Integrate Citrix SD-WAN and Zscaler using Citrix SD-WAN Center **218**

Monitoring **230**

Dashboard **230**

Diagnostic packages **256**

Events **258**

Event notifications **261**

Memory dumps **266**

Log files **268**

Polling interval **269**

Statistics **269**

System information **273**

Reporting **274**

Application report **277**

Application QoE report **278**

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Bandwidth report **280**

Class report **281**

Ethernet interface report **283**

Event report **284**

GRE tunnel report **287**

HDX report **288**

IPsec tunnel report **292**

Link performance report **294**

MOS for applications **297**

MPLS queues report **299**

Administration **300**

Configure date and time **301**

HTTPS certificates **302**

Import MCN configuration **305**

Manage database **308**

Manage views **311**

Software upgrade **312**

Timeline controls **313**

User accounts **315**

Diagnostics **320**

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

System requirements and installation

November 8, 2021

Before you install Citrix SD-WAN Center on a VM, make sure that you must understand the hardware and software requirements and have met the prerequisites.

> **Note**
>
> The system requirements are common for both single-region network and multi-region network.

Hardware requirements

Citrix SD-WAN Center has the following hardware requirements.

Processor

- 4 Core, 3 GHz (or equivalent) processor or better for a server managing up to 64 sites.
- 8 Core, 3 GHz (or equivalent) processor or better for a server managing up to 128 sites.
- 16 Core, 3 GHz (or equivalent) processor or better for a server managing up to 256 sites.
- 32 core, 3 GHz (or equivalent) processor or better for a server managing up to 550 sites.

Memory

- A minimum of 8GB of RAM is strongly recommended for a VM managing up to 64 sites.
- A minimum of 16GB of RAM is strongly recommended for a VM managing up to 128 sites.
- A minimum of 32GB of RAM is strongly recommended for a VM managing up to 256 sites.
- A minimum of 32GB of RAM is strongly recommended for a VM managing up to 550 sites.

Disk space requirements

The following table provides some guidelines for determining the disk space requirements for Citrix SD-WAN Center data storage. Use direct access storage with SSD having 5000 to 10000 IOPS.

Estimated disk space requirement

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

# Client Sites	Average # WAN Links per Site	Average # Intranet/Internet Services per Site	Average # Virtual Paths per Site	Database Size (TB) for 1 Year
32	2	2	2	1.2T
32	4	4	4	1.8T
32	8	8	8	5.3T
64	2	2	2	1.5T
64	4	4	4	2.6T
64	8	8	8	9.6T
96	2	2	2	1.8T
96	4	4	4	3.3T
96	8	8	8	14.0T
128	2	2	2	2.0T
128	4	4	4	4.1T
128	8	8	8	18.0T
192	2	2	2	2.6T
192	4	4	4	5.6T
192	8	8	8	27.0T
256	2	2	2	3.0T
256	4	4	4	7.2T
256	8	8	8	35.0T
550	2	2	2	15.9T
550	4	4	4	41.9T
550	8	8	8	195.6T

Network bandwidth

The following table provides some guidelines for determining network bandwidth requirements for the Citrix SD-WAN Center VM.

Estimated network bandwidth requirements

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

# Client Sites	Average # WAN Links	Average # Virtual Paths per Site	Total VWAN Data per 5-min Poll (MB)	Bandwidth Rate to Configure per 5-min Poll (Kbps)
32	2	2	1.2	Default 1000
32	4	4	3.6	Default 1000
32	8	8	20.0	Default 1000
64	2	2	2.3	Default 1000
64	4	4	7.2	Default 1000
64	8	8	40.0	2000
96	2	2	3.5	Default 1000
96	4	4	10.8	Default 1000
96	8	8	60.0	3000
128	2	2	4.6	Default 1000
128	4	4	14.4	Default 1000
128	8	8	80.0	4000
192	2	2	6.9	Default 1000
192	4	4	21.6	2000
192	8	8	120.0	6000
256	2	2	9.2	Default 1000
256	4	4	28.8	2000
256	8	8	160	10000
550	2	2	34.0	2000
550	4	4	89.3	6000
550	8	8	415.7	24000

Software

Citrix SD-WAN Center VPX can be configured on the following platforms :

Hypervisor

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- VMware ESXi server, version 6.5.
- Citrix XenServer 6.5 or higher.
- Microsoft Hyper-V 2012 R2 or higher.

Cloud Platform

- Microsoft Azure
- Amazon Web Services

Browsers must have cookies enabled, and JavaScript installed and enabled.

The Citrix SD-WAN Center Web Interface is supported on the following browsers:

- Google Chrome 40.0+
- Microsoft Internet Explorer 11+
- Mozilla Firefox 41.0+

Prerequisites

Following are the prerequisites for installing and deploying Citrix SD-WAN Center:

- The SD-WAN Master Control Node (MCN) and existing client nodes must be upgraded to the latest Citrix SD-WAN software version.
- It is recommended to have a DHCP server available and configured in the SD-WAN network.
- You must have the Citrix SD-WAN Center installation files.

> **Note**
>
> You cannot customize or install any third party software on Citrix SD-WAN Center. However, you can modify the vCPU, memory and storage settings.

Download Citrix SD-WAN Center software

Download the Citrix SD-WAN Center Management Console software installation files, for the required release and platform, from the Downloads page.

The Citrix SD-WAN Center installation files use the following naming convention:

ctx-sdwc-version_number-platform.extension

- *version_number* is the Citrix SD-WAN Center release version number.
- *platform* is the platform type, hypervisor, or cloud platform name.
- *extension* is the installation file extension.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Platform	File extension
Citrix XenServer	.xva
VMware ESXi	-vmware.ova
Microsoft Hyper-V	-hyperv.vhd.zip
Microsoft Azure	-azure.vhd.zip

Gather the Citrix SD-WAN Center installation and configuration information

This section provides a checklist of the information you will need to complete your Citrix SD-WAN Center installation and deployment.

Gather or determine the following information:

- The IP address of the ESXi server, XenServer, Hyper-V server, or Azure that hosts the Citrix SD-WAN Center Virtual Machine (VM).
- A unique name to assign to the Citrix SD-WAN Center VM.
- The amount of memory to allocate for the Citrix SD-WAN Center VM.
- The amount of disk capacity to allocate for the virtual disk for the VM.
- The Gateway IP Address the Citrix SD-WAN Center will use to communicate with external networks.
- The subnet mask for the network in which the Citrix SD-WAN Center VM will be installed.

Install and configure Citrix SD-WAN Center on ESXi Server

March 12, 2021

Install the VMware VSphere client

Following are the basic instructions for downloading and installing the VMware vSphere client that you will use to create and deploy the Citrix SD-WAN Center Virtual Machine. For more information, see VMware vSphere Client documentation.

To download and install the VMware vSphere Client, do the following:

1. Open a browser and navigate to the ESXi server that hosts your vSphere Client and Citrix SD-WAN Center Virtual Machine (VM) instance.

   The VMware ESXi Welcome page appears.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

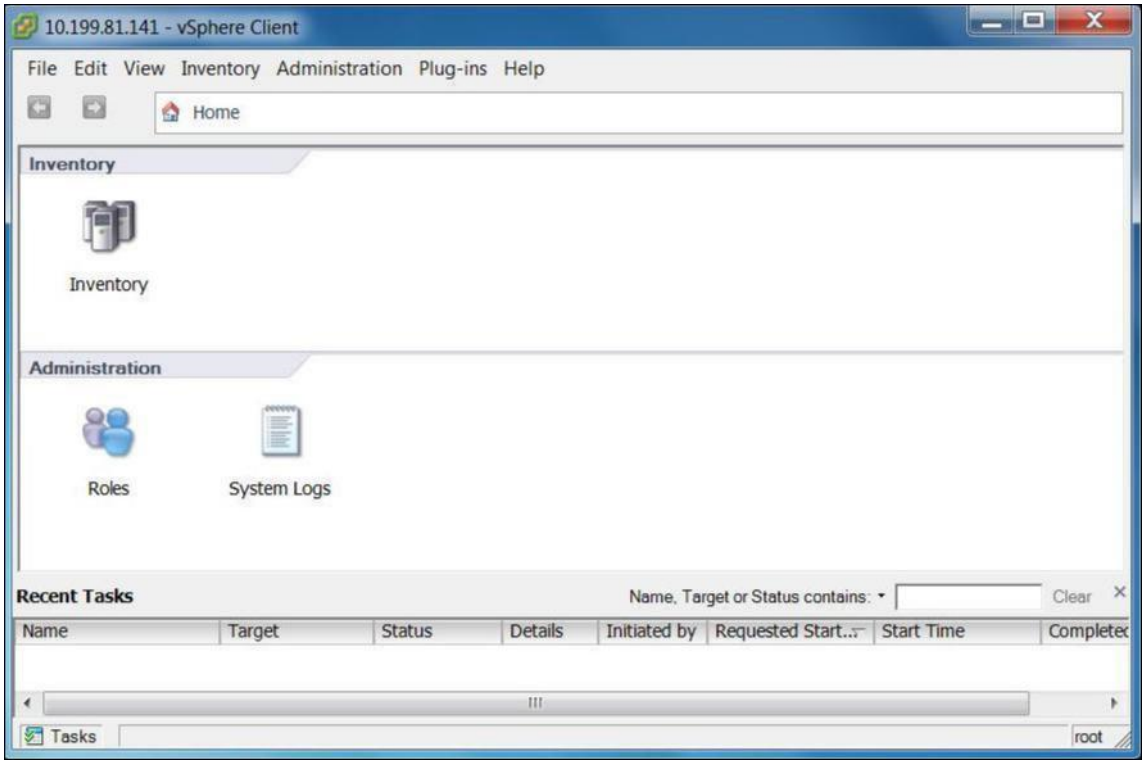
2. Click the **Download vSphere Client** link to download the vSphere Client installation file.
3. Install the vSphere Client.

   Run the vSphere Client installer file that you downloaded, and accept each of the default options when prompted.
4. After the installation completes, start the vSphere Client program.

   The VMware vSphere Client login page appears, prompting you for the ESXi server login credentials.
5. Enter the ESXi server login credentials:

   - **IP address / Name**: Enter the IP Address or Fully Qualified Domain Name (FQDN) for the ESXi server that hosts your Citrix SD-WAN Center VM instance.
   - **User name**: Enter the server administrator account name. The default is root.
   - **Password**: Enter the password associated with this administrator account.
6. Click **Login**.

   The vSphere Client main page appears.



Creating the Citrix SD-WAN Center VM using OVF template

After installing the VMware VSphere client, create the Citrix SD-WAN Center virtual machine.

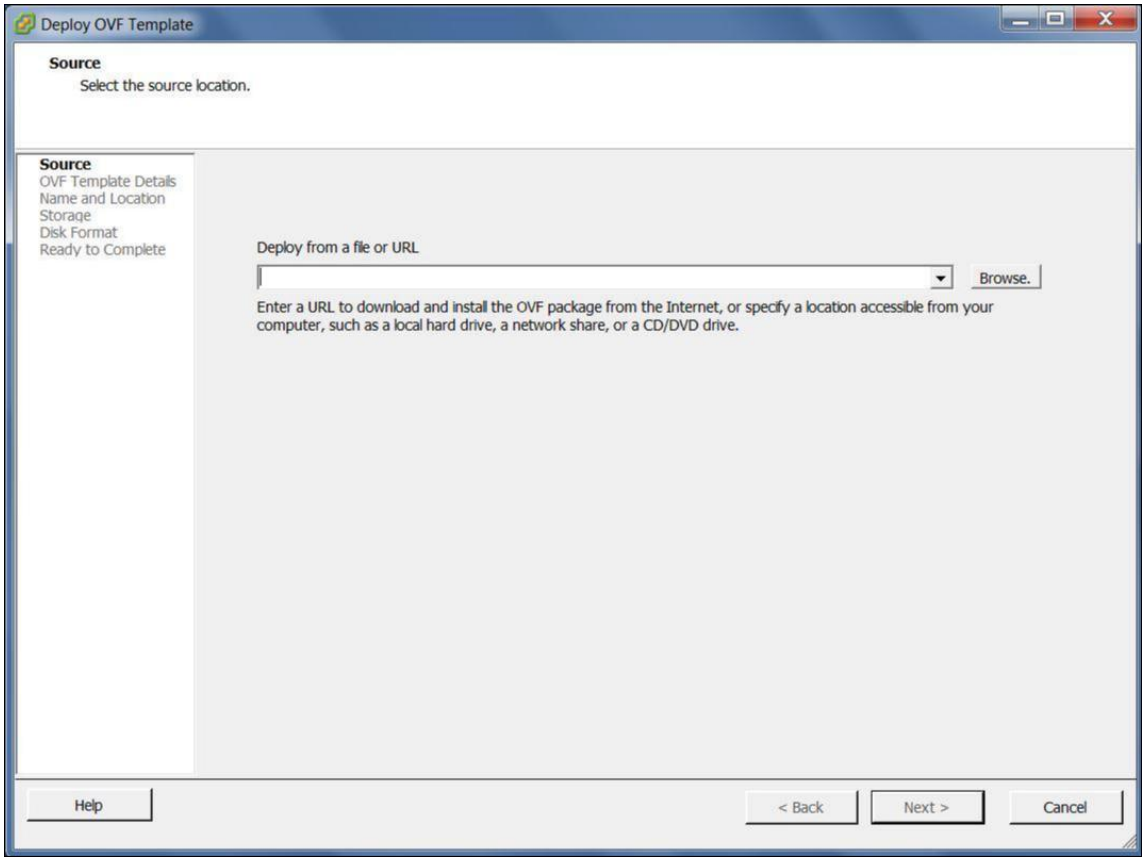
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

1. If you have not already done so, download the Citrix SD-WAN Center OVF template file (. ova file) to the local PC.

   For more information, see System requirements and installation.

2. In the vSphere Client, click **File**, and then select **Deploy OVF Template** from the drop-down menu.

   The **Deploy OVF Template** wizard appears.



3. Click **Browse** and select the Citrix SD-WAN Center OVF template (.ova file) that you want to install.
4. Click **Next**.

   The ova file is imported and the OVF Template Details page appears.

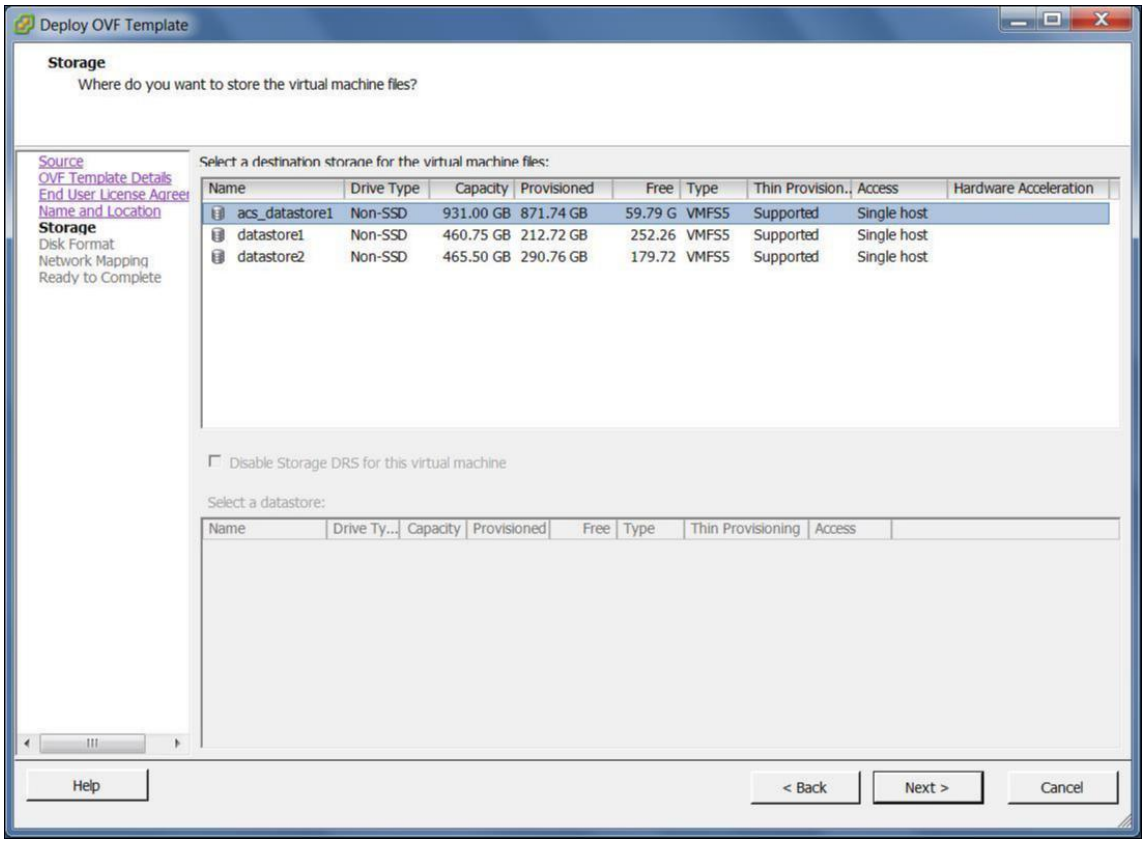
5. Click **Next**.
6. On the End User License Agreement page, click **Accept**, and then click **Next**.
7. On the Name and Location page, enter a unique name for the new VM (or accept the default value).

   The name must be unique within the current **Inventory** folder, and can be up to 80 characters in length.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

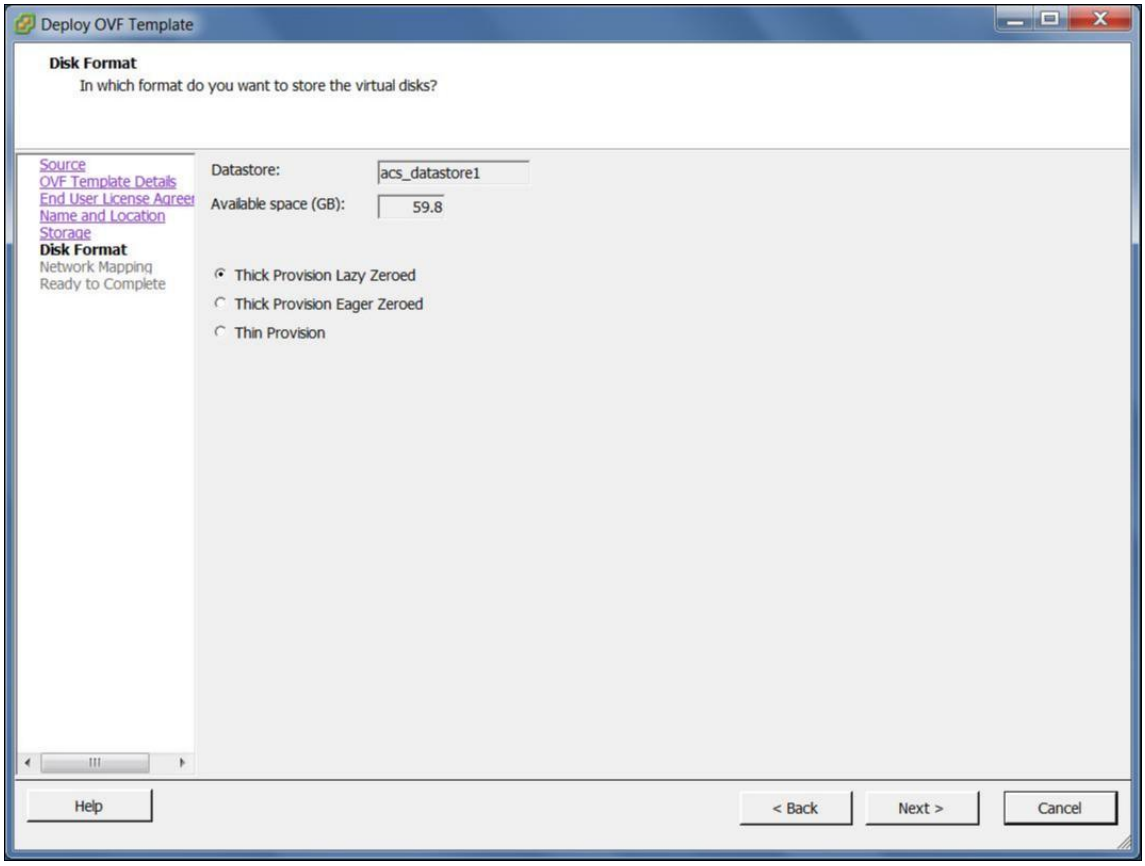
8. Click **Next**.

   The Storage page appears.



9. For now, accept the default storage resource by clicking **Next**. You can also configure the datastore. For more information see Add and configure the Datastore on ESXi server.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



10. On the Disk Format page, accept the default settings, and click **Next**.
11. On the Network Mapping page, accept the default (VM Network) and click **Next**.
12. On the Ready to Complete page, click **Finish** to create the VM.

    > **Note**:
    >
    > Decompressing the disk image onto the server can take several minutes.

13. Click **Close**.

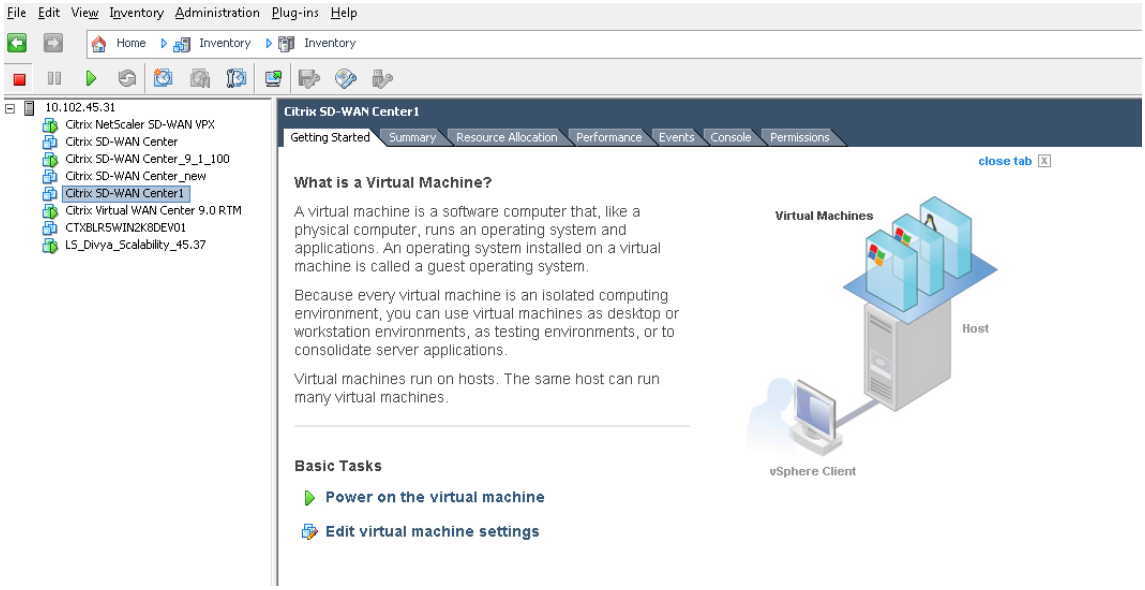
View and record the management IP address on ESXi server

The management IP address is the IP address of the SD-WAN Center VM, use this IP address to log into the Citrix SD-WAN Center Web UI.

To display the management IP address, do the following:

1. On the vSphere client Inventory page, select the new Citrix SD-WAN Center VM in the **Inventory** tree (left pane).

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

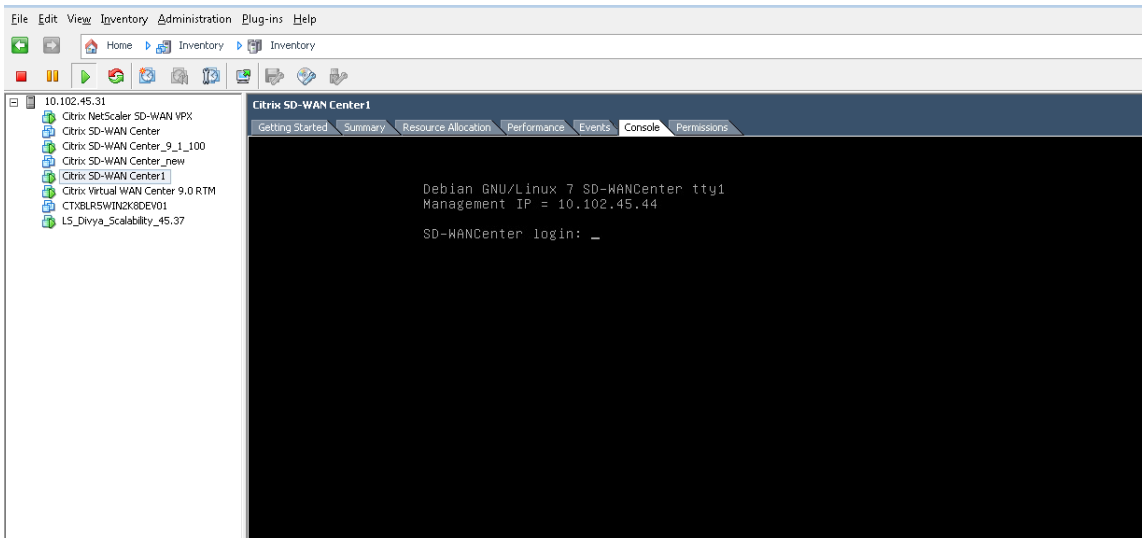


2. On the Citrix SD-WAN Center page, under Basic Tasks, click **Power on the Virtual Machine**.
3. Select the **Console** tab, and then click anywhere inside the console area to enter console mode.

   This turns control of your mouse cursor over to the VM console.

   > **Note**
   >
   > To release console control of your cursor, press the <Ctrl> and <Alt> keys simultaneously.

4. Press **Enter** to display the console login prompt.



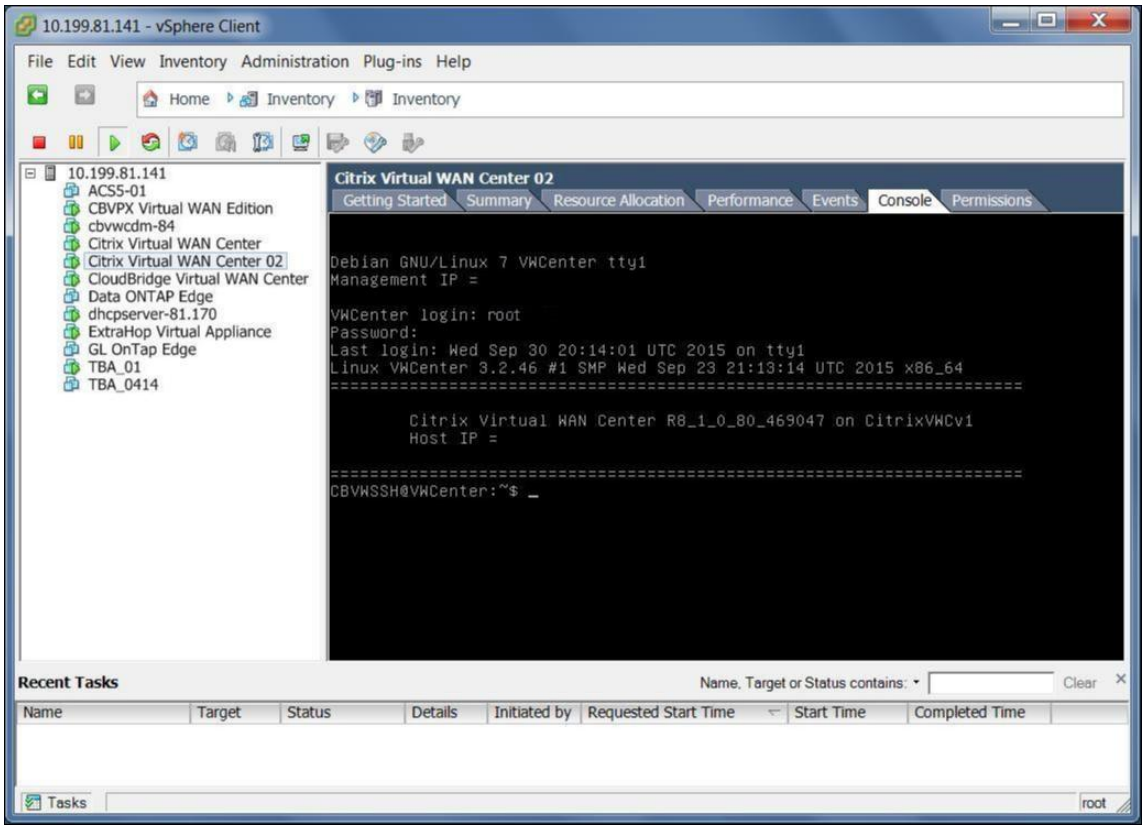
5. Log into the VM console.

   The default login credentials for the new Citrix SD-WAN Center VM are as follows:

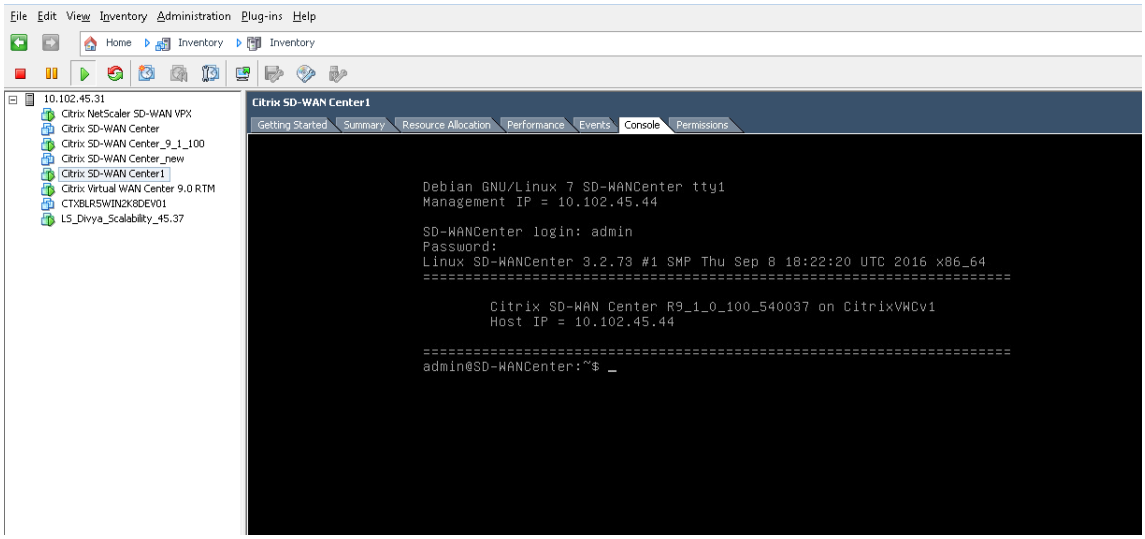
   - Login: admin

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- Password: password



6. Record the Citrix SD-WAN Center VM's management IP address, which is shown as the Host IP address in a welcome message that appears when you log on.



> **Note**
>
> The DHCP server must be present and available in the SD-WAN network, or this step cannot be

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> completed.

If the DHCP server is not configured in the SD-WAN network, you have to manually enter a static IP address.

To configure a static IP address as the management IP address:

1. When the VM is started, click the **Console** tab.
2. Log into the VM. The default login credentials for the new Citrix SD-WAN Center VM are as follows:

   Login: admin

   Password: password
3. In the console enter the CLI command **management_ip**.
4. Enter the command **set interface <ipaddress> <subnetmask> <gateway>**, to configure management IP.

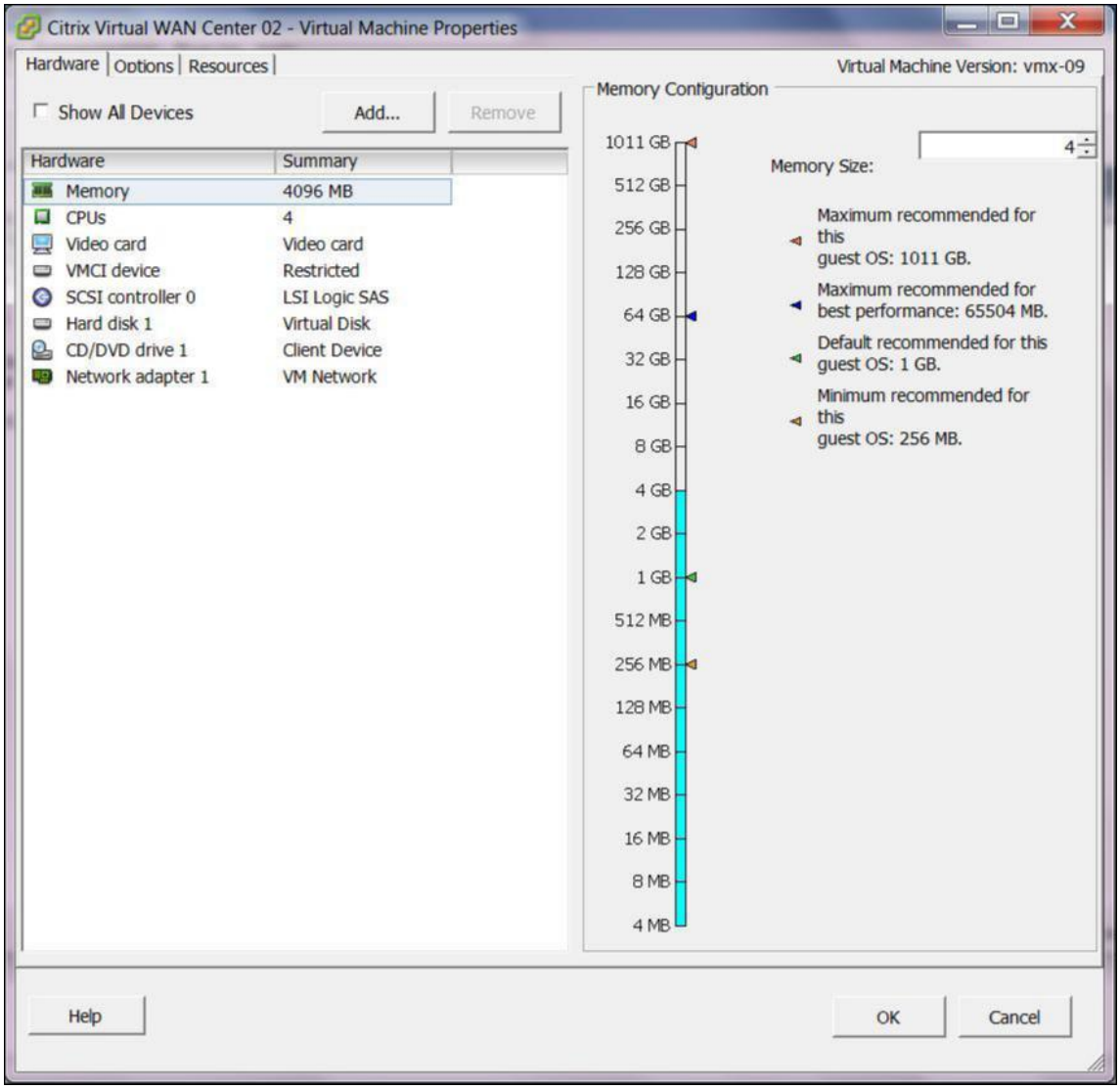
Add and Configure the Datastore on an ESXi server

You can add and configure datastore to store statistics from Citrix SD-WAN Center.

To add and configure the datastore:

1. In the vSphere client, click the **Inventory** icon to open the Inventory page.
2. Expand the **Inventory** tree branch for the Citrix SD-WAN Center VM host server.
3. In the left pane, click **+** next to the IP Address for the server hosting the Citrix SD-WAN Center VM you created.
4. Open the new Citrix SD-WAN Center VM for editing.
5. In the **Inventory** tree, right-click on the name of the Citrix SD-WAN Center VM you created and select **Edit Setting** from the drop-down menu.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

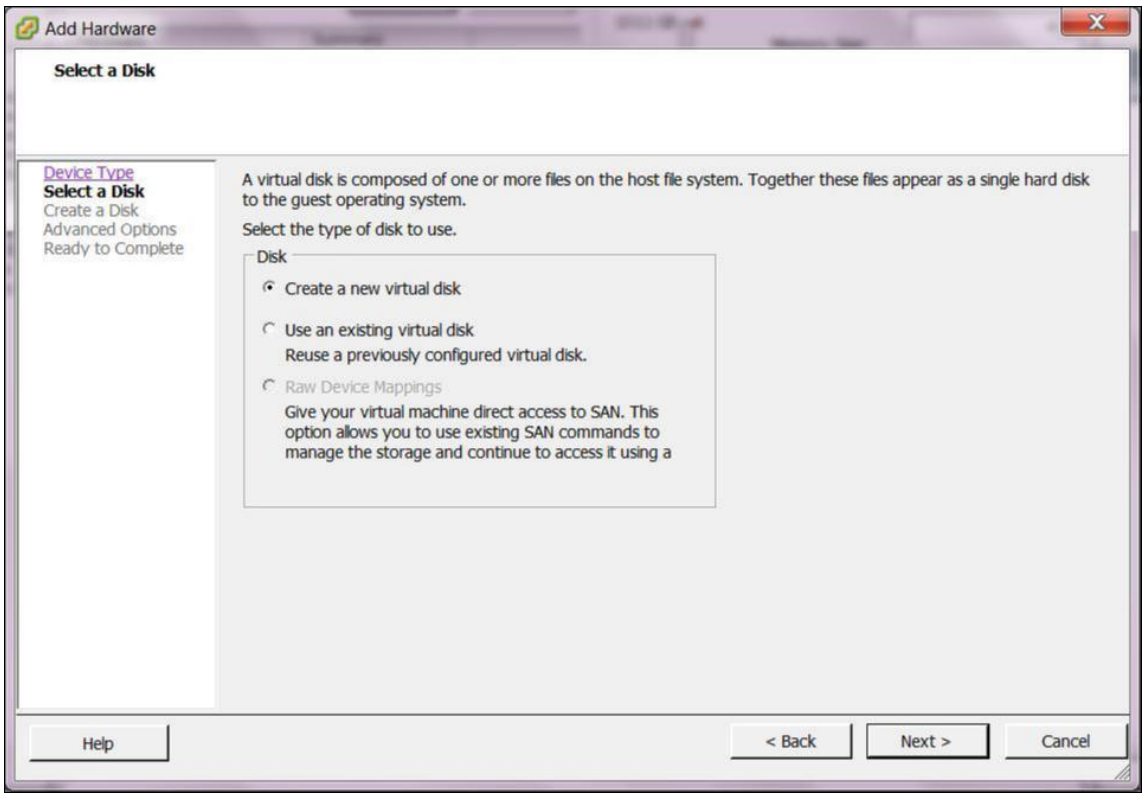


6. In the Memory Size field, enter the amount of memory to allocate for to this VM.

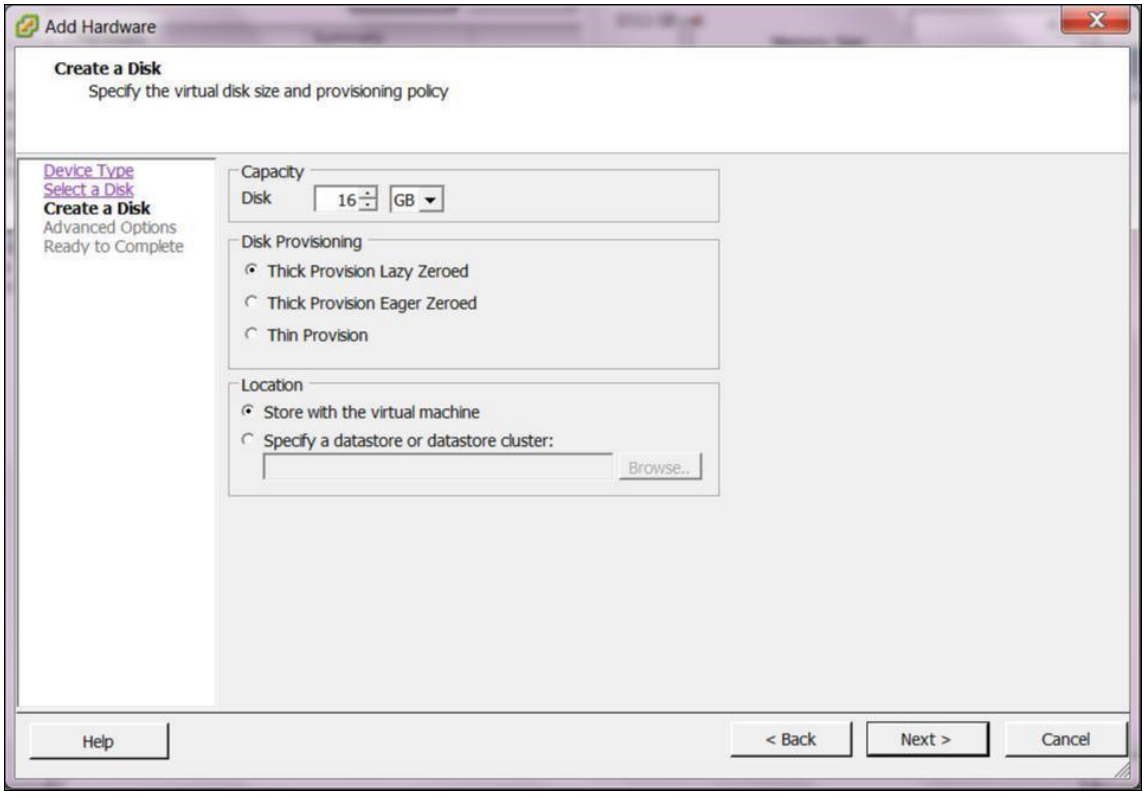
   For more information, see Memory Requirements.

7. Click **Add**.
8. On the Device Type page of the Add Hardware wizard, select **Hard Disk** and then click **Next**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



9. On the Select a Disk page, select **Create a new virtual disk** and click **Next**.

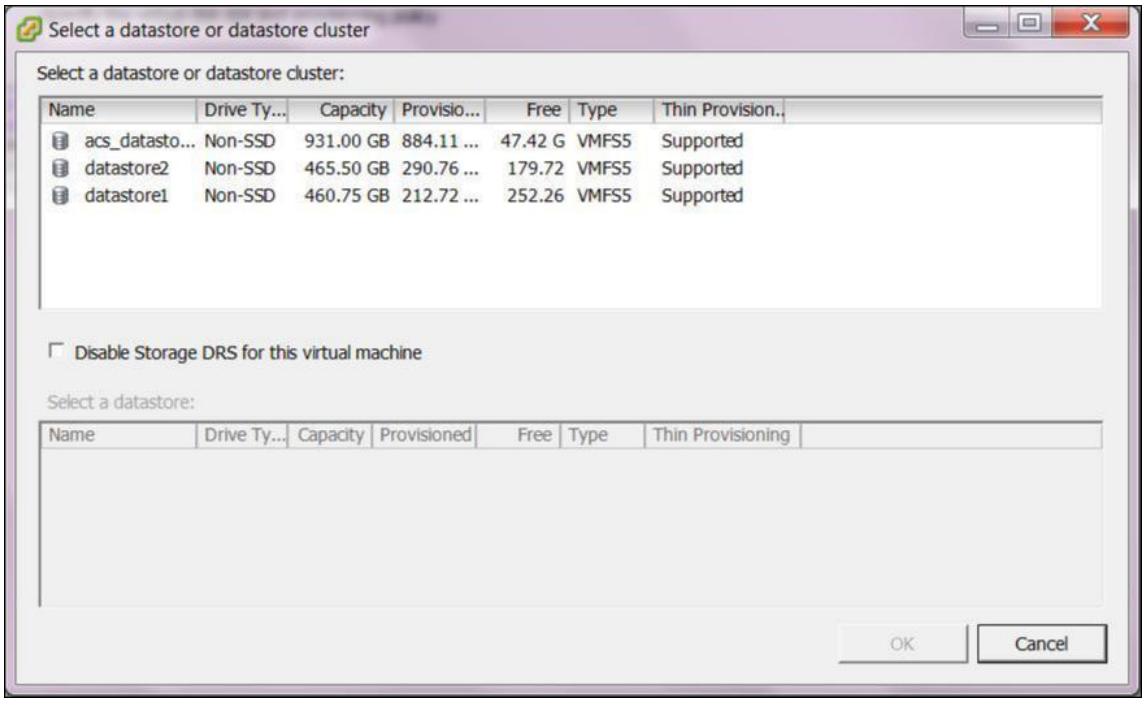


10. On the Create a Disk page, in the **Capacity** section, select the disk capacity for the new virtual

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

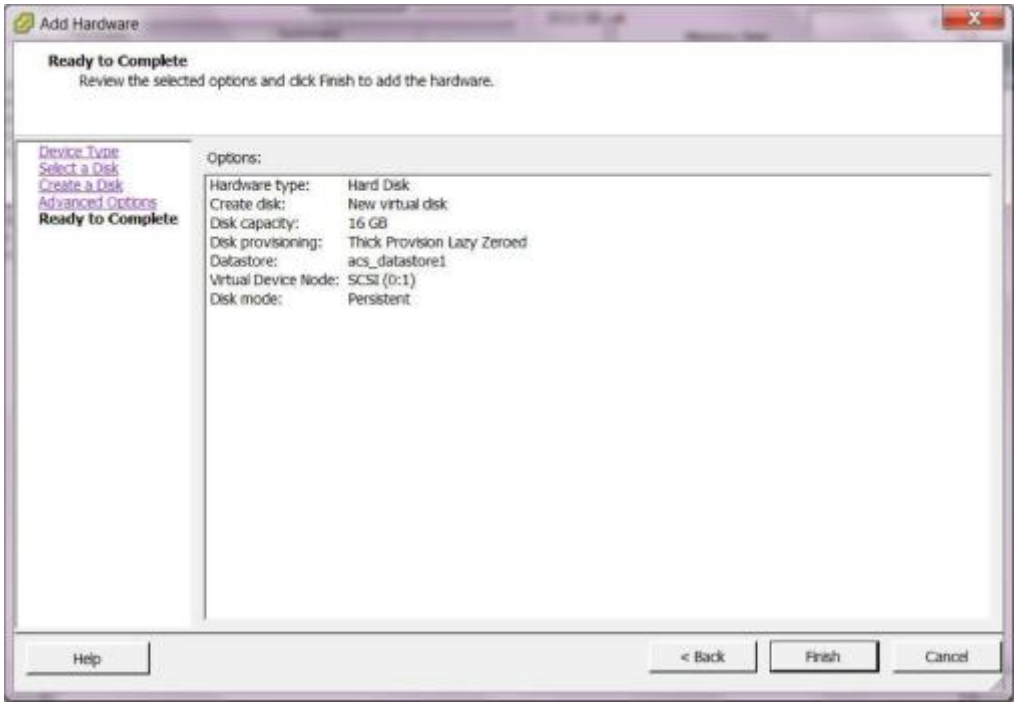
disk.

11. In the Disk Provisioning section, select **Thick Provision Lazy Zeroed** (the default).
12. In the Location section, select **Specify a datastore or datastore cluster**.
13. Click **Browse**.



14. Select a datastore with sufficient available space, and click **OK**.
15. Click **Next**.
16. On the Advanced Options page, accept the **Advanced Options** default settings and click **Next**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

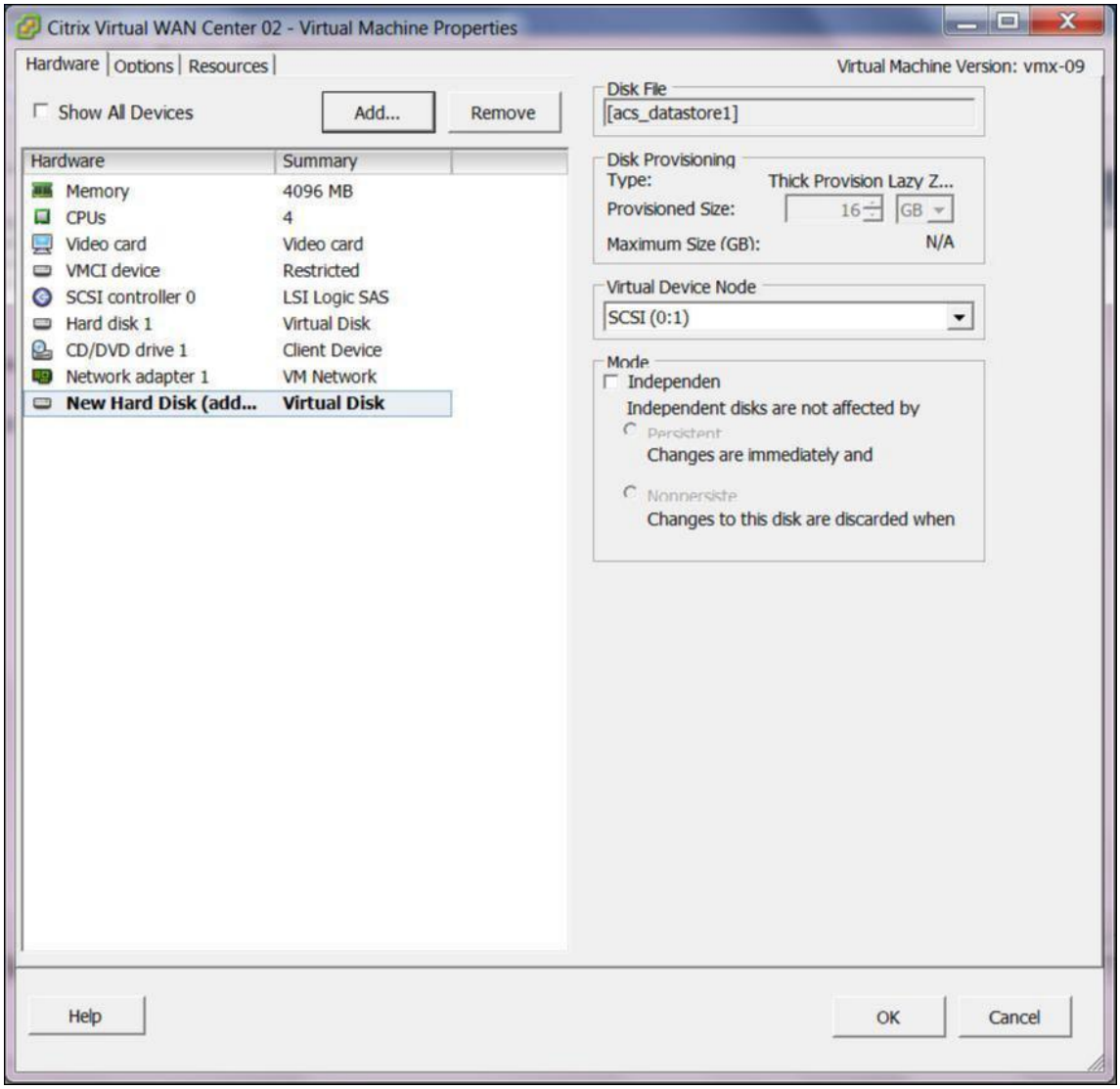


17. Click **Finish**.

    This adds the new virtual disk, dismisses the Add Hardware wizard, and returns you to the Virtual Machine Properties page.

18. Click **OK**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Install and configure Citrix SD-WAN Center on XenServer

March 12, 2021

Before installing the Citrix SD-WAN Center virtual machine on a XenServer server, gather the necessary information as described in Gathering the Citrix SD-WAN Center Installation and Configuration Information.

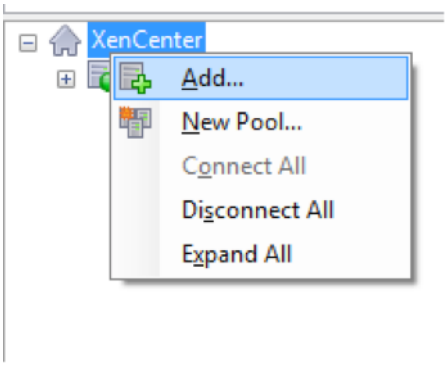
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Install the XenServer server

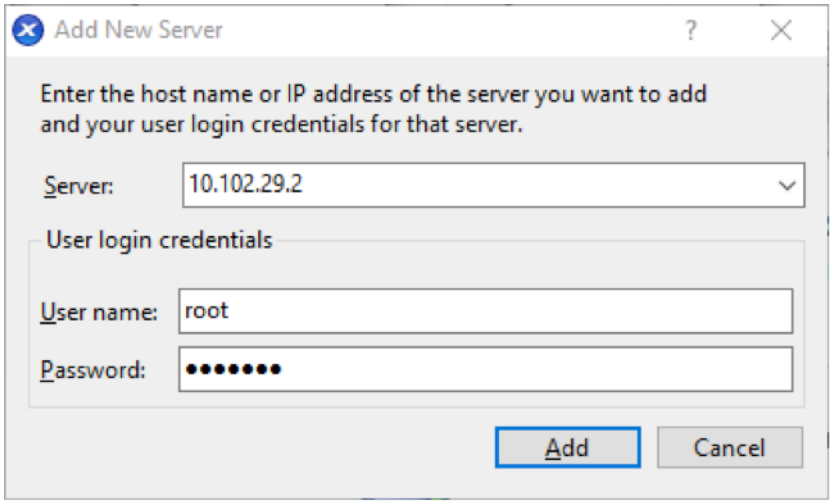
To install the Citrix XenServer server on which you will deploy the Citrix SD-WAN Center virtual machine, you must have XenCenter installed on your computer. If you have not already done so, download and install XenCenter.

To install a XenServer server:

1. Open the XenCenter application on your computer.
2. In the left tree pane, right-click on **XenCenter** and select **Add**.



3. In the **Add New Server** window, enter the required information in the following fields:
   - **Server**: Enter the IP Address or Fully Qualified Domain Name (FQDN) of the XenServer server that will host your Citrix SD-WAN Center VM instance.
   - **User name**: Enter the server administrator account name. The default is root.
   - **Password**: Enter the password associated with this administrator account.



4. Click **Add**.

   The new server's IP address appears in the left pane.

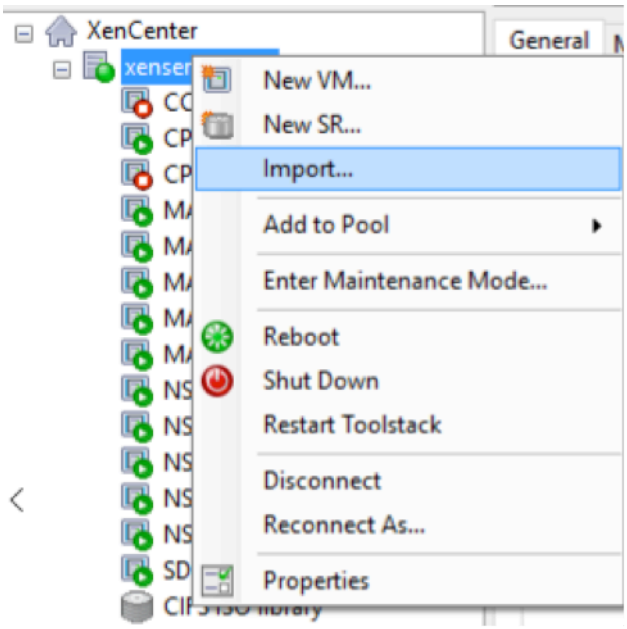
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Create the Citrix SD-WAN Center VM using the XVA file

The Citrix SD-WAN Center virtual machine software is distributed as an XVA file. If you have not already done so, download the .xva file. For more information, see System requirements and installation.

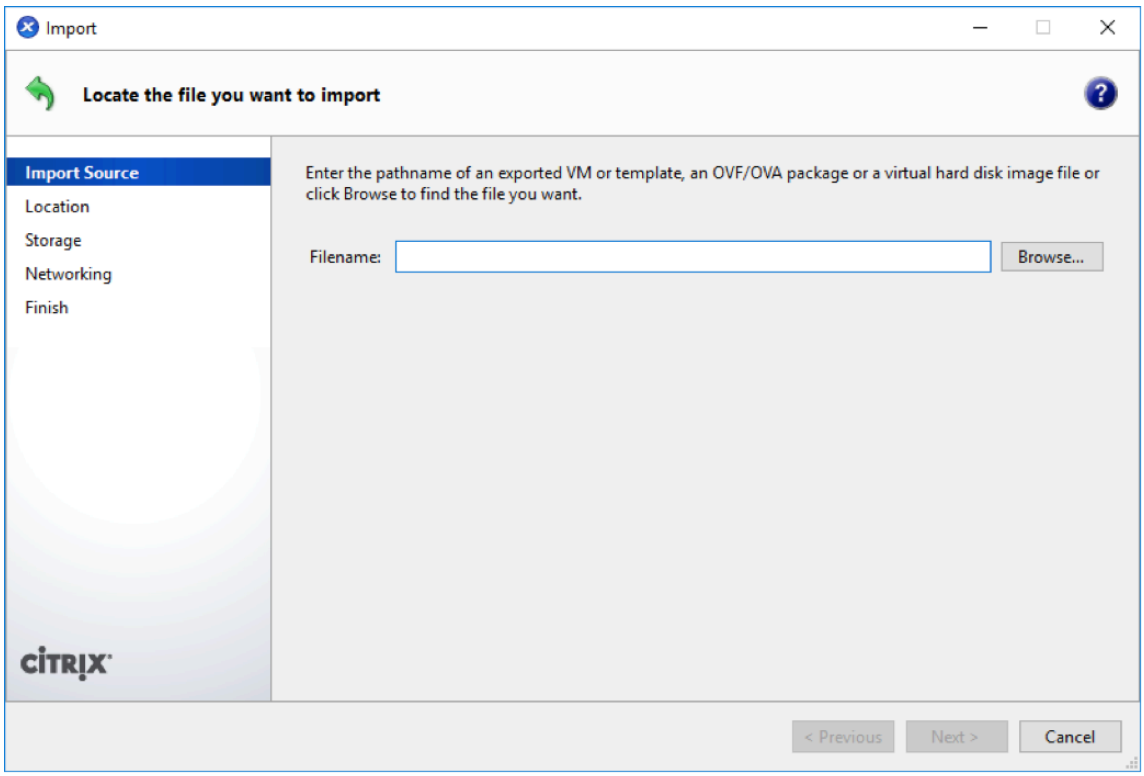
To create the Citrix SD-WAN Center VM:

1. In XenCenter, right-click **XenServer** and click **Import**.

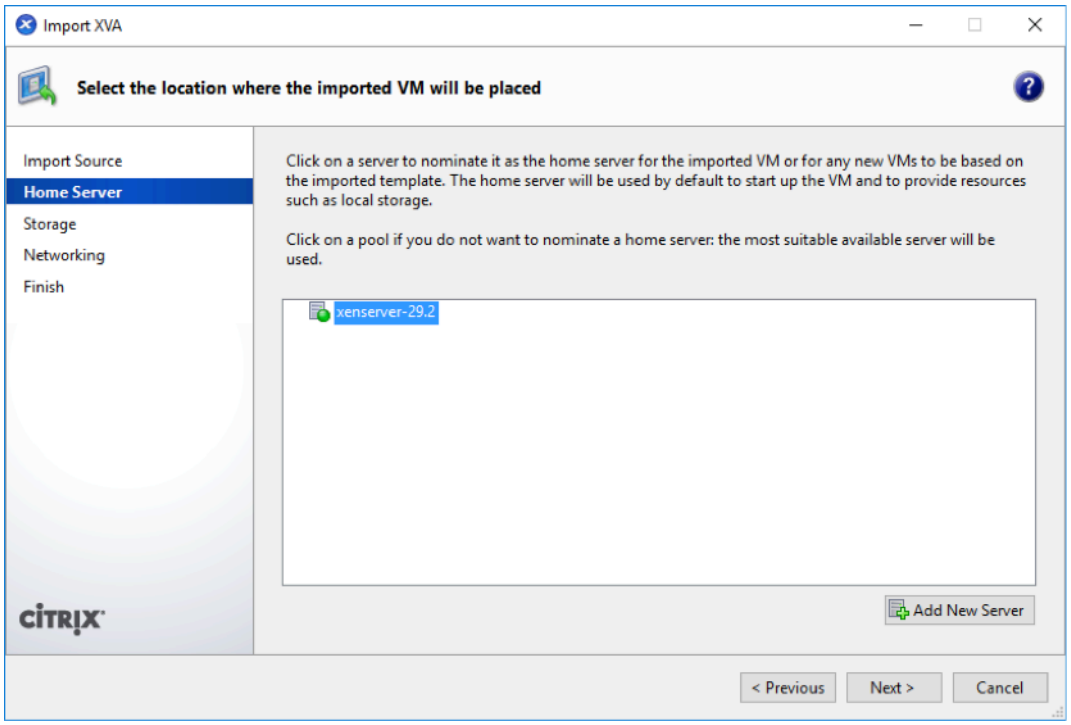


2. Browse to the downloaded .xva file, select it, and click **Next**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



3. Select a previously created XenServer server as the location to which to import the VM, and click **Next**.

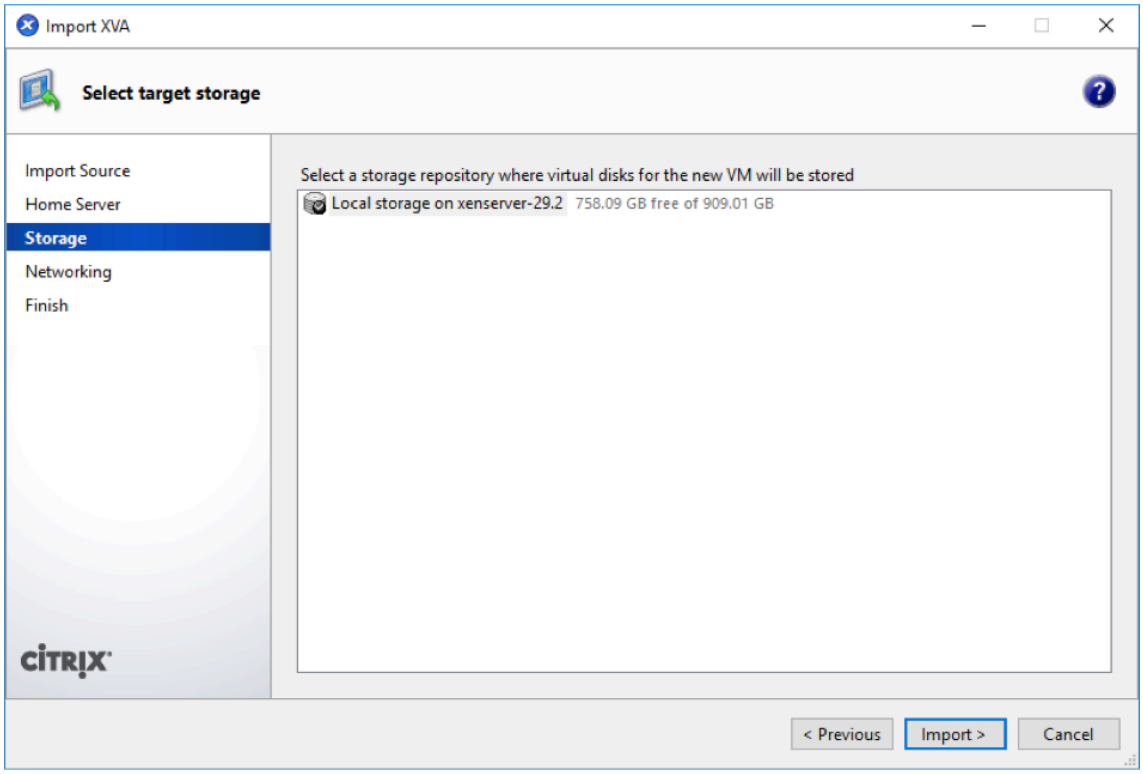


4. Select a storage repository where the virtual disk for the new VM will be stored, and click **Import.**

   For now, you can accept the default storage resource. Or you can configure the datastore. For

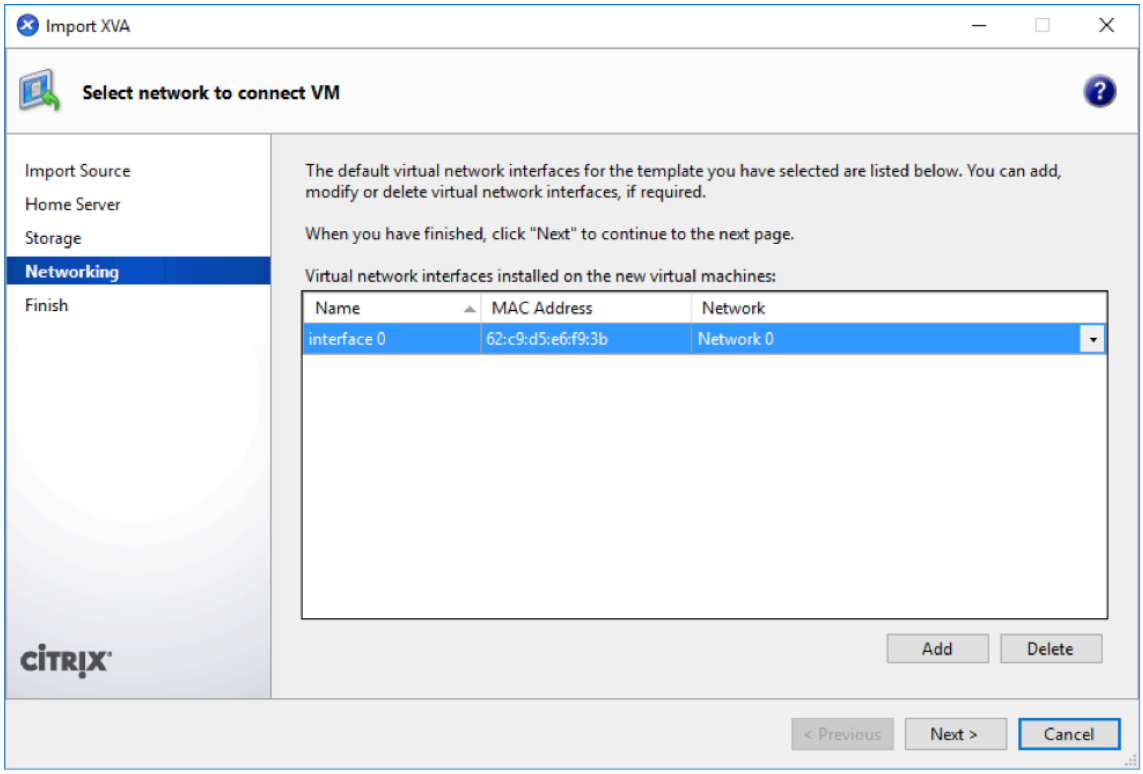
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

more information see **Add and configure the Datastore on XenServer** section.



The imported Citrix SD-WAN Center VM appears in the left pane.

5. Select a network to which to connect the VM, and click **Next**.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

6. Click **Finish**.

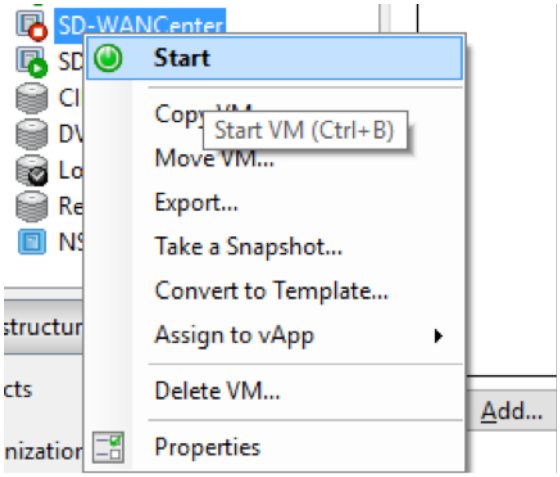
View and record the management IP address on XenServer

The management IP address is the IP address of the Citrix SD-WAN Center VM, use this IP address to log into the Citrix SD-WAN Center Web UI.

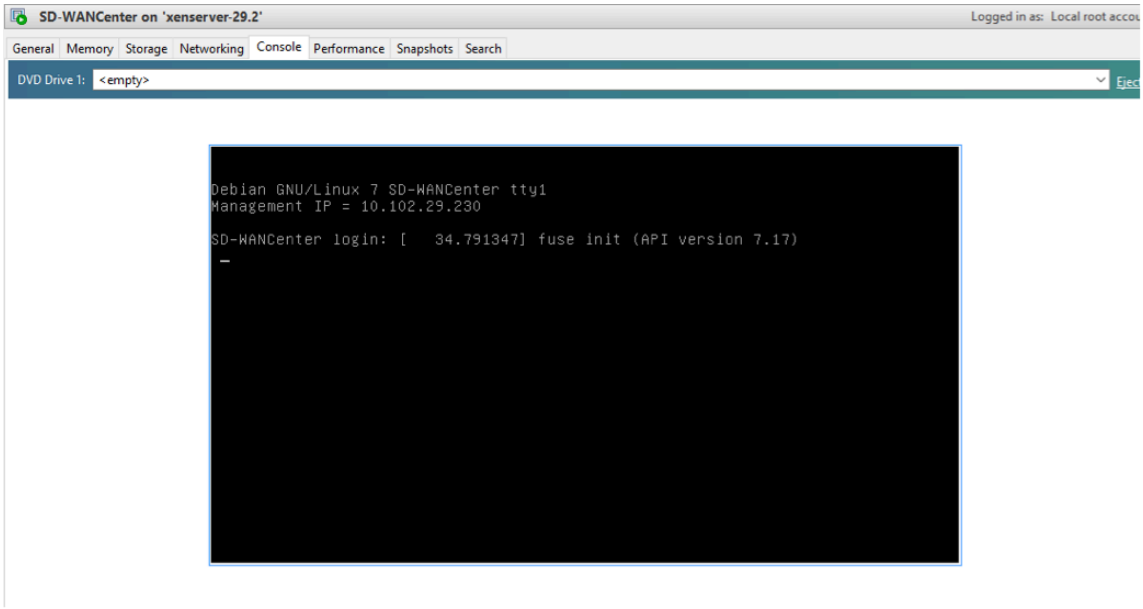
> **Note**
>
> The DHCP server must be present and available in the SD-WAN network.

To display the management IP Address:

1. In the XenCenter interface, in the left pane, right-click the new Citrix SD-WAN Center VM and select **Start**.



2. When the VM is started, click the **Console** tab.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

3. Make a note of the management IP address.

   > **Note**
   >
   > The DHCP server must be present and available in the SD-WAN network, or this step cannot be completed.

4. Log into the VM. The default login credentials for the new Citrix SD-WAN Center VM are as follows:

   Login: admin

   Password: password

   If the DHCP server is not configured in the Citrix SD-WAN network, you have to manually enter a static IP address.

To configure a static IP address as the management IP address:

1. When the VM is started, click the **Console** tab.
2. Log into the VM. The default login credentials for the new Citrix SD-WAN Center VM are as follows:

   Login: admin
   , **Password**: password
3. In the console enter the CLI command **management_ip.**
4. Enter the command **set interface <ipaddress> <subnetmask> <gateway>**, to configure management IP.

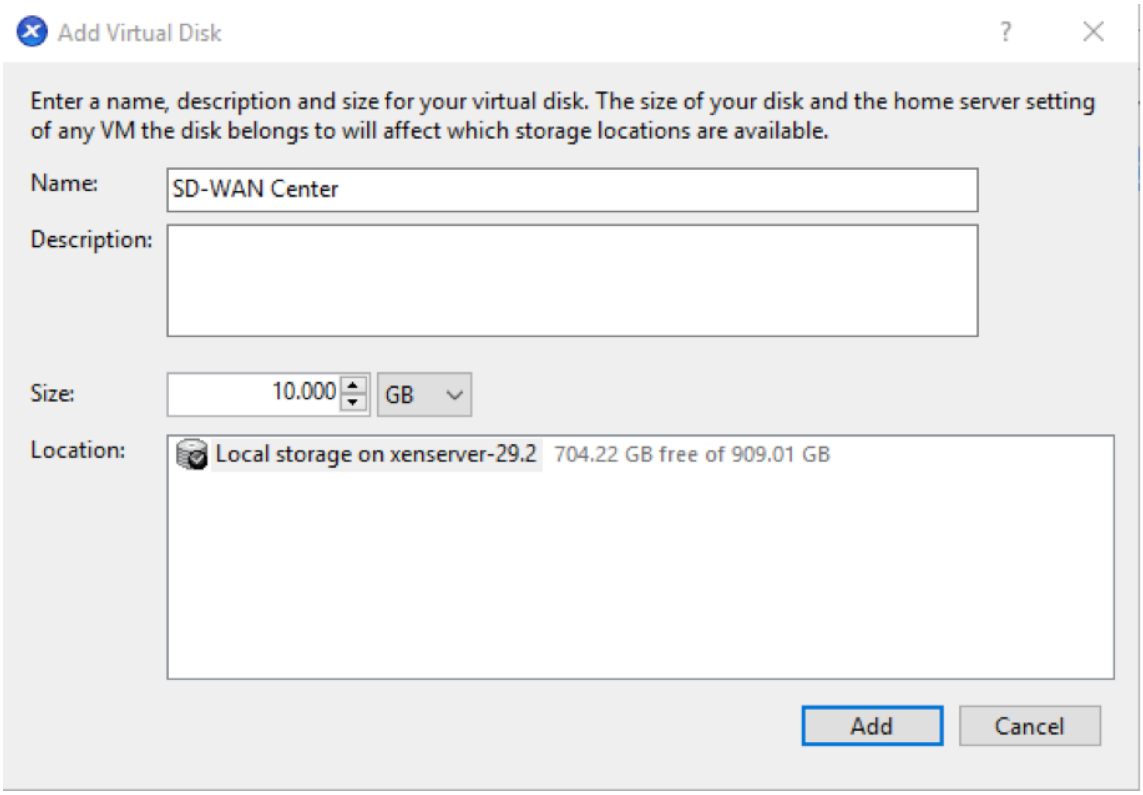
Add and configuring data storage for a XenServer server

You can add and configure data storage to store statistics from Citrix SD-WAN center.

To add and configure the data storage:

1. In XenCenter, shut down the Citrix SD-WAN Center VM.
2. On the **Storage** tab, click **Add**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



3. In the **Name** field, enter a name for the virtual disk.
4. In the **Description** field enter a description of the virtual disk.
5. In the **Size** field select the size required.
6. In the **Location** field select the local storage.
7. Click **Add**.

Install and configure Citrix SD-WAN Center on Microsoft Hyper-V

March 12, 2021

Before installing the Citrix SD-WAN Center virtual machine (VM) on the Microsoft Hyper-V server, gather the necessary information as described in System requirements and installation.

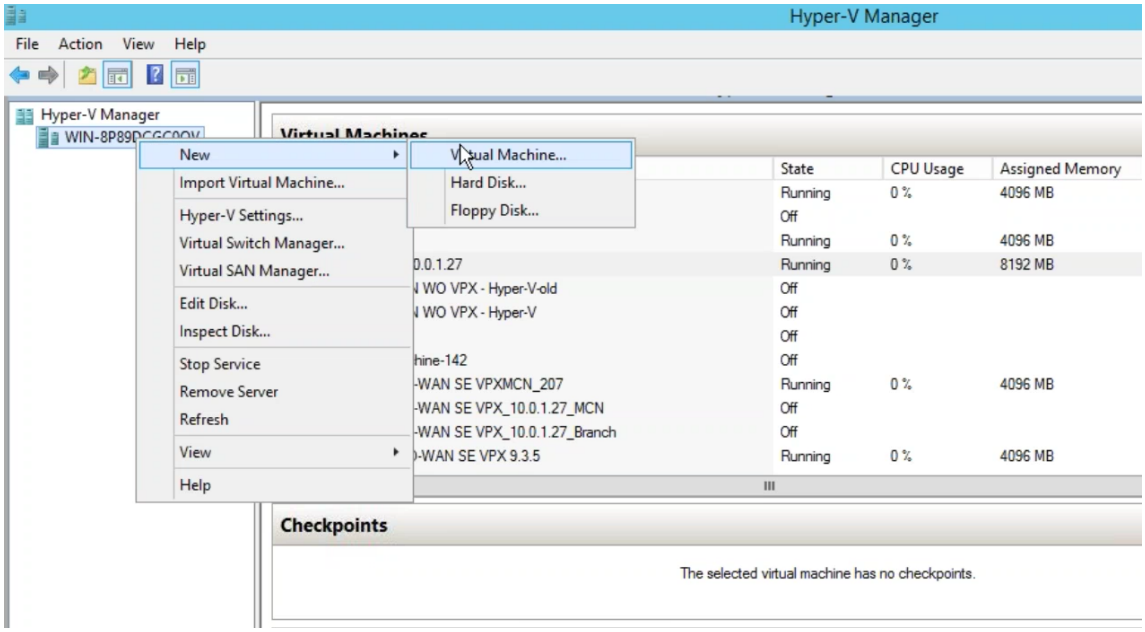
Download the SD-WAN Center software for Hyper-V, as described in Downloading the Citrix SD-WAN Center Software section of System requirements and installation.

Ensure that the Hyper-V feature and management tool are enabled on your Windows server.

To create the SD-WAN Center VM on Hyper-V server:

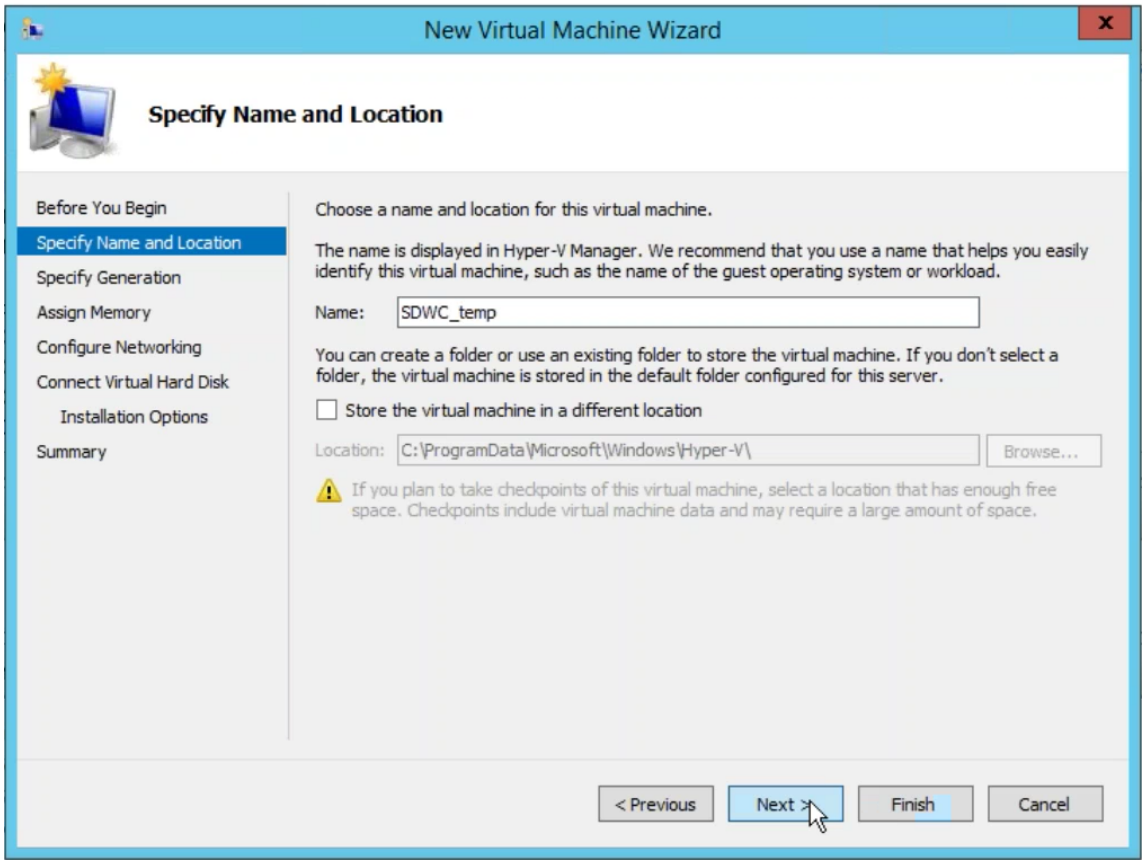
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

1. On the Hyper-V Manager, right-click the Hyper-V server and select **New** > **Virtual Machine**.



   The **New Virtual Machine Wizard** appears. Click **Next**.

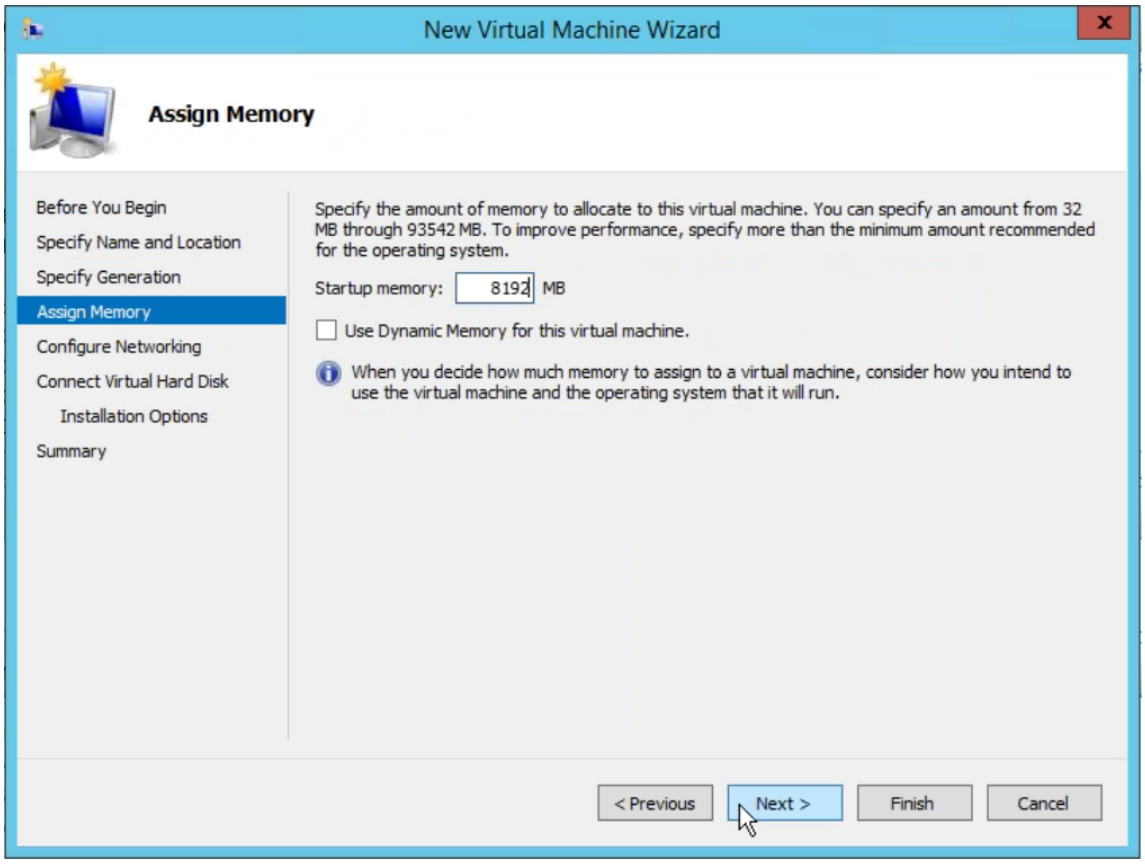
2. Specify a name for your SD-WAN center VM and change the VM storage location, if necessary. Click **Next**.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

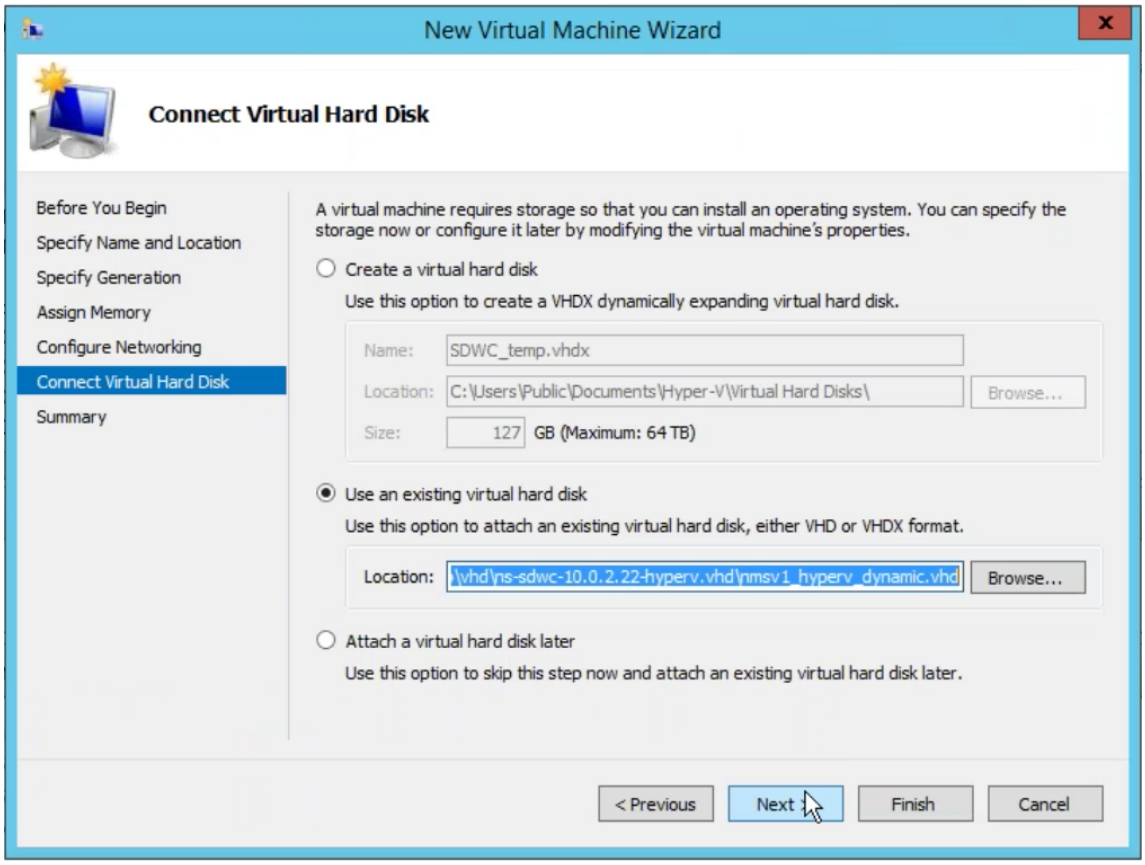
3. Choose the required, VM generation. Click **Next**.
4. Assign a memory of 8 GB for the VM. Click **Next**.

> **Note**
>
> The Citrix SD-WAN Center VM requires a minimum of 8 GB memory to manage up to 64 sites. For more information on memory to the number of sites mapping, see System requirements and installation.



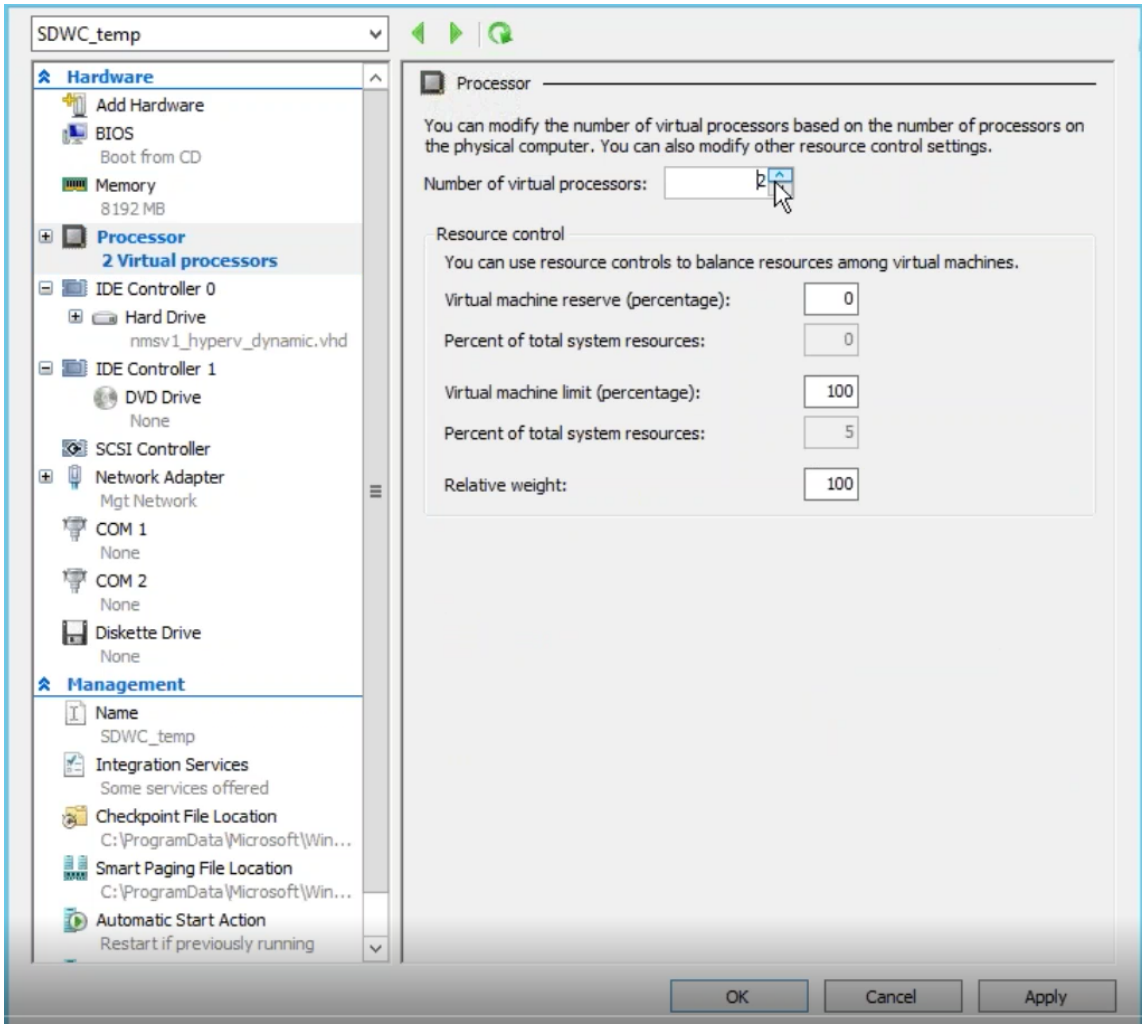
5. Choose the Virtual switch to be used by the VM's network adapter, Click **Next**.
6. Select **Use an existing virtual hard disk**, browse, and select the SD-WAN Center VHD file that you downloaded. Click **Next**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

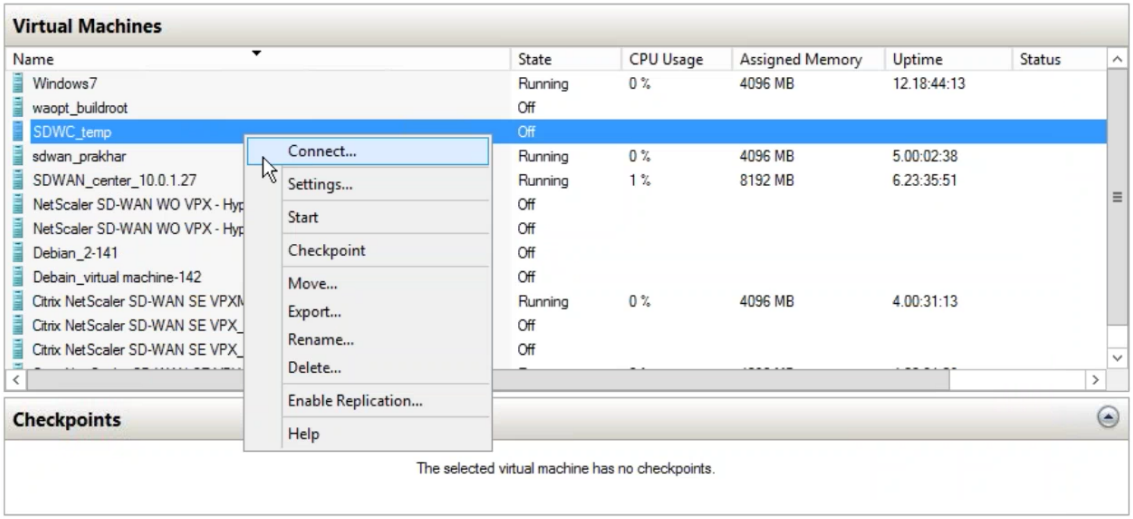


7. Review the VM summary and change the settings if necessary, else click **Finish**. The SD-WAN Center VM is created and is listed in the **Virtual Machines** section.
8. Right-click the SD-WAN Center VM and select **Settings**. Set the number of virtual processors to four and click **Apply**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

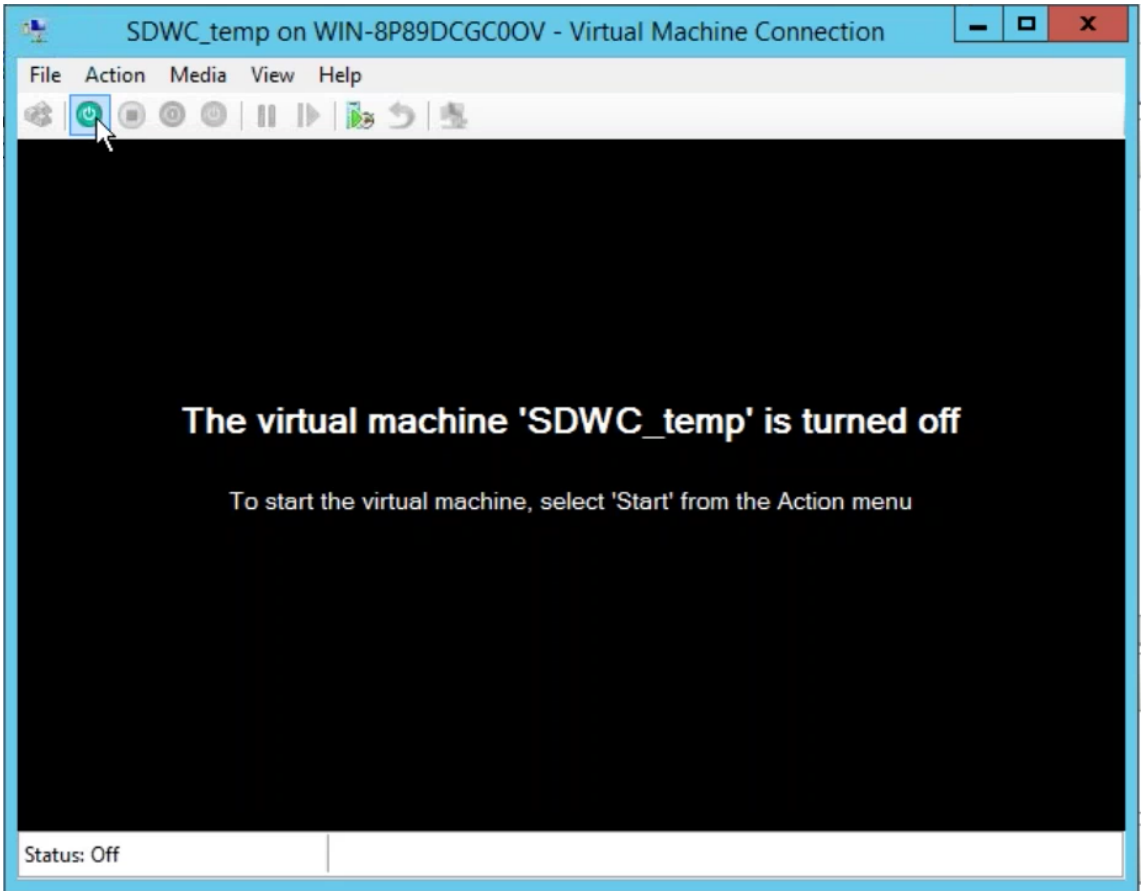


9. Right-click the SD-WAN Center VM and click **Connect**.



10. Click the **Start** button.

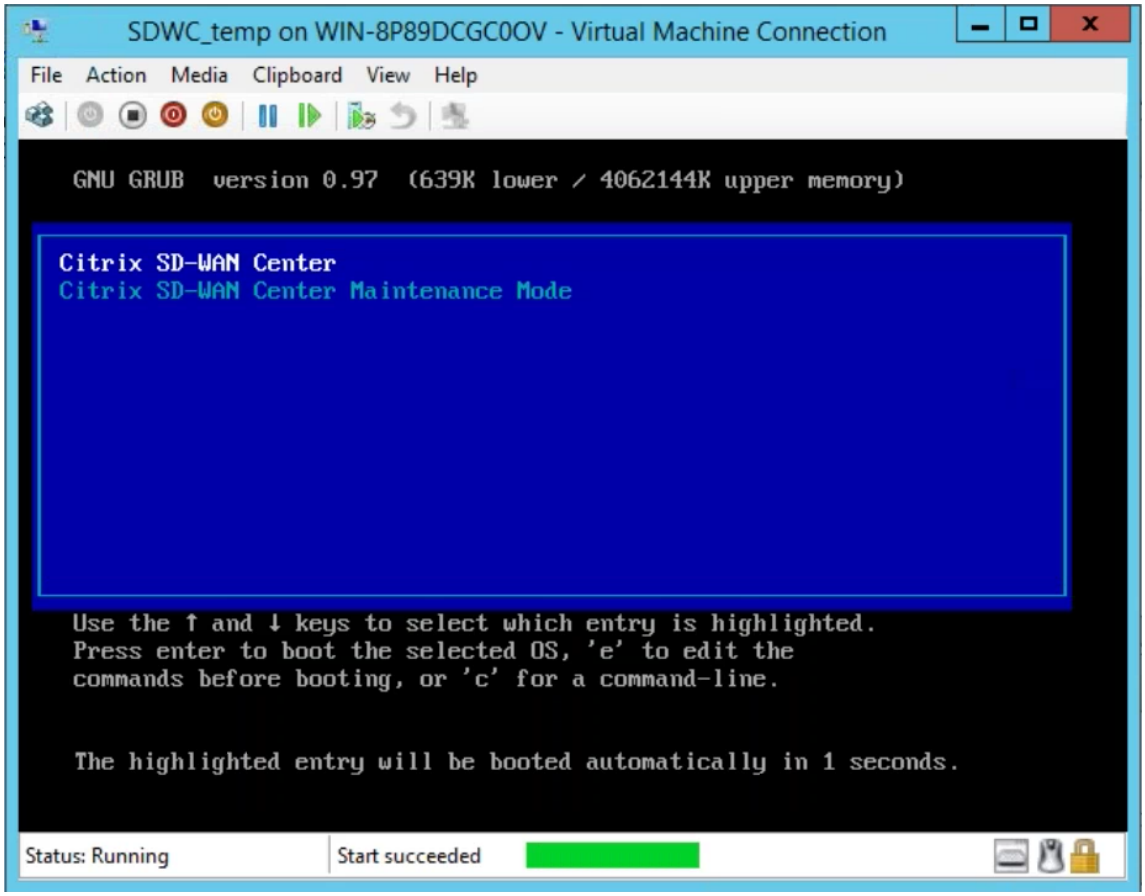
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



> **Note**
>
> The initial installation may take up to 50 min, depending on the number of CPUs and RAM that you have configured.

11. Once the VM is started, selected Citrix SD-WAN Center and hit enter.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

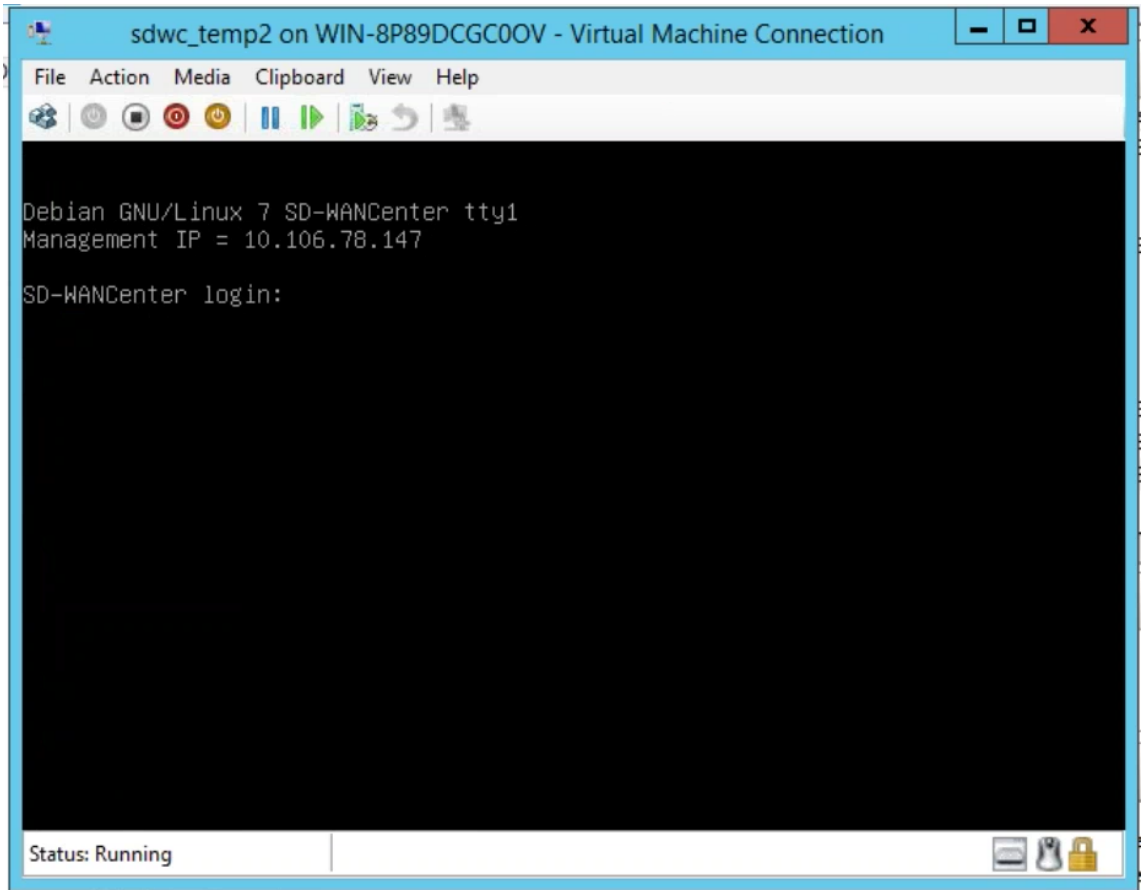


12. Log into the VM. The default login credentials for the new SD-WAN Center VM are as follows:

    Login: admin

    Password: password

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



The management IP address is displayed in the console use this IP to access the SD-WAN Center web interface.

> **Note**
>
> If DHCP is not configured in the SD-WAN network, you have to enter a static IP address manually.

To configure a static IP address as the management IP address:

1. Log into the VM. The default login credentials for the new SD-WAN Center VM are as follows:

   Login: admin

   Password: password

2. In the console, enter the CLI command ***management_ip***.
3. Enter the command **set interface <ipaddress> <subnetmask> <gateway>**, to configure the management IP.

Use the management IP to access the Citrix SD-WAN Center web interface.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Citrix SD-WAN Center on Azure Marketplace using solution template

March 12, 2021

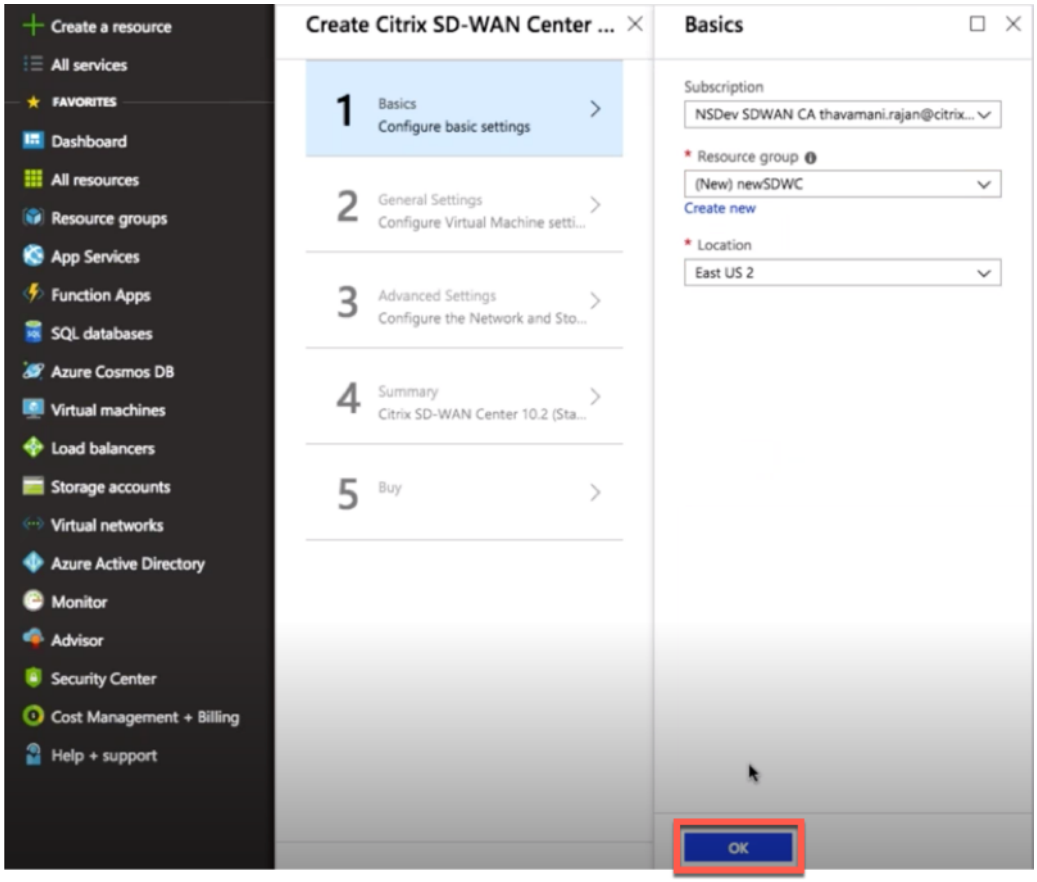
Citrix SD-WAN Center is now available in the Azure Marketplace. You can deploy Citrix SD-WAN Center as a Virtual Machine (VM) in Azure Cloud using solution template.

Before installing the Citrix SD-WAN Center virtual machine (VM) on the Microsoft Azure, gather the necessary information as described in System requirements and installation.

Ensure that you have access to Microsoft Azure.

To deploy Citrix SD-WAN Center VPX on Microsoft Azure:

1. In Microsoft Azure, navigate to **Home > Marketplace**. Search and select the **Citrix SD-WAN Center**.
2. Click **Create** on the **Citrix SD-WAN Center** page. The **Create Citrix SD-WAN Center** page appears.
3. In the **Basics** section, select the subscription type, resource group, and location. Click **OK**.

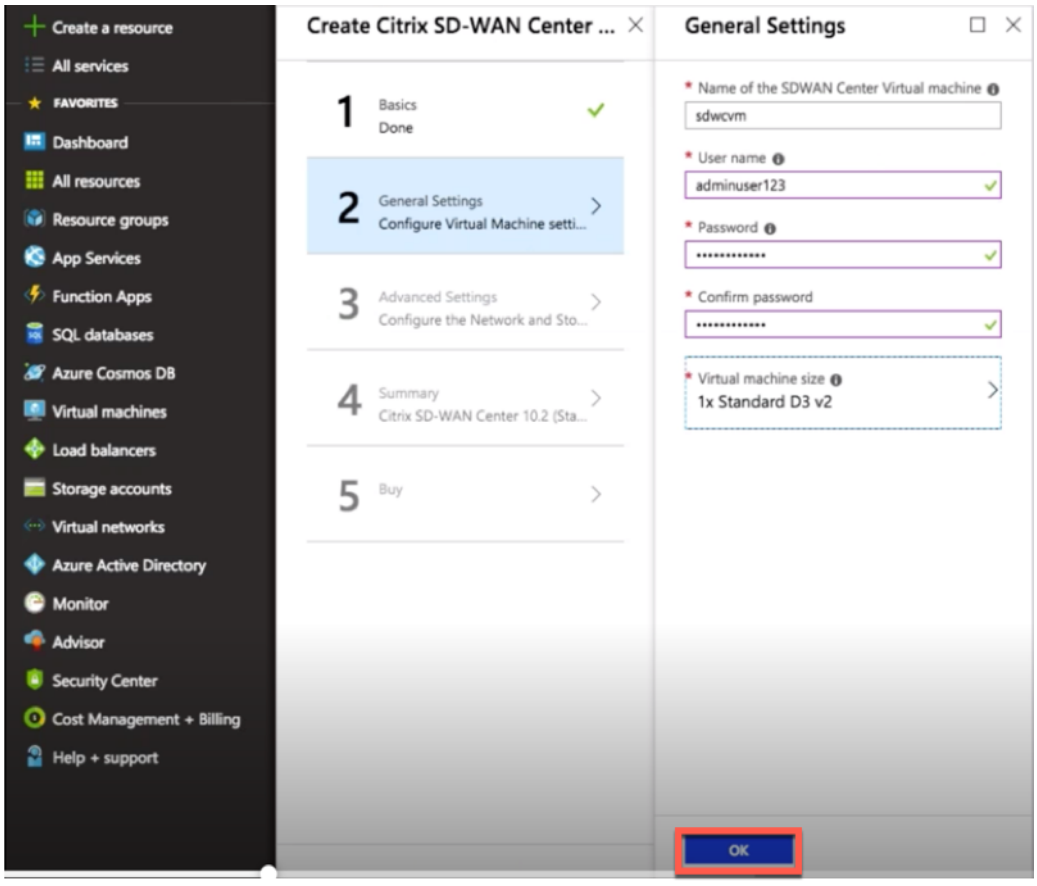


© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> **NOTE:**
>
> A resource group is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You can decide how you want to allocate resources to resource groups based on your deployment.

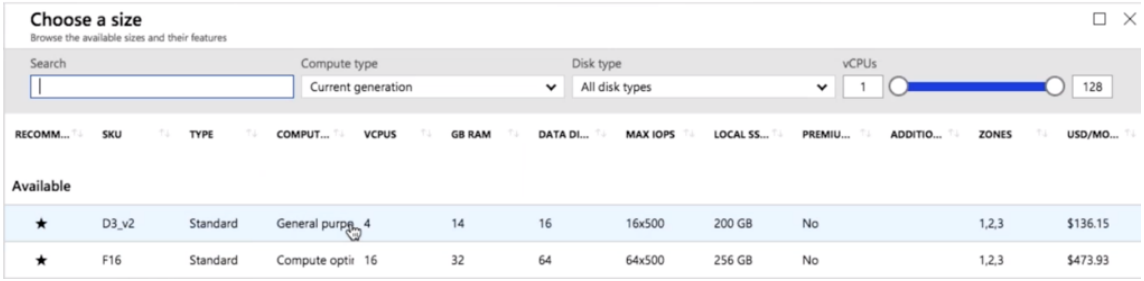
4. In the **General Settings** section, enter the name and credentials that provide admin level access or privileges for the Citrix SD-WAN Center virtual machine.

   Credentials that are provided in this step 4, would also be used to set the password for **Admin** user login account (default admin account password can be modified with this password credential). Click **OK**.

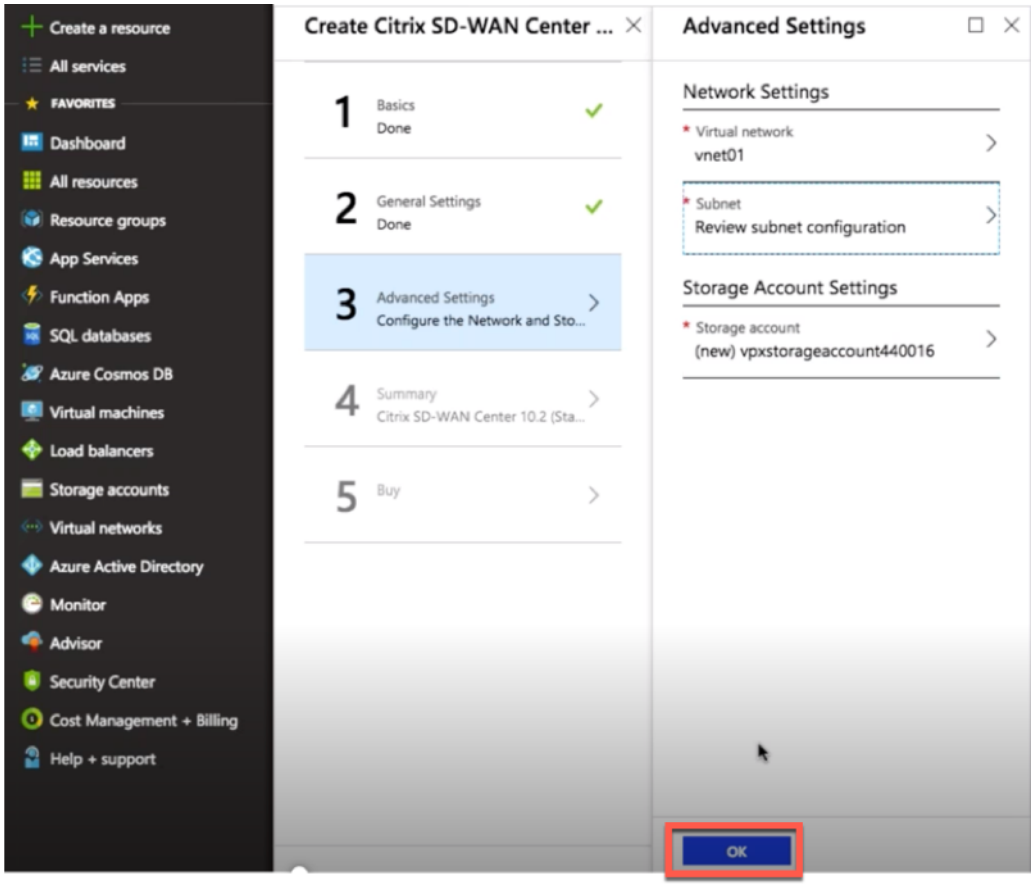


> **NOTE:**
>
> Currently there are two sizes instance types are available –**Standard_D3_v2** and **Standard_F16**. D3_v2 instance can be used to monitor network that has up to 64 sites. The F16 instance is useful to monitor network that has up to 128 sites. You can also search and choose an available virtual machine size.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

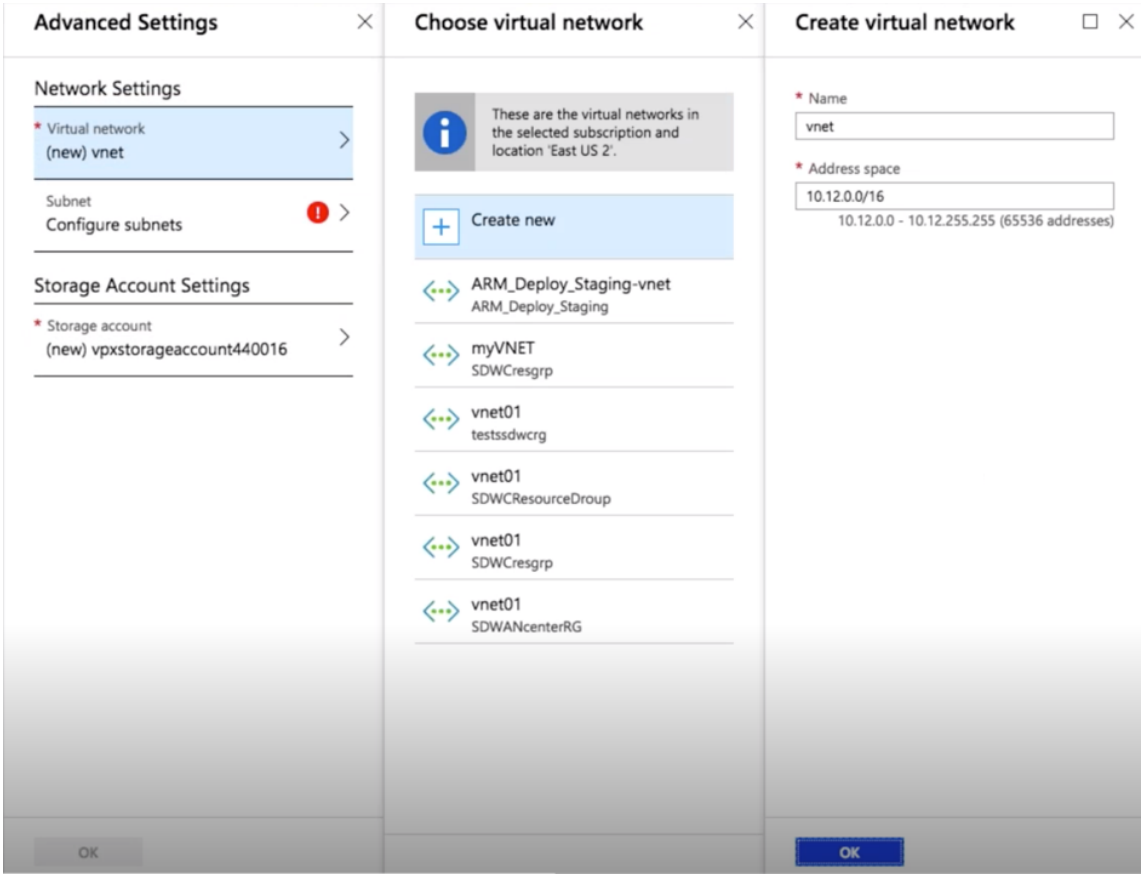


5. In the **Advanced settings** section, configure the **Network and Storage account** setting for the **Citrix SD-WAN Center VPX** based on the number of sites to be monitored.



Select virtual network from the available list or you can create a new virtual network by giving a **Name** and **Address Space**.

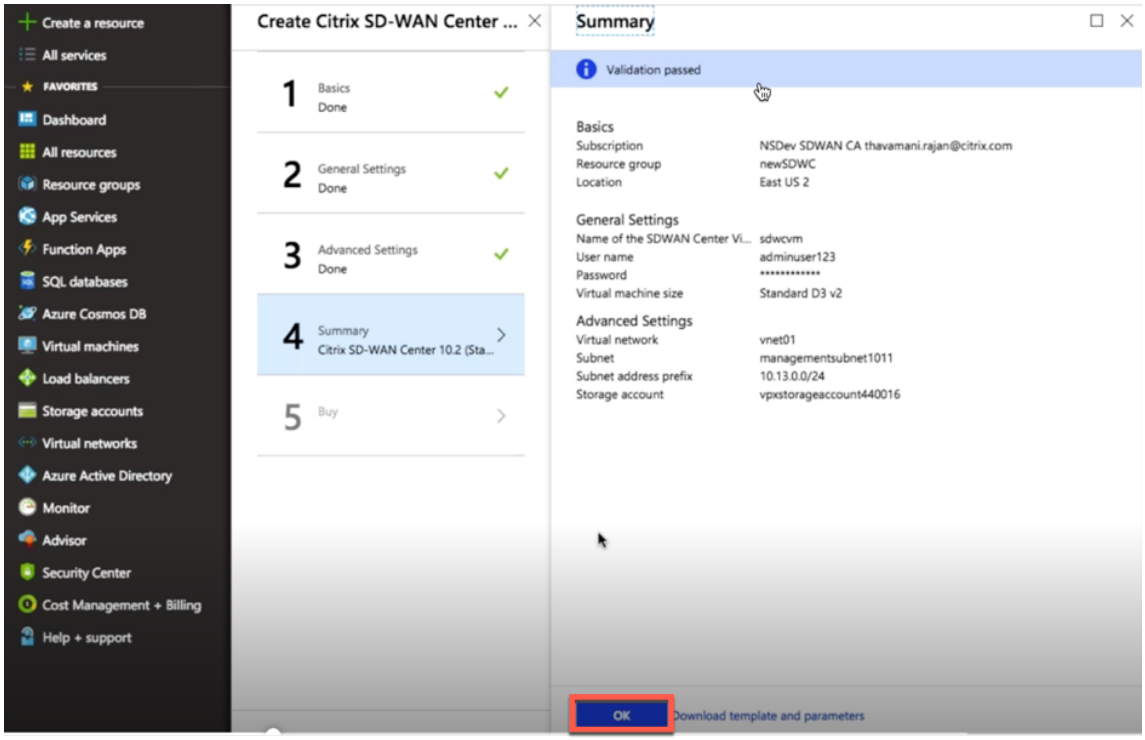
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



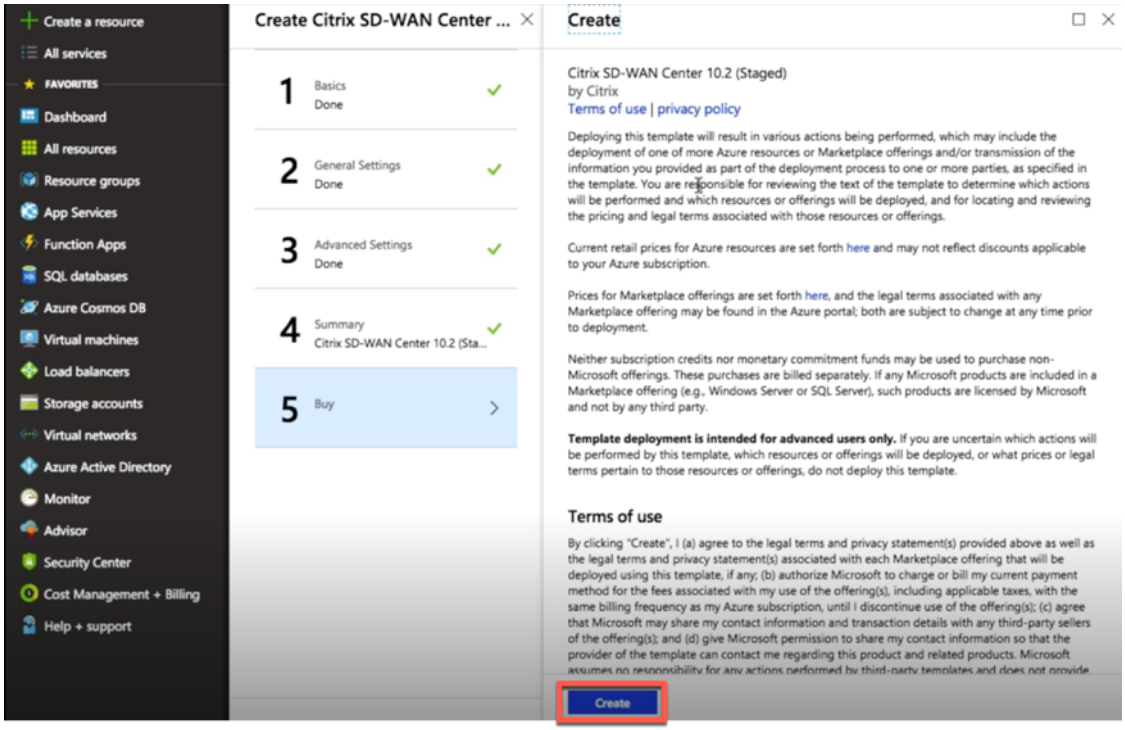
Select **Subnet** from the drop-down list. Create a **Storage Account** and click **OK**.

6. The configuration that you provided in previous steps is validated and applied. If you have configured correctly, the validation passed message appears. Click **OK**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



7. After successful deployment, **Create** page appears. Read the **Terms of use and Privacy policy** carefully and click **Create**.



Wait for the VM provisioning to get complete and then login with the IP that is been assigned to that VM (by checking the networking section and use the admin credentials (that was set in step 4) and

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

follow the general SD-WAN Center deployment guidelines.

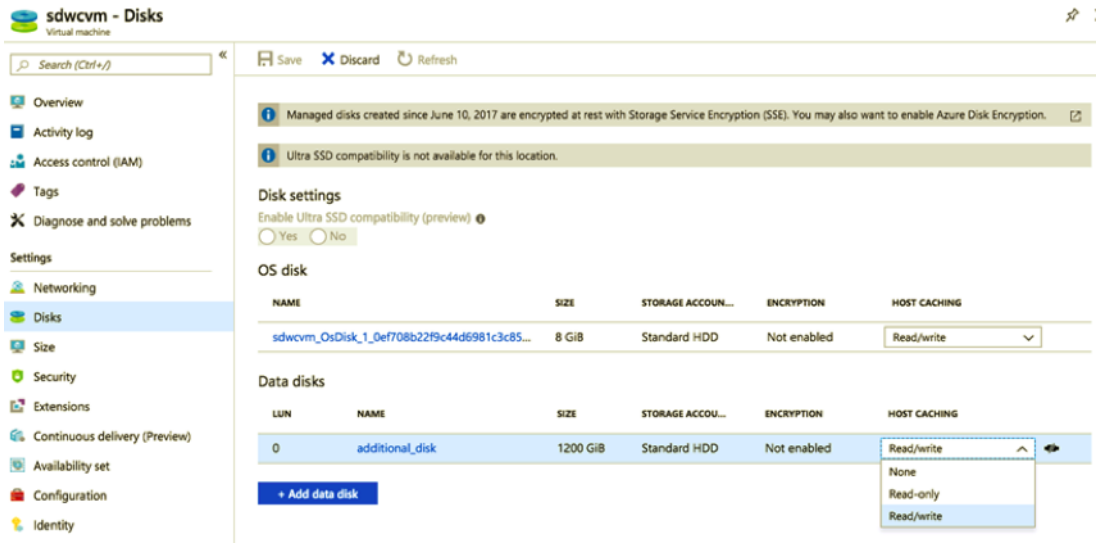
Add data disk

This section describes how to attach a new managed data disk to a Virtual Machine (VM) by using the Azure portal. The VM size determines how many data disks you can attach.

In the Azure portal, from the menu on the left, select **Virtual machines** and select a virtual machine from the list.

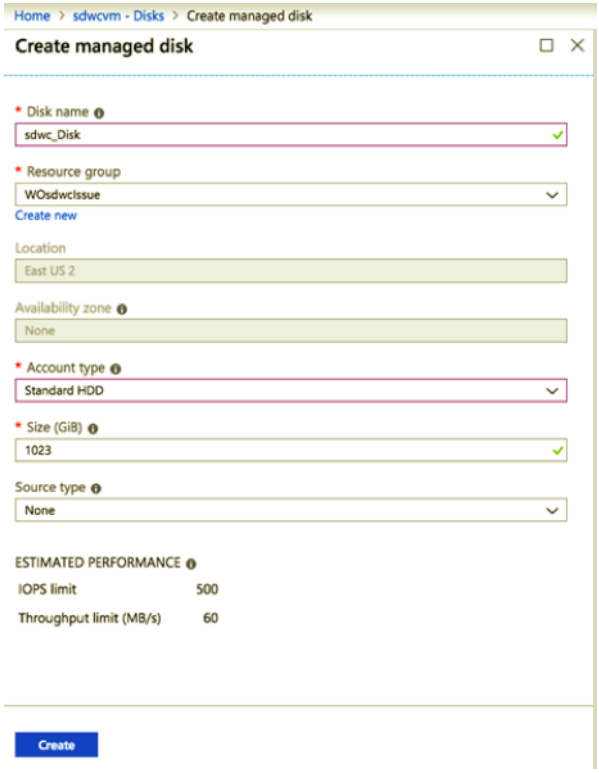
Perform the following actions to add additional data disk in Azure SD-WAN Center:

1. Shut down the VM.
2. From the VM dashboard, select **Disks** under **Settings** section.



3. Click **+ Add data disk** and create a new data disk with read and write permission.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Attach a disk by filling the following mandatory details:

- **Disk name** –Provide a name for SD-WAN Center data disk.
- **Resource group** –Select a resource group from the drop-down list.
- **Account type** –Select an account type from the drop-down list.
- **Size (GIB)** –Provide a size in gibibyte.
- **Storage type** - Select a source type from the drop-down list.

4. Once you are done, Click **OK**.

To turn on the VM refer the Switch the active storage to new data storage topic.

Citrix SD-WAN Center on AWS in VM importable image format

March 12, 2021

The Citrix SD-WAN Center is a centralized management system or a single pane of glass management solution that enables enterprises to configure, monitor, and analyze all Citrix SD-WAN appliances on their WAN.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Instantiating an SD-WAN Center virtual Appliance (AMI) on AWS

You need an AWS account to install an SD-WAN Center virtual appliance in an AWS VPC. You can create an AWS account here. SD-WAN Center is available as an Amazon Machine Image (AMI) in AWS Marketplace.

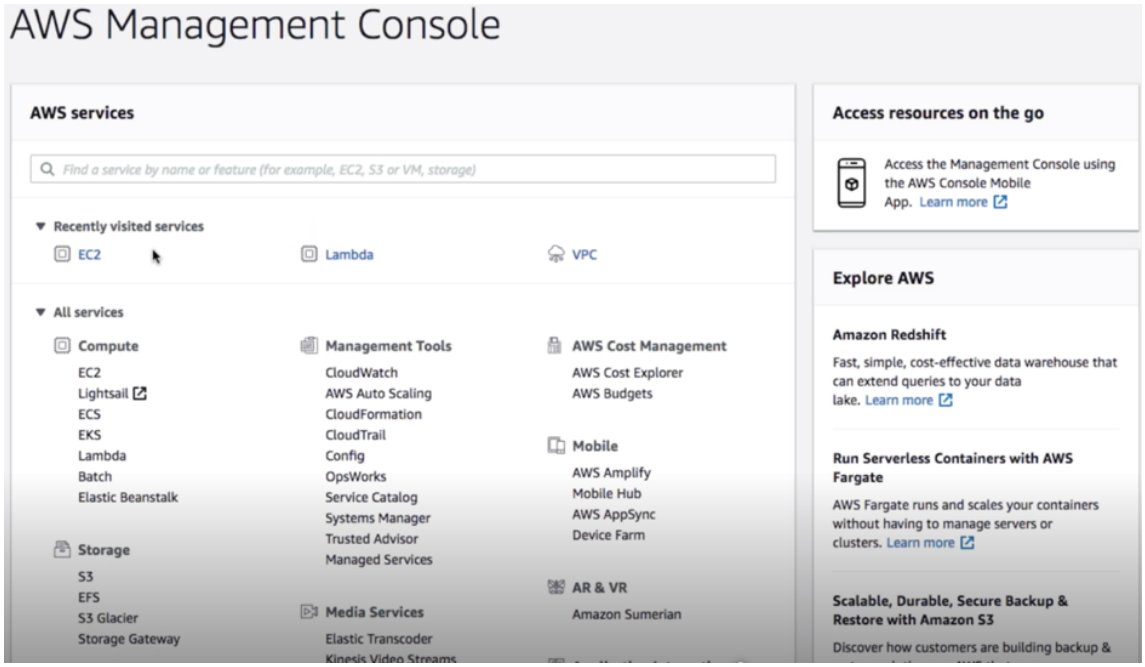
> **Note:**
>
> Amazon makes frequent changes to its AWS pages, so the following instructions may not be up-to-date.

There are two approaches to instantiate an SD-WAN Center virtual appliance (AMI) on AWS:

1. **First approach:** In a web browser, type http://aws.amazon.com/. Select AWS Management Console under My Account to open the Amazon Web Services (AWS).

   Second approach:
   In a web browser, type http://console.aws.amazon.com to open the **Amazon Web Services**.

2. Use your AWS account credentials to sign in. This takes you to the **Amazon Web Services** page. You can view the **Recently visited services** list along with all other services.

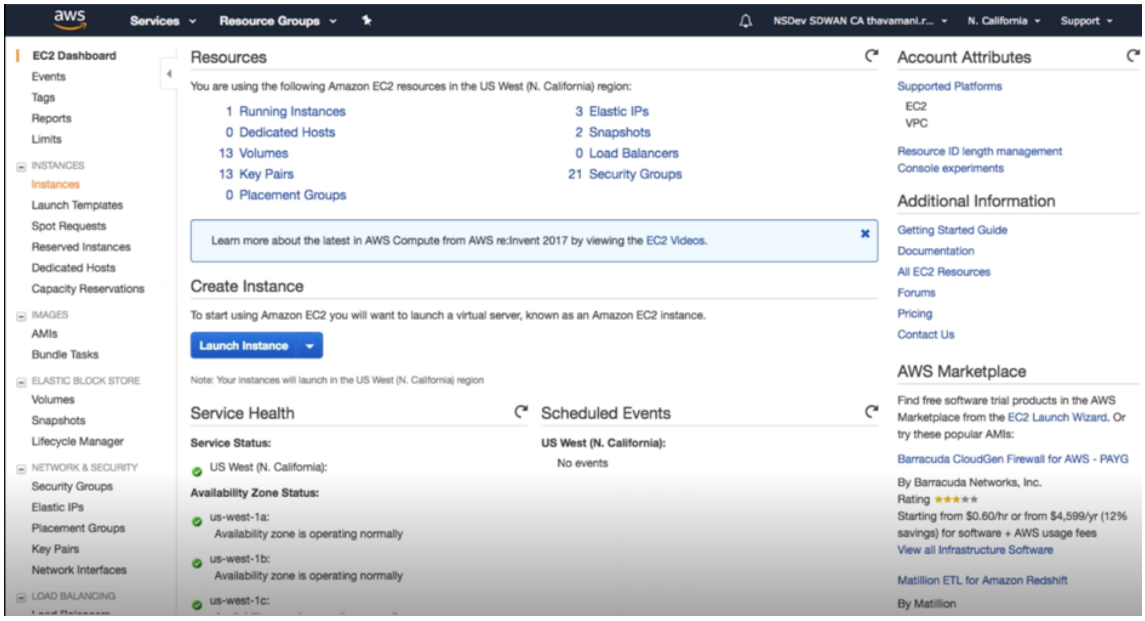


   Citrix SD-WAN Center appliances offer the EC2 as an AWS service instances.

   - **EC2 Dashboard** - elastic compute cloud, resizable virtual services / instances

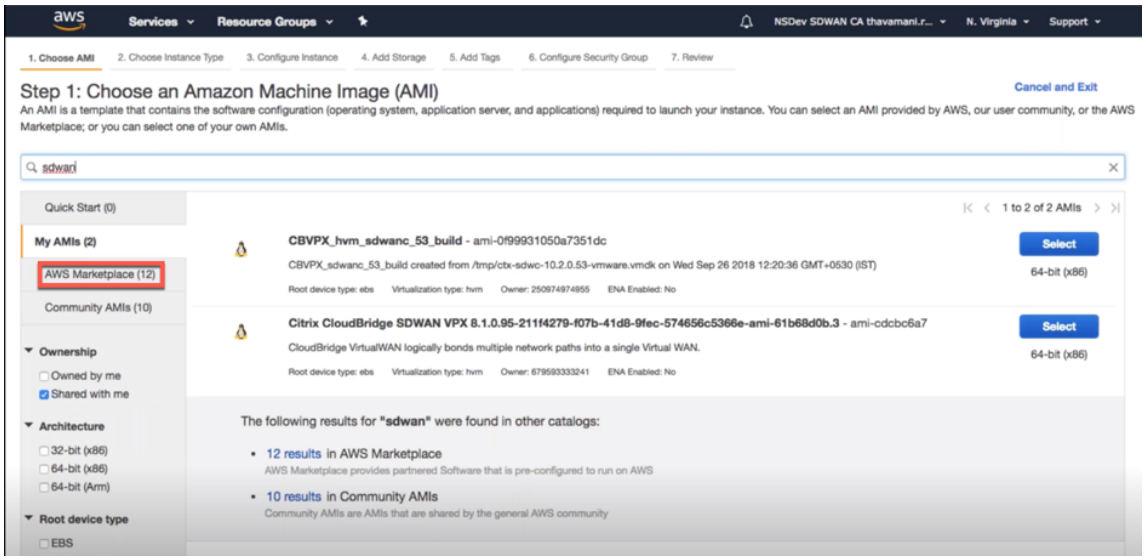
3. Click **EC2** in the **Compute** section, then select **Launch Instance**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



You can either select the **Launch Instance** option or manually reach to **Instance** screen by selecting the **Instances** option location on the left side under **INSTANCES** (refer the above screenshot).

4. In the **Choose AMI** page, click **AWS Marketplace** tab.
5. In the Search text field, type SD-WAN to search for the SD-WAN AMI, and click **Search**.



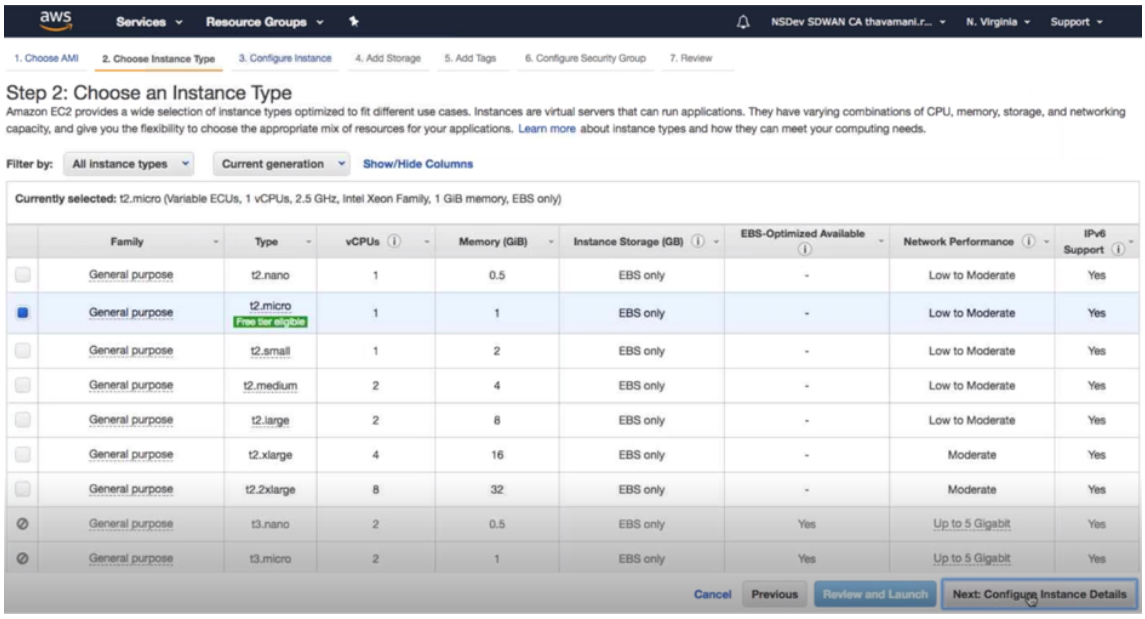
On the search result page, select one of the Citrix SD-WAN Center AMI with the latest release, click **Select**.

An **AMI** template contains the software configuration including operating system, application server, and applications. This template is required to launch instances.

6. Choose an instance type and select **Next: Configure Instance Detail**. You can filter your search

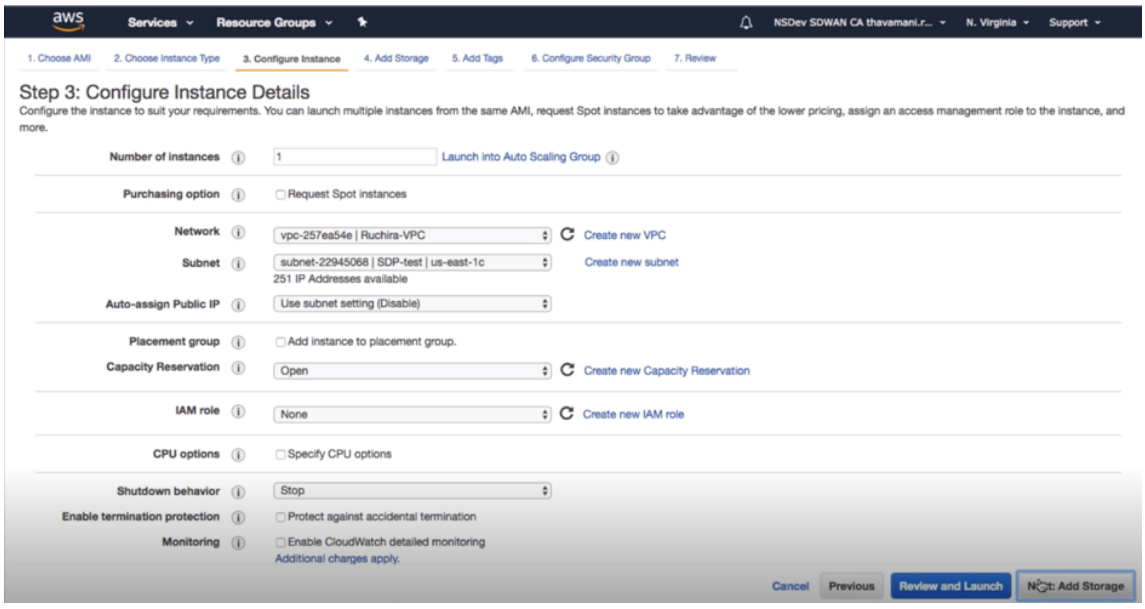
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

by selecting a specific instance type or all instance type with current generation.



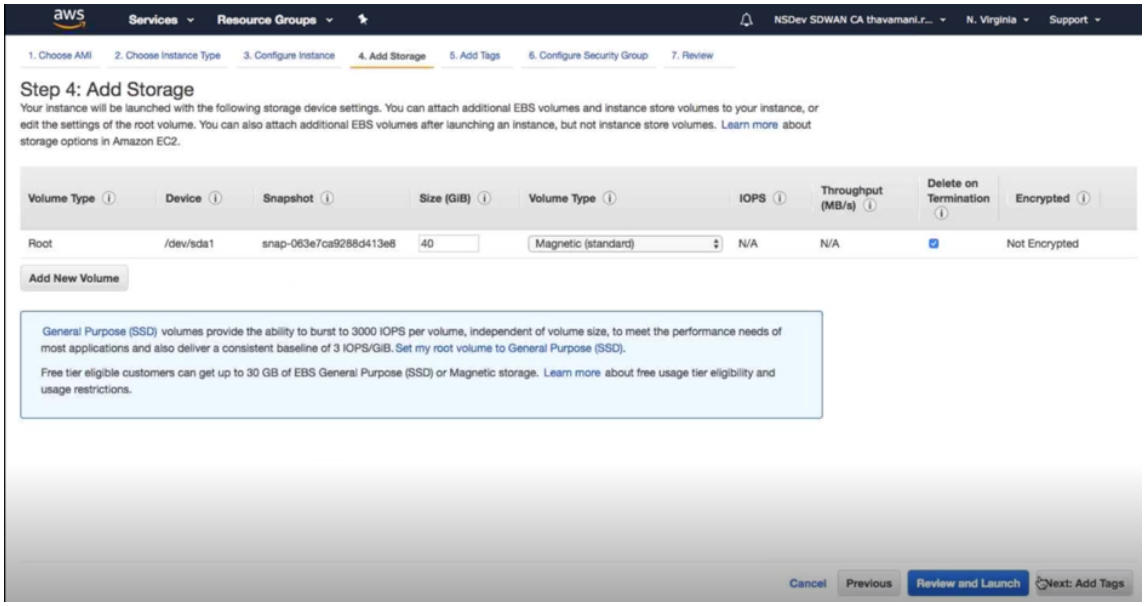
The amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications.

7. On the **Configure Instance** page, type 1 in the **Number of Instances** text box, and fill the other details such as Network, Subnet, and so on for a specific instance as needed. Click **Next: Add Storage**.

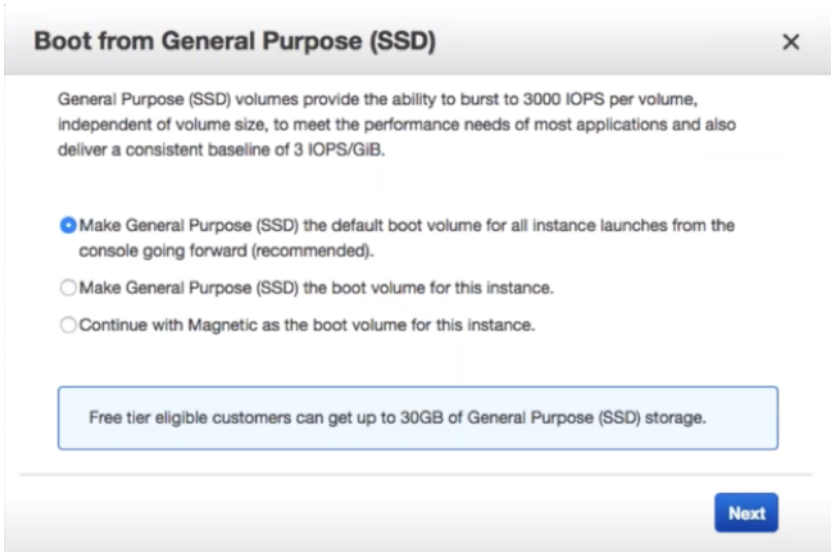


8. The instance is launched with the storage device settings. You can add a new volume separately once the instance is provisioned.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

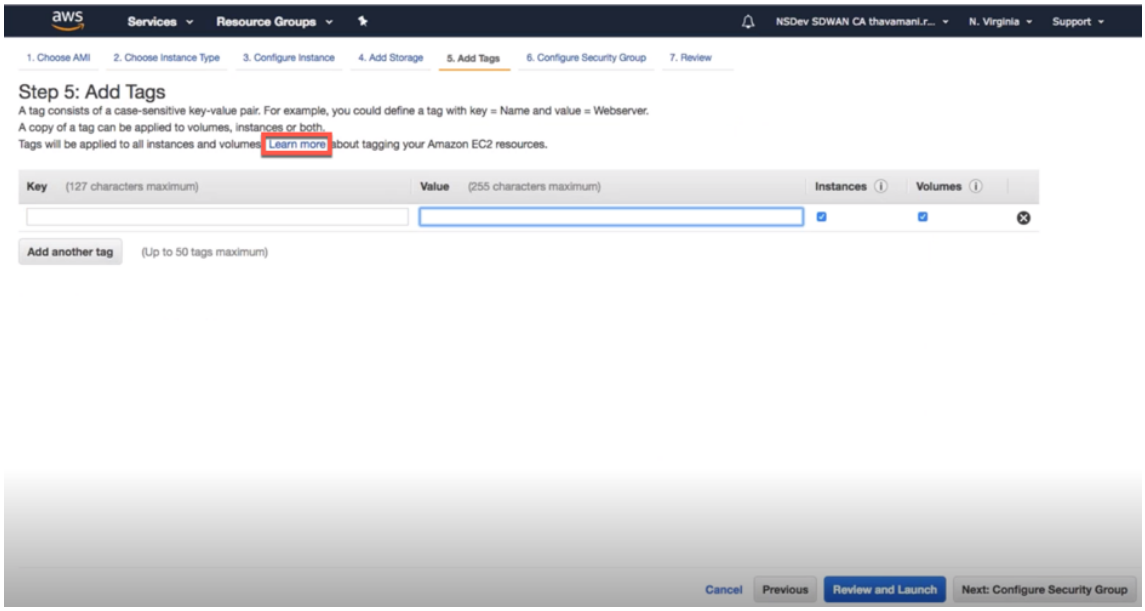


9. Click **Review and Launch** to select the boot volume option as per your requirement. Click **Next**.



10. Add or define a tag with a **Key Name** and **Value**. Click **Learn more** to learn more about tagging. You can add up to 50 tags maximum. Click **Next: Configure Security Group**.

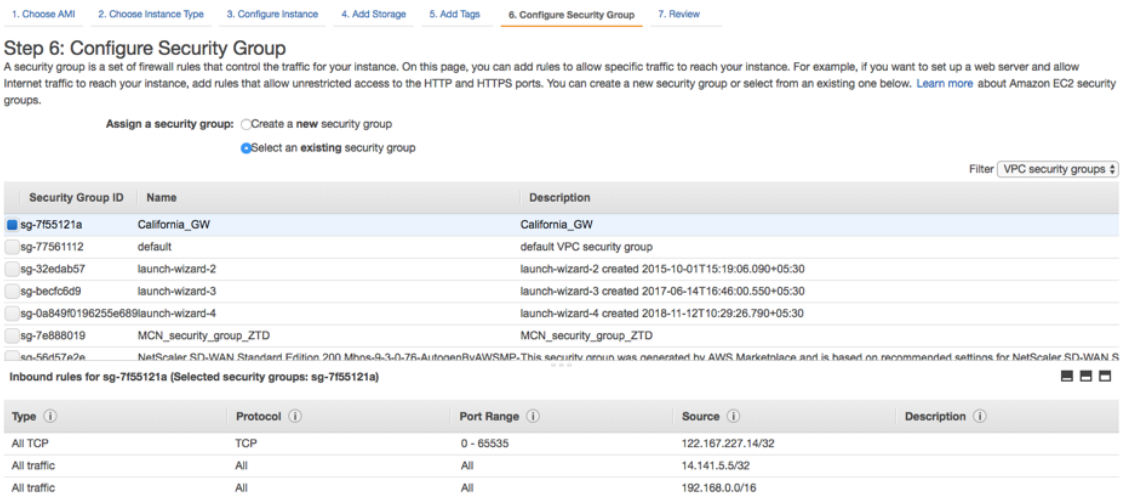
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



> **Note:**
>
> NOTE: A tag key length must be between 1–127 characters.

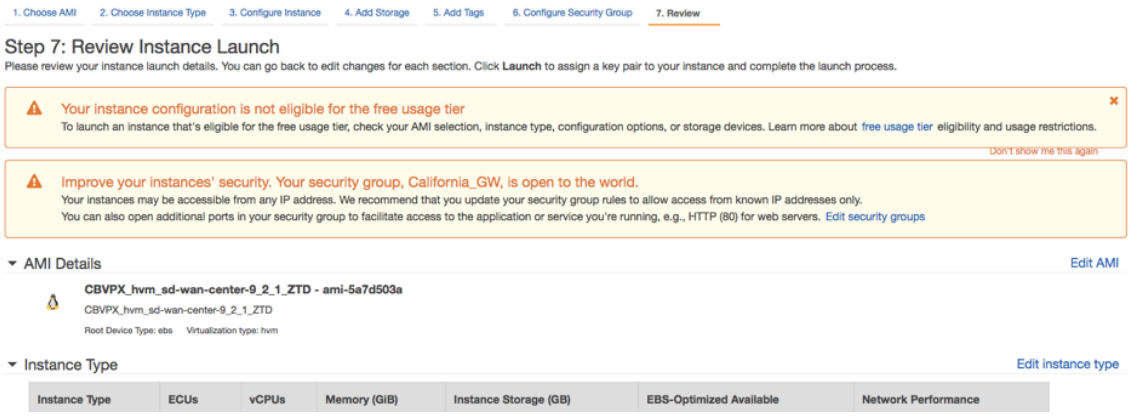
11. You can create a general security group that helps to control traffic for the instance. You can create a new security group or select an existing security group from the list.

> **Note:**
>
> Ensure the security group allows the inbound connections over 2156 port to collects data from Citrix SD-WAN appliances.



12. Review the instance launch details, and then click **Launch**. A pop-up box appears to ask for creating a key pair. It is mandatory to create a Key pair for the instance.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Two factor authentication

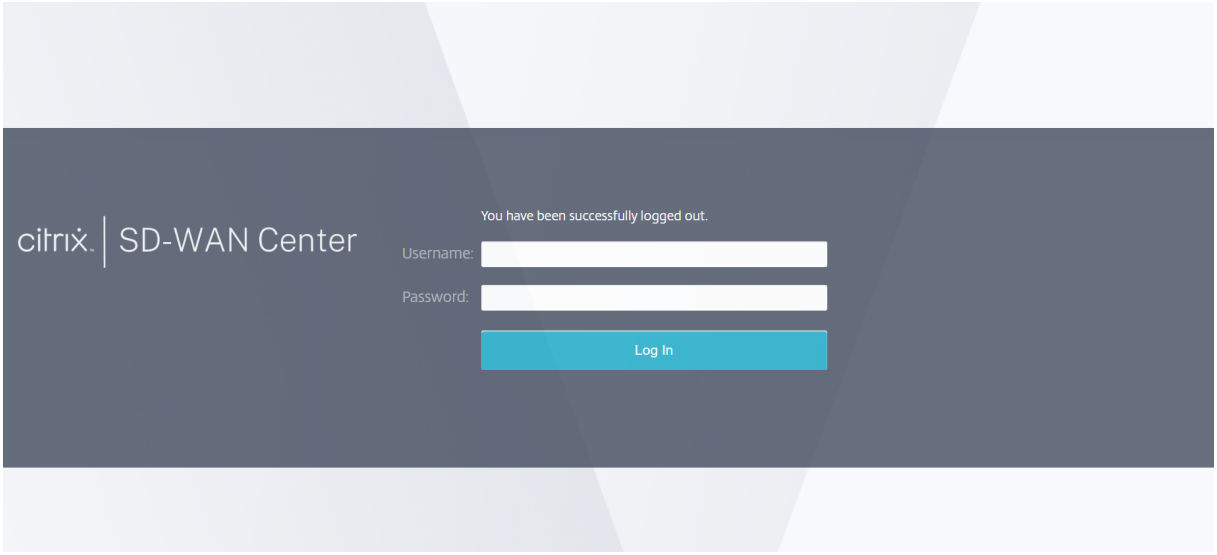
March 12, 2021

Two-factor authentication (TFA) presents two authentication factors to gain access to Citrix SD-WAN Center for both local and remote user accounts. It introduces an extra layer of security in the Citrix SD-WAN Center login sequence.

The first level of authentication for a local user account is achieved by using the password configured on Citrix SD-WAN Center. For more information, see User accounts.

The first level of authentication for a remote user account is achieved by using the primary RADIUS or TACACS+ authentication server. For more information, see Primary authentication.

An extra secondary RADIUS or TACACS+ authentication server can be configured for both local and remote user accounts to enable two-factor authentication. For more information, see Secondary authentication.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Citrix SD-WAN Center login credentials:

- **Username**: The username configured on SD-WAN Center or the primary authentication server.
- **Password**: The password configured on SD-WAN Center or the primary authentication server.
- **Secondary Password**: The password configured on the secondary authentication server.

> **Note**
>
> The **Secondary Password** option appears only when the secondary authentication server is configured.

Primary authentication

March 12, 2021

You can configure authentication servers such as RADIUS or TACACS+ to authenticate remote users logging on to Citrix SD-WAN Center. Primary authentication is the first authenticating factor for remote users when two-factor authentication is enabled. For more information, see Two-factor authentication.

> **Note**
>
> Ensure that user accounts are created on the required authentication servers.

RADIUS authentication server

To use RADIUS authentication, you must specify and configure at least one RADIUS server. Optionally, you configure redundant backup servers, up to a maximum of three RADIUS servers. The servers are checked sequentially, starting with the server listed first in the **Servers** section. Ensure that the required user accounts are created on the RADIUS authentication server.

To enable and configure RADIUS authentication:

1. In the Citrix SD-WAN Center web interface, navigate to **Administration** > **User/Authentication Settings**.
2. In the **Primary Authentication** > **RADIUS Authentication** section, select the **Enable RADIUS Authentication** check box.

   > **Note**
   >
   > If TACACS+ authentication is already enabled, it gets disabled.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

3. In the **Timeout** field, enter the time interval (in seconds) to wait for an authentication response from the RADIUS server.

   The timeout value should be less than or equal to 60 seconds.

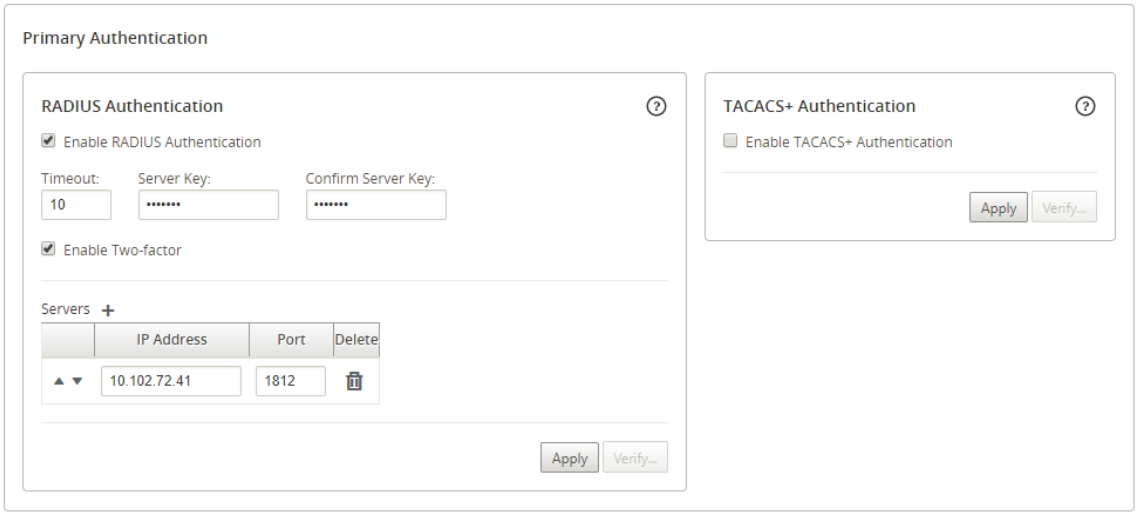
4. In the **Server Key** field, enter a secret key to use when connecting to the RADIUS servers.
5. In the **Confirm Server Key** fields, reenter the secret key.

   > **Note**
   >
   > The **Timeout** and **Server Key** settings are applied to all configured servers.

6. Select **Enable Two-factor**, to enable two-factor authentication.

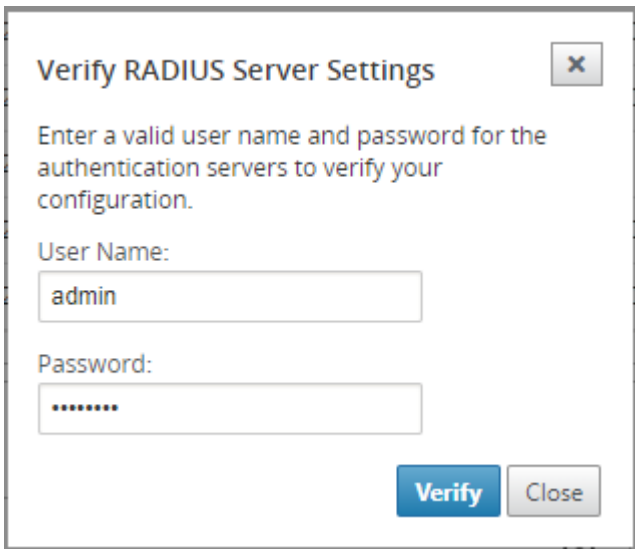
   > **Note**
   >
   > The **Enable Two-factor** option appears only when the secondary authentication server is configured.
   >
   > Configure a secondary authentication server, either RADIUS, or TACAS+. For more information, see Secondary authentication.

7. Click the plus icon (+) next to **Servers** to add a RADIUS server.
8. In the **IP Address** field, enter the host IP address for the RADIUS server.
9. In the **Port** field, enter the port number for RADIUS server. The default port number is 1812.



10. Click **Apply**.
11. Click **Verify** to verify the connection to the RADIUS server. The **Verify RADIUS Server Settings** dialog box appears.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



12. Enter a valid username and password for the authentication servers, and click **Verify**.

To configure more servers, repeat the steps 7 through 12.

TACACS+ authentication server

To use TACACS+, you must specify and configure at least one TACACS+ server. Optionally, you configure redundant backup servers, up to a maximum of three TACACS+ servers. The servers are checked sequentially, starting with the server listed first in the **Servers** section. Ensure that the required user accounts are created on the TACACS+ authentication server.

To enable and configure TACACS+ authentication:

1. In the Citrix SD-WAN Center web interface, navigate to **Administration** > **User/Authentication Settings**.
2. In the **Primary Authentication** > **TACACS+ Authentication**section, select the **Enable TACACS+ Authentication** check box.

   > **Note**
   >
   > If RADIUS authentication is already enabled, it gets disabled.

3. In the **Timeout** field, enter the time interval (in seconds) to wait for an authentication response from the TACACS+ server.

   The timeout value should be less than or equal to 60 seconds.
4. In the **Authentication Type** field, select the encryption method to use to send the username and password to the TACACS+ server.
5. In the **Server Key** field, enter a secret key to use when connecting to the TACACS+ servers.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

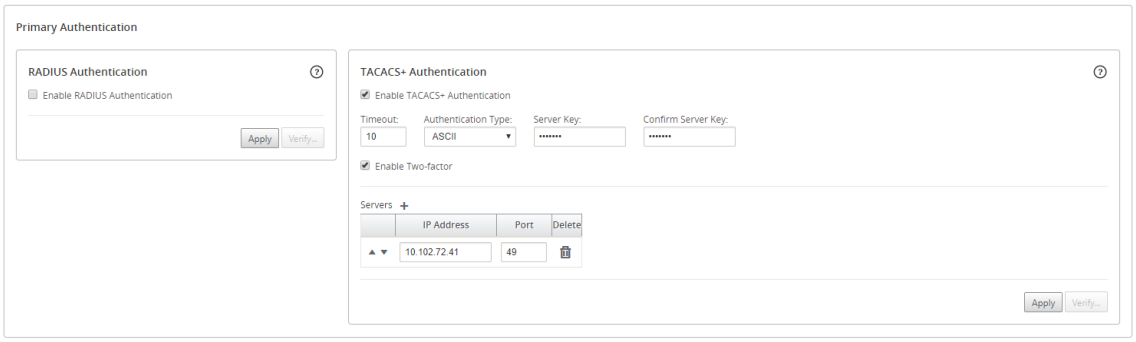
6. In the **Confirm Server Key** fields, reenter the secret key.

> **Note**
>
> The **Timeout**, **Authentication Type**, and **Server Key settings** are applied to all the configured servers.

7. Select **Enable Two-factor**, to enable two-factor authentication.

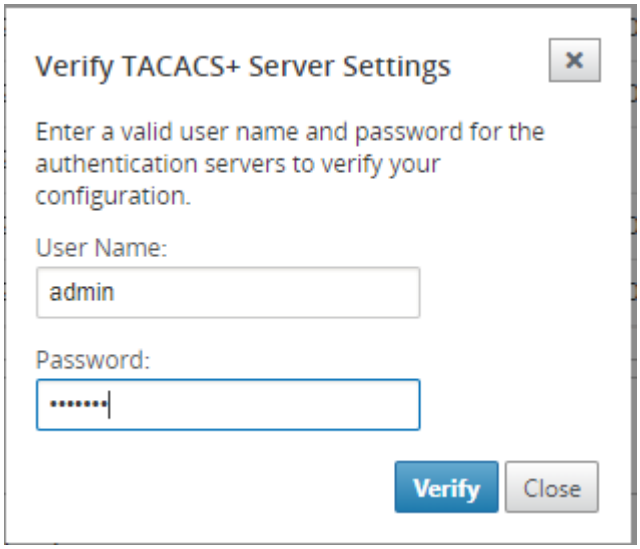
> **Note**
>
> The **Enable Two-factor** option appears only when the secondary authentication server is configured.
>
> Configure a secondary authentication server, either RADIUS, or TACAS+. For more information, see Secondary authentication.

8. Click the plus icon (+) next to **Servers** to add a TACACS+ server.
9. In the **IP Address** field, enter the host IP address for the TACACS+ server.
10. In the **Port** field, enter the port number for TACACS+ server. The default port number is 49.



11. Click **Apply**.
12. Click **Verify** to verify the connection to the RADIUS server. The **Verify TACACS+ Server Settings** dialog box appears.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



13. Enter a valid username and password for the authentication servers, and click **Verify**.

    To configure more servers, repeat the steps 8 through 13.

Secondary authentication

March 12, 2021

Secondary authentication is configured to enable Two-factor authentication for local and remote user accounts. You can configure either the RADIUS or TACACS+ authentication server as the secondary authenticating serve. For more information, see Two-factor authentication.

> **Note**
>
> Ensure that user accounts are created on the required authentication servers. The user account password is to be used as the second factor in the Citrix SD-WAN Center login sequence.

Secondary RADIUS authentication server

To use RADIUS authentication, you must specify and configure at least one RADIUS server. Optionally, you configure redundant backup servers, up to a maximum of three RADIUS servers. The servers are checked sequentially, starting with the server listed first in the **Servers** section. Ensure that the required user accounts are created on the RADIUS authentication server.

To enable and configure RADIUS authentication:

1. In the Citrix SD-WAN Center web interface, navigate to **Administration** > **User/Authentication Settings**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

2. In the **Secondary Authentication** > **RADIUS Authentication** section, select the **Enable Secondary RADIUS Authentication** check box.

   > **Note**
   >
   > If TACACS+ authentication is already enabled, it gets disabled.

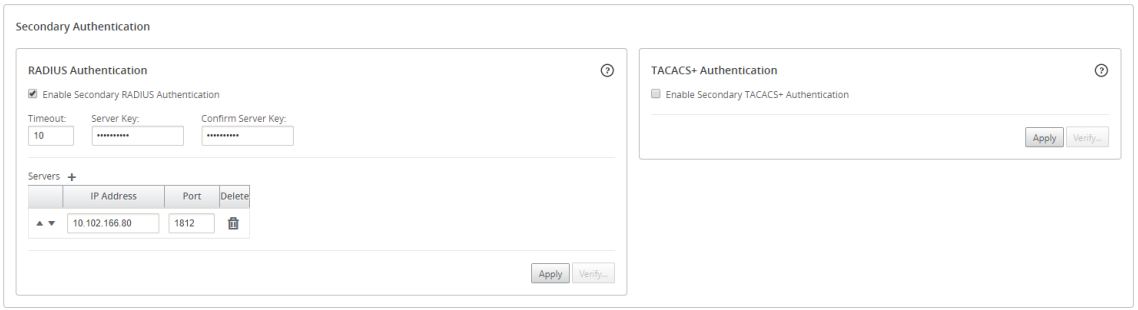
3. In the **Timeout** field, enter the time interval (in seconds) to wait for an authentication response from the RADIUS server.

   The timeout value should be less than or equal to 60 seconds.

4. In the **Server Key** field, enter a secret key to use when connecting to the RADIUS servers.
5. In the **Confirm Server Key** fields, reenter the secret key.

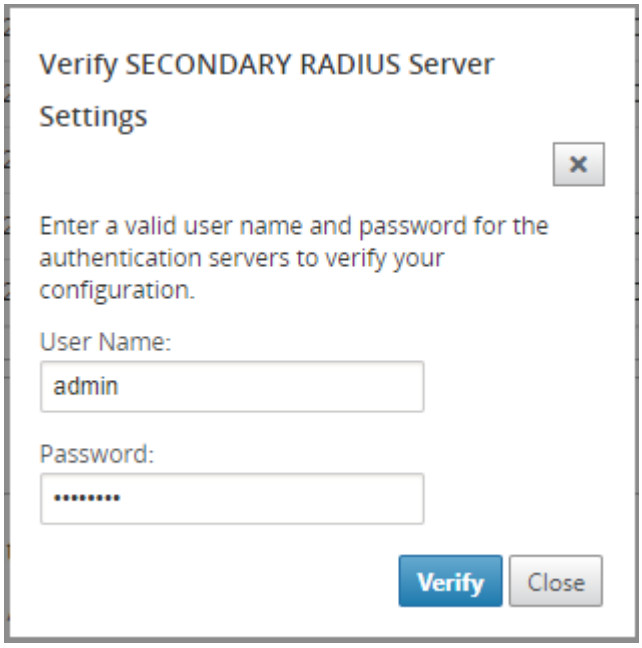
   > **Note**
   >
   > The **Timeout** and **Server Key** settings are applied to all configured servers**.**

6. Click the plus icon (+) next to **Servers** to add a RADIUS server.
7. In the **IP Address** field, enter the host IP address for the RADIUS server.
8. In the **Port** field, enter the port number for RADIUS server. The default port number is 1812.



9. Click **Apply**.
10. Click **Verify** to verify the connection to the RADIUS server. The **Verify Secondary RADIUS Server Settings** dialog box appears.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



11. Enter a valid username and password for the authentication servers, and click **Verify**.

To configure more servers, repeat the steps 6 through 11.

Secondary TACACS+ authentication server

To use TACACS+, you must specify and configure at least one TACACS+ server. Optionally, you configure redundant backup servers, up to a maximum of three TACACS+ servers. The servers are checked sequentially, starting with the server listed first in the **Servers** section. Ensure that the required user accounts are created on the TACACS+ authentication server.

To enable and configure TACACS+ authentication:

1. In the SD-WAN Center web interface, navigate to **Administration** > **User/Authentication Settings**.
2. In the **Secondary Authentication** > **TACACS+ Authentication**section, select the **Enable Secondary TACACS+ Authentication** check box.

   > **Note**
   >
   > If RADIUS authentication is already enabled, it gets disabled.

3. In the **Timeout** field, enter the time interval (in seconds) to wait for an authentication response from the TACACS+ server.

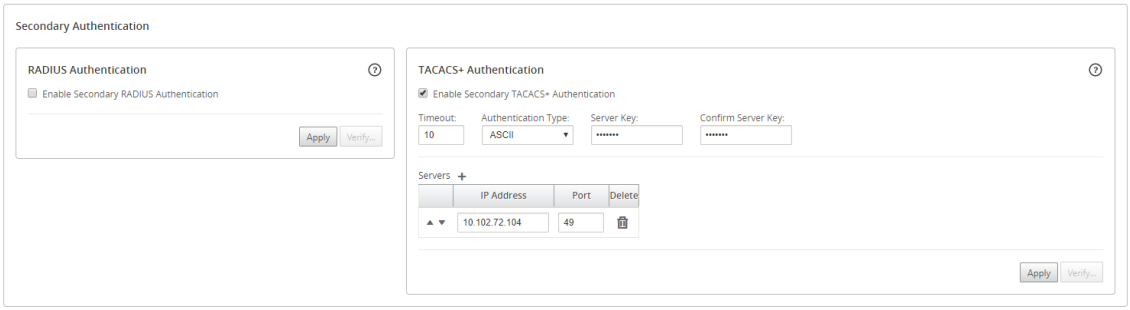
   The timeout value should be less than or equal to 60 seconds.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

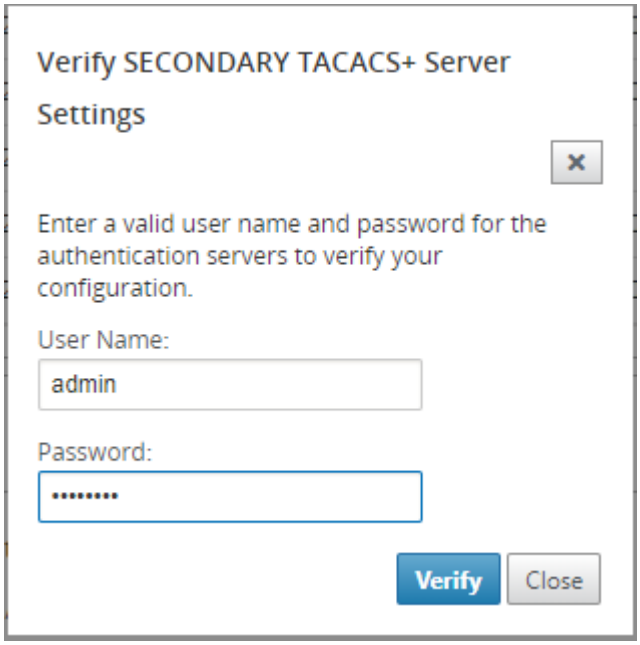
4. In the **Authentication Type** field, select the encryption method to use to send the username and password to the TACACS+ server.
5. In the **Server Key** field, enter a secret key to use when connecting to the TACACS+ servers.
6. In the **Confirm Server Key** fields, reenter the secret key.

> **Note**
>
> The **Timeout**, **Authentication Type**, and **Server Key settings** are applied to all the configured servers.

7. Click the plus icon (+) next to **Servers** to add a TACACS+ server.
8. In the **IP Address** field, enter the host IP address for the TACACS+ server.
9. In the **Port** field, enter the port number for TACACS+ server. The default port number is 49



10. Click **Apply**.
11. Click **Verify** to verify the connection to the RADIUS server. The **Verify TACACS+ Server Settings** dialog box appears.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

12. Enter a valid username and password for the authentication servers, and click **Verify**.

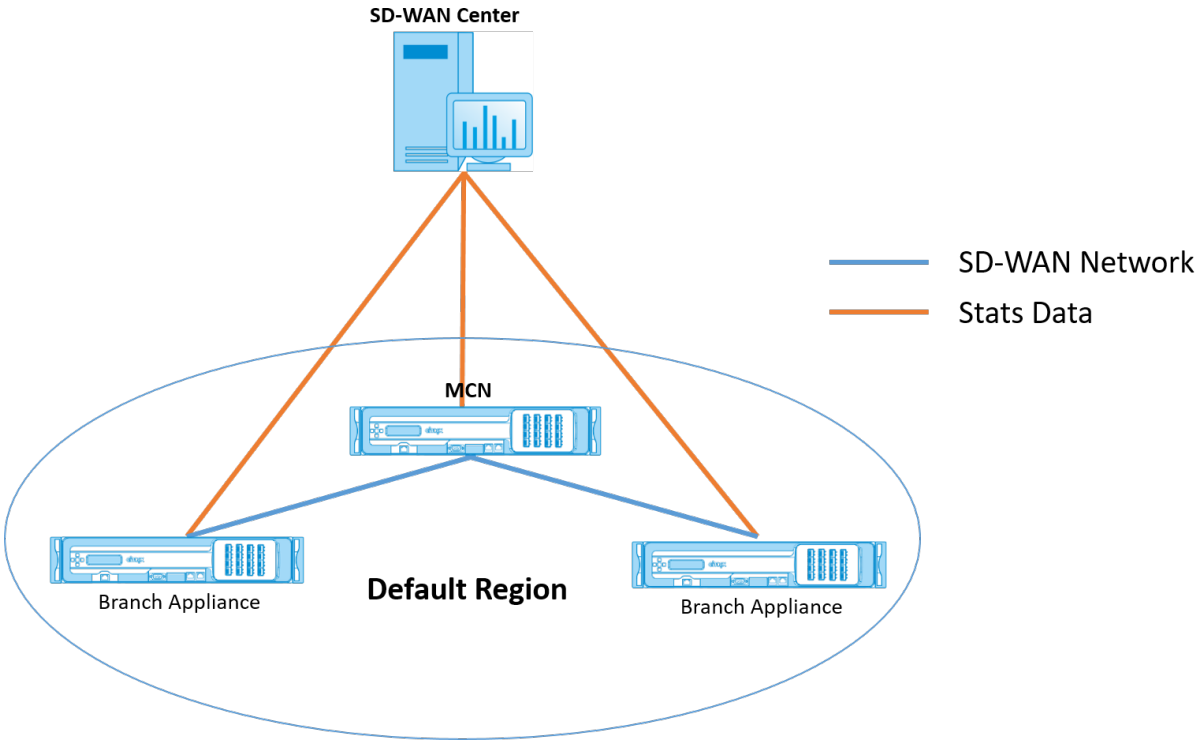
    To configure more servers, repeat the steps 7 through 12.

Single-region network deployment

March 12, 2021

If your organization has a small network spanning a single administrative (or geographical) boundary, you can use Citrix SD-WAN Center in the default mode (with single "default region"). A region can support a maximum of up to 550 sites.

A single region network has a Master Control Node (MCN) for centralized control, and Citrix SD-WAN Center for centralized management. The region associated with and controlled by the MCN is referred to as the default region. The Citrix SD-WAN Center polls the MCN and all the branch appliances in the default region.

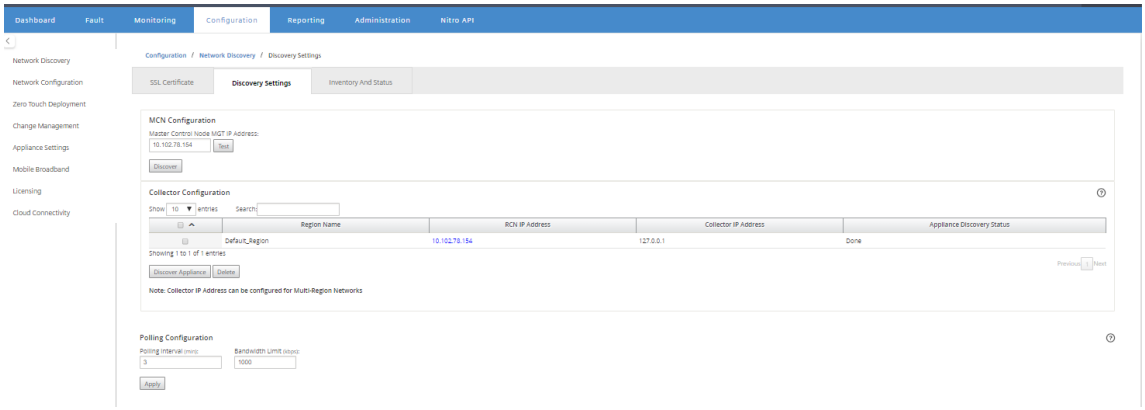


To deploy Citrix SD-WAN Center for single-region:

1. Download the Citrix SD-WAN Center Software. For more information, see System requirements and installation.
2. Install the Citrix SD-WAN Center on ESXi Server, XenServer, Hyper-V or Azure.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

3. Configuring the management interface settings. For more information, see Configure the management interface settings.
4. Generate, download and install the SD-WAN MCN SSL Certificate on the SD-WAN Center. For more information, see Install the Citrix SD-WAN SSL certificate.
5. Generate, download and install the SD-WAN Center SSL Certificate on the MCN appliance. For more information, see Install the Citrix SD-WAN Center SSL certificate.
6. In the Citrix SD-WAN Center GUI navigate to **Configuration** > **Network Discovery** > **Discover Settings.**
7. In the **Master Controller Node MGT IP Address** field, enter the MCN IP address and click **Test**. This establishes a connection between the MCN and Citrix SD-WAN Center.



8. Click **Discover**. If you have already discovered an MCN, this option changes to **Rediscover**.

   > **Note**
   >
   > The MCN must be active and the SD-WAN service should be enabled. For more information, see Enabling SD-WAN service.

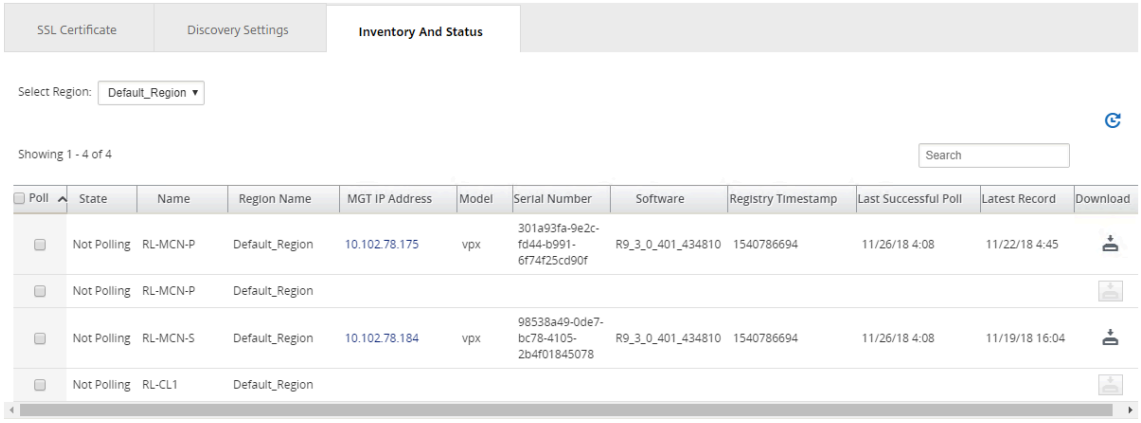
9. After the discovery operation completes, click the **Inventory and Status** tab.

   The **Inventory and Status** table displays the status information for all the discovered Citrix SD-WAN Appliances.

10. Select the **Poll** checkbox in the top left corner of the table heading.

    This selects the **Poll** checkbox for each appliance listed in the table. To exclude an appliance from the polling list, clear its check box.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



11. Click **Apply**.

> **Tip**
>
> You can increase the storage size of the Citrix SD-WAN Center by creating a data store on your virtual machine and switching the data store. For more information see, Switch the active storage to new data storage.

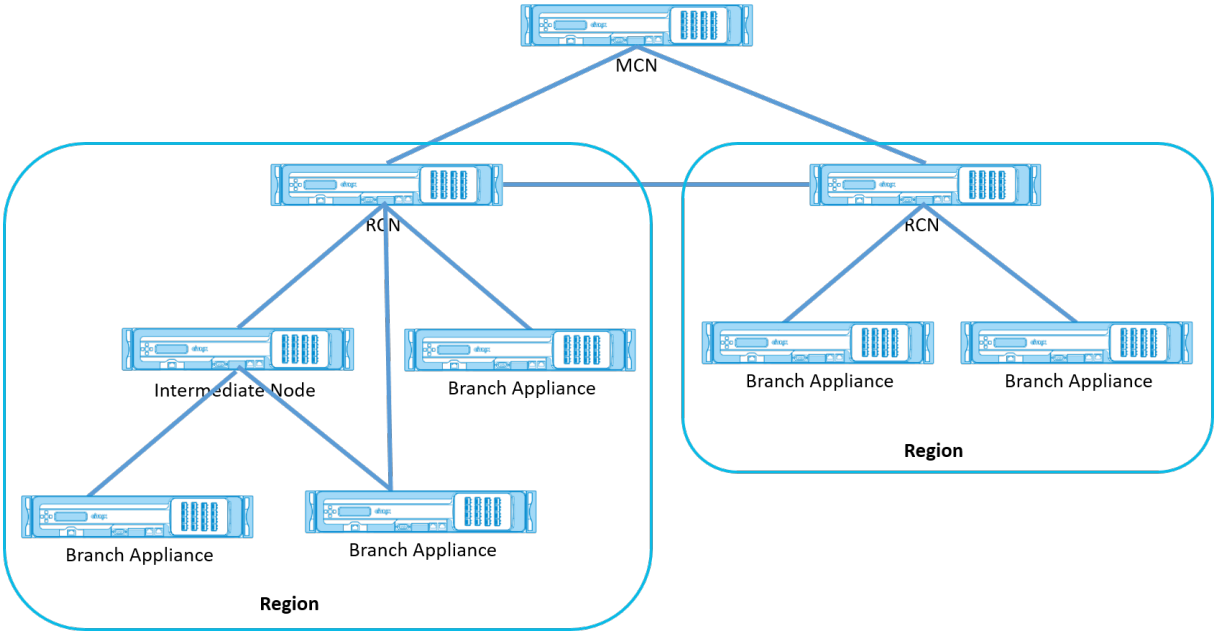
Multi-region network deployment

March 12, 2021

If your organization has a large network spanning multiple administrative (or geographical) boundaries, you can use Citrix SD-WAN Center in multi-region mode, with each region supporting a maximum of up to 550 sites.

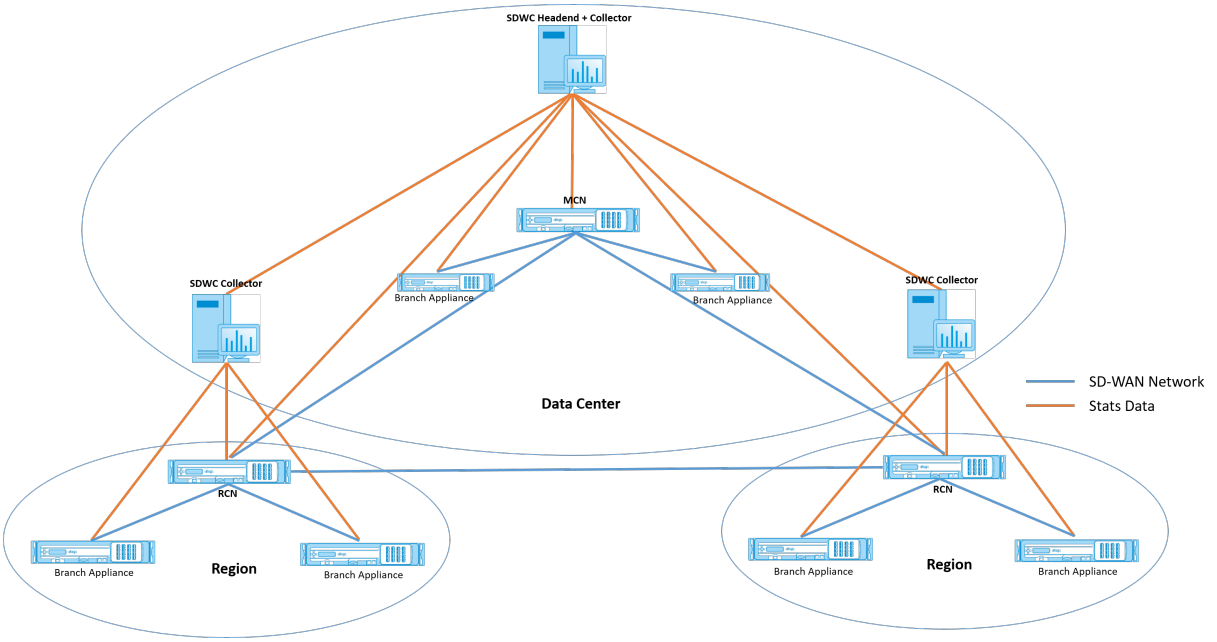
The multi-region network supports a hierarchical architecture with a Master Control Node (MCN) controlling multiple Regional Control Nodes (RCNs). Each RCN, in turn, controls multiple client sites. The MCN can also be optionally used to control some client sites directly as part of the “default region” . This hierarchical and distributed architecture enables higher scale, and effective delegation of regional administration.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



The Citrix SD-WAN Center polls the MCN, RCNs and all the associated branch appliances.

The multi-region Citrix SD-WAN Center architecture requires addition of a collector per region, to collect and store region level data and statistics. This distributed architecture enables higher scale across multiple regions, while preserving the "single pane of glass"view for managing the entire network.



> **Note**
>
> For a multi-region deployment, the default region statistics include statistics of all the sites managed by the MCN and the RCN. However, the RCN data is not stored on the SD-WAN Center collector. The SD-WAN Center collector obtains the RCN site data from the respective regional col-

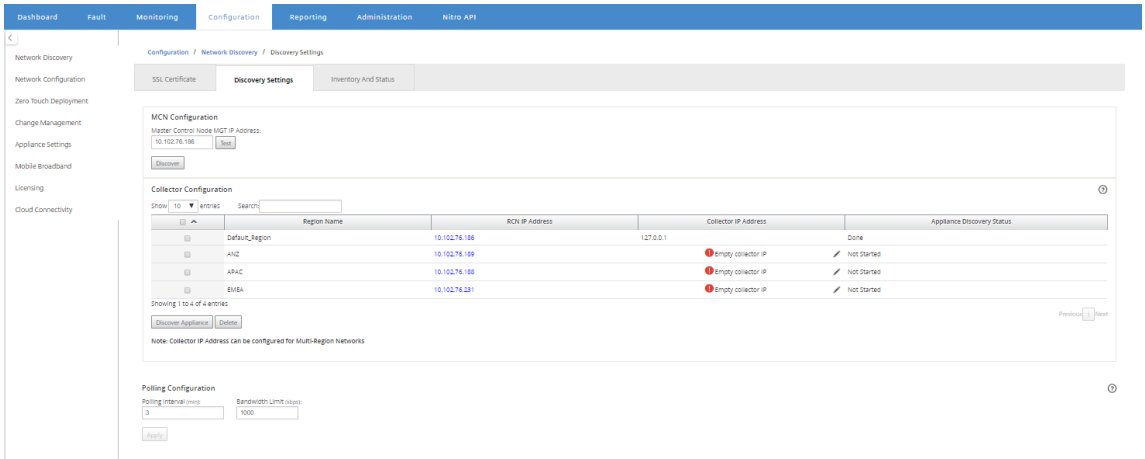
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> lectors.

To deploy Citrix SD-WAN Center for Multi-region:

1. Download the Citrix SD-WAN Center Software. For more information, see System requirements and installation.
2. Install the Citrix SD-WAN Center on ESXi Server, XenServer, Hyper-V or Azure.
3. Configuring the management interface settings. For more information, see Configure the management interface settings.
4. Generate, download and install the SD-WAN MCN SSL Certificate on the SD-WAN Center. For more information, see Install the Citrix SD-WAN SSL certificate.
5. Generate, download and install the SD-WAN Center SSL Certificate on the MCN appliance. For more information, see Install the Citrix SD-WAN Center SSL certificate.
6. In the Citrix SD-WAN Center GUI navigate to **Configuration** > **Network Discovery** > **Discover Settings.**
7. In the **Master Controller Node MGT IP Address** field, enter the MCN IP address and click **Test**. This establishes a connection between the MCN and Citrix SD-WAN Center.
8. Click **Discover**. A list of all the RCNs connected to the MCN appears in the **Collector Configuration** section. To discover the non default region sites, you need to have an active RCN with active paths to MCN.

   > **Note**
   >
   > The Citrix SD-WAN Center acts a collector for the default region.

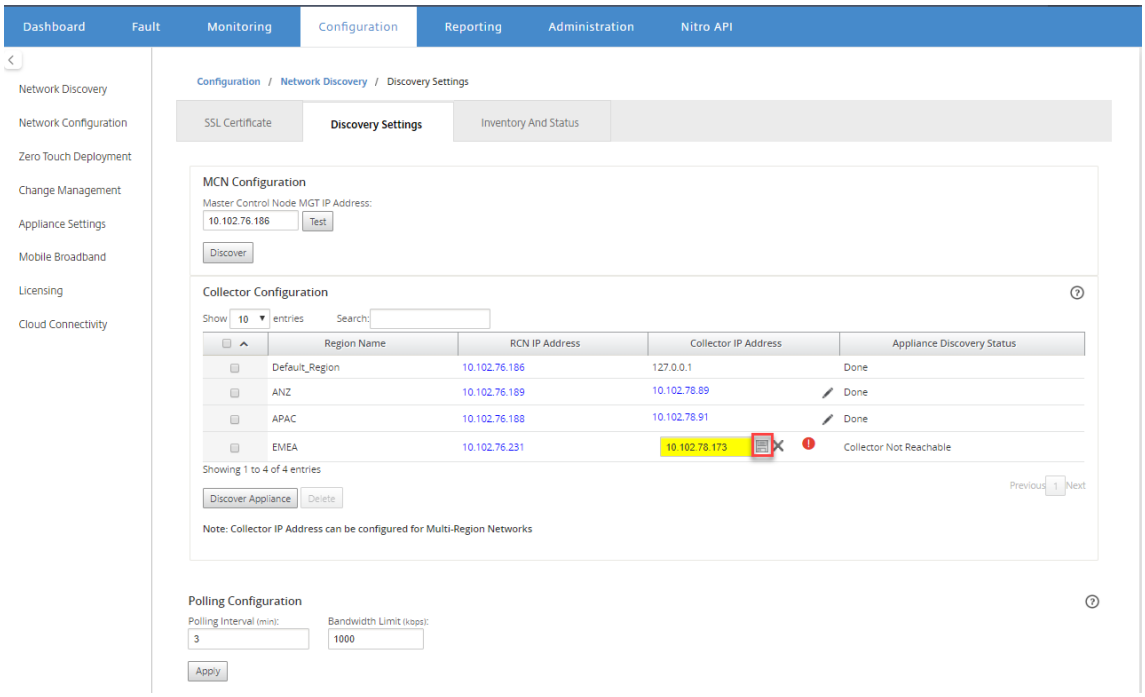


9. Click the edit icon and in the **Collector IP** field, enter the IP address of the Citrix SD-WAN Center that you want to configure as a collector for a region.

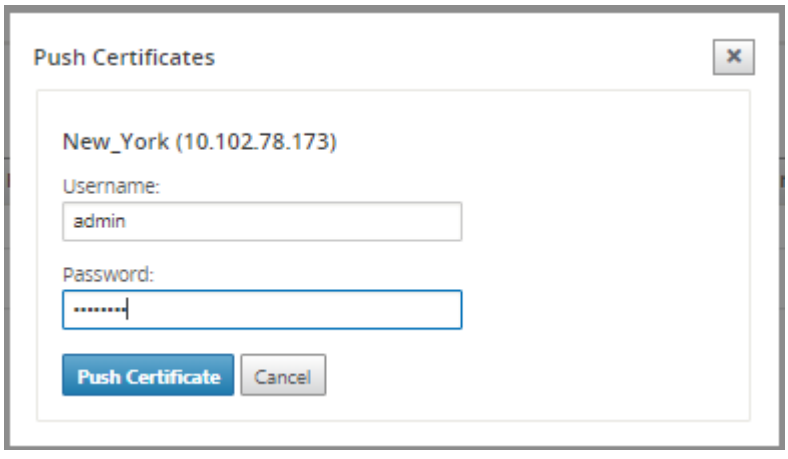
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> **Note**
>
> To set up a collector, install a Citrix SD-WAN Center VM and configure the management IP address. The management IP address of that Citrix SD-WAN Center is the collector IP address.

10. Click the Save icon to save the collector IP address and push the Certificate-Key pair to the RCN.



11. Enter the credentials for the RCN and click **Push Certificate**.

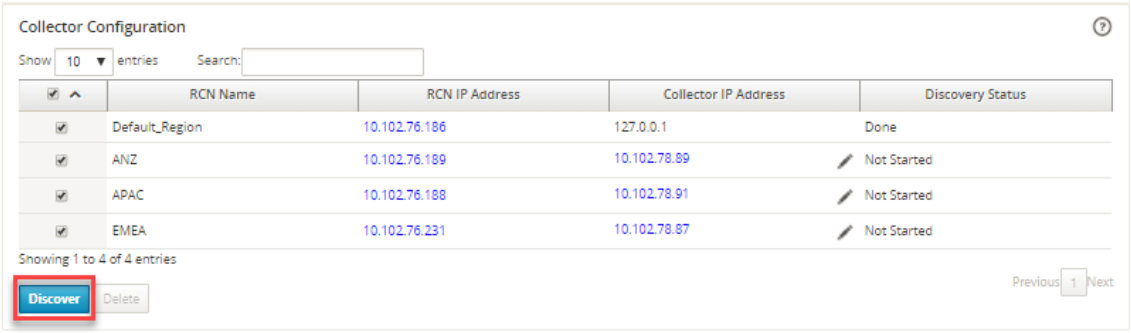


12. Similarly, configure collector IP address for all the RCNs.

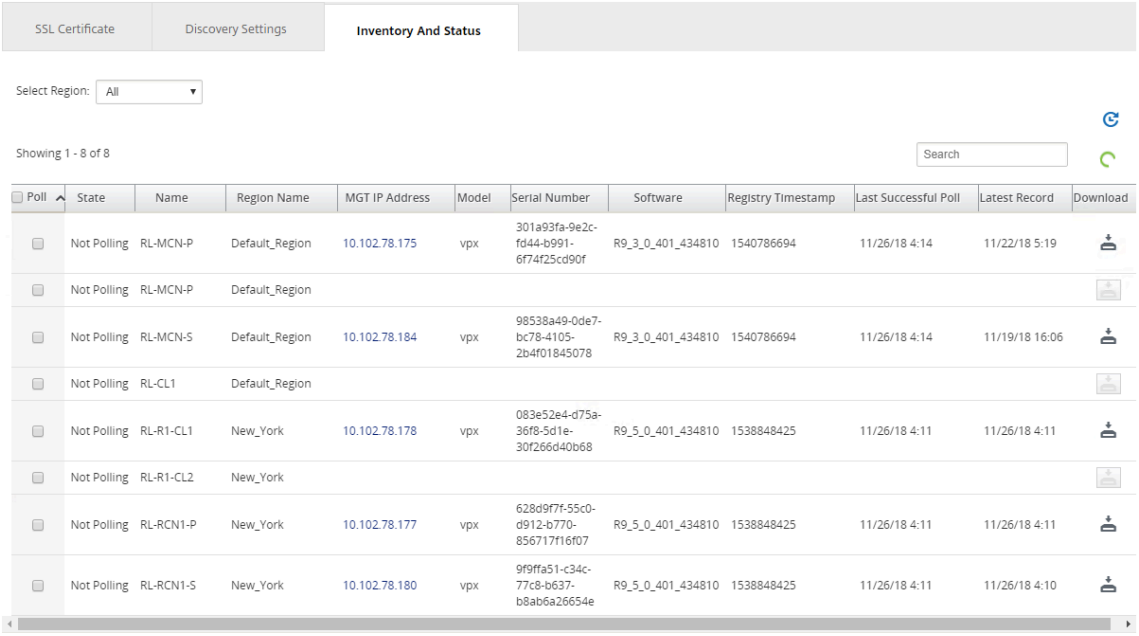
> **Note**
>
> The appliances are discovered automatically every 30 minutes. If new RCNs are added to

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> the network and a change management is done, you could select the appliance and click **Discover Appliance** to discover the appliance immediately.



After the **Discovery Status** changes to **Done**, you can view the discovered sites in the **Inventory and Status** Page.



> **Tip**
>
> You can filter the sites based on the region name. In the **Select Region** field, select the region.

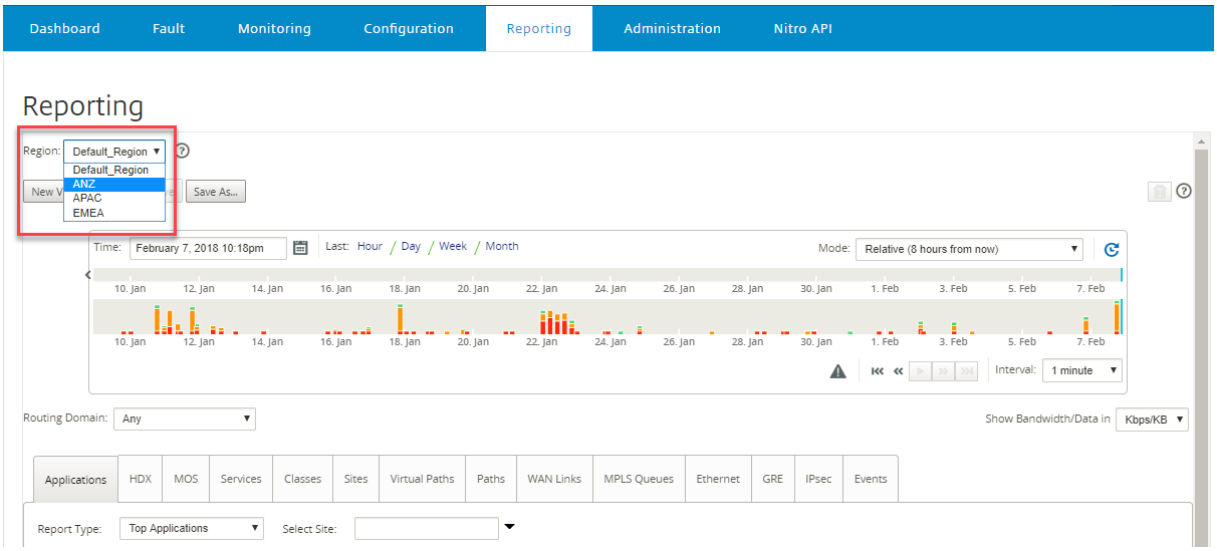
13. In the **Inventory and Status** Page, select the sites that you want to start polling and click **Apply**.

> **Tip**
>
> You can increase the storage size of the collector by creating a data store on your virtual machine. For more information see, Switching the active storage to new data storage.

You can select specific regions to view event and statistic reports.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

The events and statistic reports data is fetched from the respective region's collector.



Configuration

March 12, 2021

The initial few steps to configure Citrix SD-WAN Center is common for both single-region network and multi-region network. The following is a list of the common configuration procedures:

- Configure the management interface settings
- Install the Citrix SD-WAN Center certificates.
- Switch the activre storage to new data sorage.

Configure the management interface settings

March 12, 2021

You can use the Citrix SD-WAN Center web interface to configure the management interface settings.

The management Interface settings include the following:

- Citrix SD-WAN Center Management IP Address
- Gateway IP Address
- Subnet Mask
- Primary DNS

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- Secondary DNS

To configure the management interface settings:

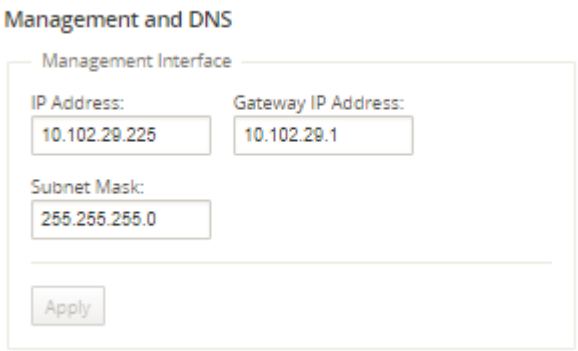
1. In the Citrix SD-WAN Center web interface, select the **Administration** tab.

   By default, the **User/Authentication Settings** page appears.

2. In the navigation tree, select **Global Settings**.
3. Configure the Management and DNS settings.

   In the **Management and DNS** section, add the required information to the following fields:

   - **IP Address**: Enter the IP Address for the Citirx SD-WAN Center.
   - **Gateway IP Address**: Enter the Gateway IP Address the Citrix SD-WAN Center VM will use to communicate with external networks.
   - **Subnet Mask**: Enter the subnet mask to define the network in which the Citrix SD-WAN Center VM resides.



4. Click **Apply**.

> **Note**
>
> Connectivity to the Citrix SD-WAN Center will be terminated when your changes are applied.

Install the SD-WAN Center SSL certificate

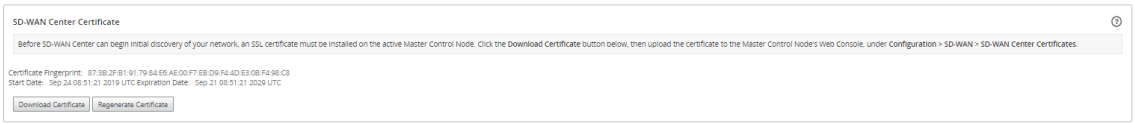
March 12, 2021

To establish connection between Citrix SD-WAN Center and Citrix SD-WAN Master Control Node (MCN), download the SSL certificate from the SD-WAN Center and install it on the MCN.

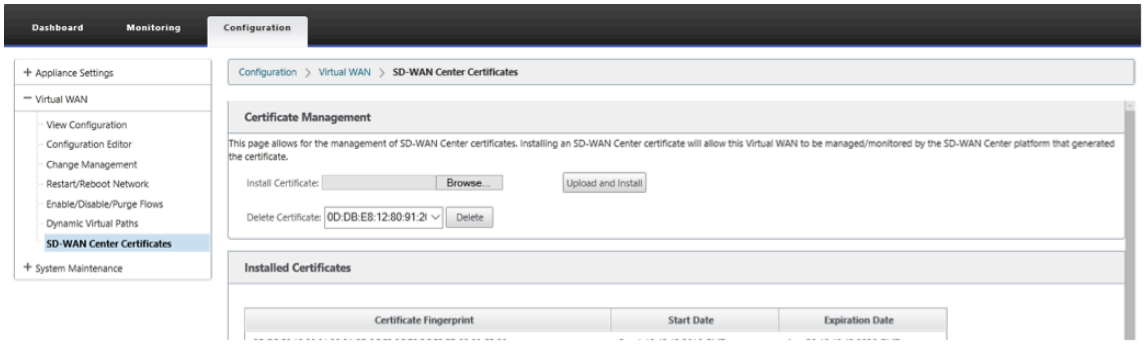
To generate and install the Citrix SD-WAN Center certificate:

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

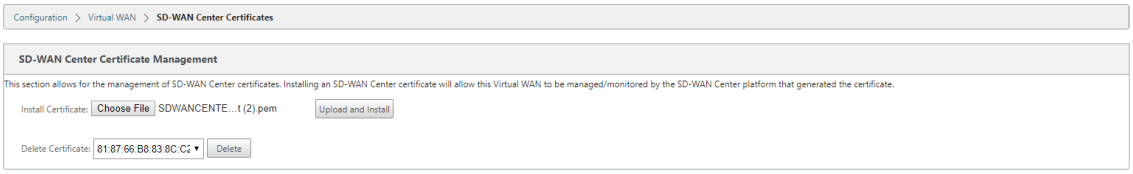
1. In the Citrix SD-WAN Center web interface, navigate to **Configuration** > **Network Discovery** > **SSL Certificate** > **SD-WAN Center Certificate**.
2. Click **Regenerate Certificate** to generate a new SSL certificate to establish communication with the MCN.



3. Click **Download Certificate**. Navigate to the desired location and save the certificate.
4. In the Citrix SD-WAN MCN web interface, navigate to **Configuration** > **Virtual WAN** > **SD-WAN Center Certificates** > **SD-WAN Center Certificate Management**.



5. Click **Choose File**, browse and select the downloaded SD-WAN Center SSL certificate.



6. Click **Upload and Install**, it uploads the SD-WAN center SSL certificate to the MCN and displays a success message when installation is complete.

Install the Citrix SD-WAN SSL certificate

March 12, 2021

To establish connection between Citrix SD-WAN MCN and Citrix SD-WAN Center, download the SSL certificate from the MCN SD-WAN appliance and install it on SD-WAN Center.

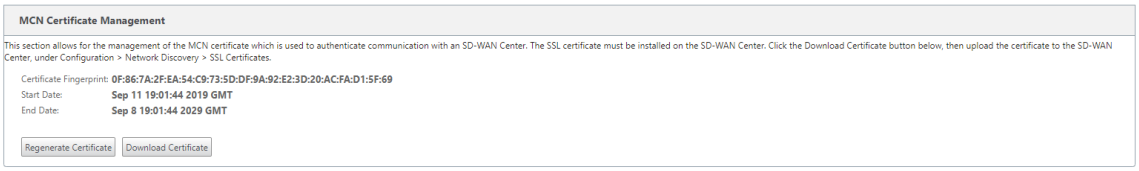
You can regenerate the appliance certificate on the MCN which replaces the pre-defined certificate and then install it on SD-WAN Center.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Installing the appliance certificate to the SD-WAN Center is mandatory for new deployments and for SSL communication to work. MCN generates a network certificate and distributes the certificate with a private key through the certificate manager to all nodes. The certificates are used by each branch to authenticate the SD-WAN Center.

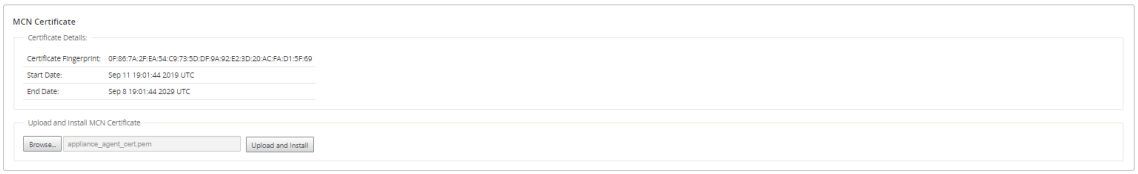
To generate and install the SD-WANcertificate:

1. In the MCN SD-WAN appliance, navigate to **Configuration** > **Virtual WAN** > **SD-WAN Center Certificates**> **MCN Certificate Management**.
2. Click **Regenerate Certificate** to generate a new SSL certificate to establish communication with SD-WAN Center.

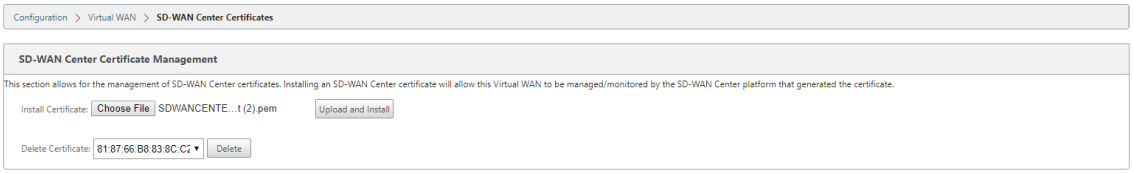


> **Note:**
>
> When you regenerate the SSL certificate, the SD-WAN appliance uses the new certificate immediately for communication with discovered SD-WAN Center. However, communication with the appliances is not established, until you download and install the newly generated certificate on SD-WAN Center.

3. Click **Download Certificate**. Navigate to the desired location and save the certificate.
4. In the Citrix SD-WAN Center web interface, navigate to **Configuration** > **SSL Certificate** > **MCN Certificate**.



5. Click **Browse** and select the downloaded MCN SSL certificate.



6. Click **Upload and Install**, it uploads the MCN SSL certificate to SD-WAN Center.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Switch the active storage to new data storage

March 12, 2021

In Citrix SD-WAN Center, you can switch the active storage to the data store you created on your virtual server. This allows you to store more statistics data obtained by polling all the Citrix SD-WAN appliances in the WAN. For information on creating a datastore on ESXi server, see Adding and Configuring the Datastore on ESXi Server. For information on creating a datastore on XenServer, see Adding and Configuring the Data Storage on XenServer

To specify the active storage for the Citrix SD-WAN Center VM:

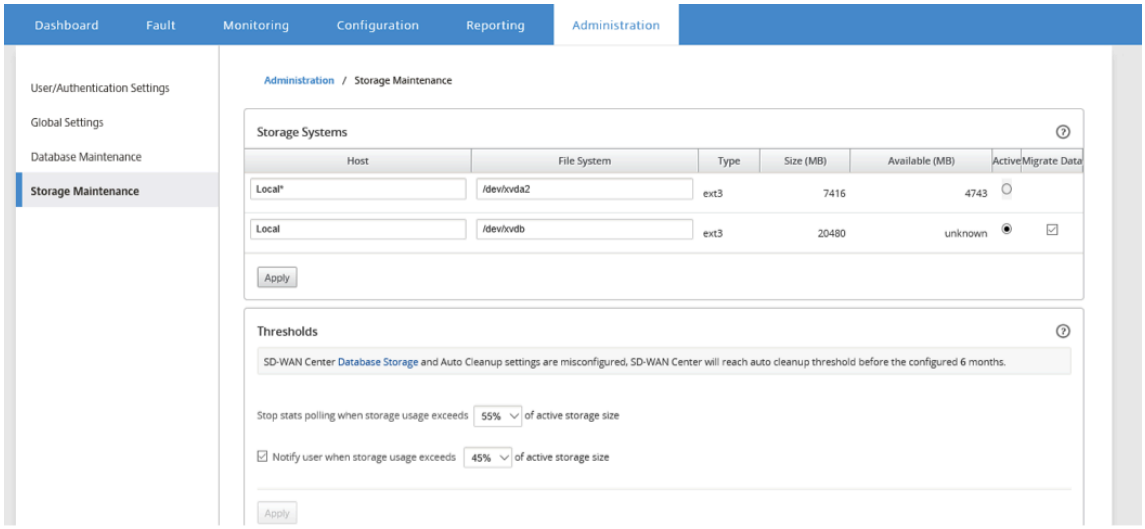
1. Log into Citrix SD-WAN Center VM.

   The default login credentials for Citrix SD-WAN Center are as follows:

   Login: admin

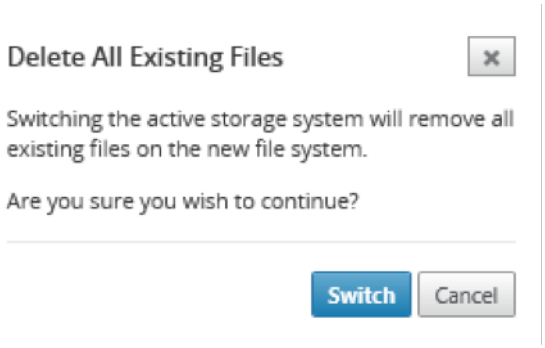
   Password: password

2. Click the **Administration** tab and then click **Storage Maintenance**.



3. In the **Active** column of the Storage Systems table, select the storage you created.
4. Select **Migrate Data** and click **Apply**.
5. The **Delete All Existing Files** message appears, click **Switch**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



This places Citrix SD-WAN Center into **Maintenance Mode** and displays a progress bar in the main page area.

6. When the activation completes, click **Continue**.

   This dismisses the progress bar and returns to the main **Storage Maintenance** page.

Deploy Citrix SD-WAN appliance

March 12, 2021

You can use Citrix SD-WAN Center to create the appliance configuration or appliance settings file and use the change management wizard to push the configuration to the appliances on the network. For more information, see Configure Citrix SD-WAN appliances.

You can configure Citrix SD-WAN Center to act as the central licensing server and provides licensing services to all the nodes in the network. This eliminates the need to install licenses on individual nodes locally. For more information, see Citrix SD-WAN Center as a license server.

You can use Citrix SD-WAN Center to streamline the process of deploying the SD-WAN applainces at branch offices using the Zero Touch Deployment feature. For more information, see Zero Touch Deployment.

Configure Citrix SD-WAN appliances

March 12, 2021

Use the Configuration Editor to edit the configuration settings and to export the configuration package to the MCN. For more information see, Configuration Editor.

You can use the change management wizard of the MCN appliance through Citrix SD-WAN Center. For more information see, Change Management Wizard.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

You can configure appliance setting on Citrix SD-WAN Center and export it to a set of managed Citrix SD-WAN appliances in your SD-WAN network. For more information see, Appliance settings.

Configuration Editor

March 12, 2021

The Configuration Editor is available as a component of the Citrix SD-WAN Center Web Interface, and in the Citrix SD-WAN Management Web Interface running on the Master Control Node (MCN) of the SD-WAN network.

> **Note**
>
> You cannot push configurations to the discovered appliances directly from Citrix SD-WAN Center. You can use the Configuration Editor to edit the configuration settings and to create a configuration package. When the configuration package has been created, you can export it to the MCN and install it. The changes are then reflected in the MCN.
>
> You have to log on with administrative rights to the Citrix SD-WAN Center appliance and the MCN, to edit the configurations on Citrix SD-WAN center and to export and install the configurations on the MCN.

For detailed instructions on using the Configuration Editor to configure your Citrix SD-WAN, see Citrix SD-WAN 10.1 documentation.

The Configuration Editor enables you to do the following:

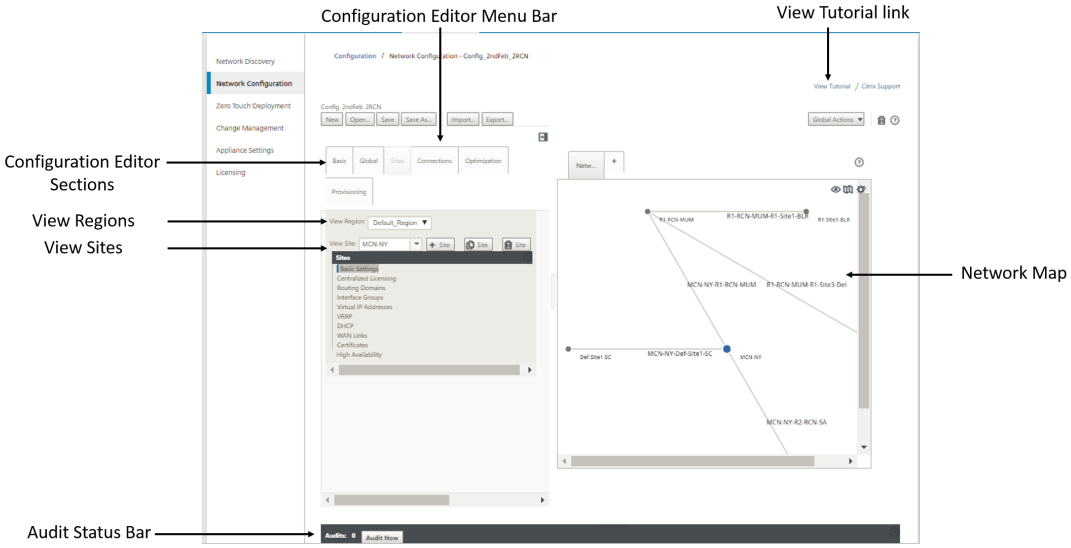
- Add and configure Citrix SD-WAN Appliance sites and connections.
- Provision the Citrix SD-WAN appliance.
- Create and define Citrix SD-WAN Configuration.
- Define and view Network Maps of your SD-WAN system.

To open the Configuration Editor:

1. In the Citrix SD-WAN Center web interface, click the **Configuration** tab.
2. Click **Network Configuration**.

   The below figure outlines the basic navigation and page elements of the **Configuration Editor**, and the terminology used in this guide to identify them.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



The primary screen of the Configuration Editor has the following navigation elements:

- **Configuration Editor Menu Bar**: Contains the primary activity buttons for Configuration Editor operations. In addition, at the far right edge of the menu bar is the **View Tutorial** link button for initiating the Configuration Editor tutorial. The tutorial walks you through a series of bubble descriptions for each element of the Configuration Editor display.
- **Configuration Editor Sections** : Each tab represents a top-level section. There are six sections: **Basic**, **Global**, **Sites**, **Connections**, **Optimization** and **Provisioning**. Click a section tab to reveal the configuration tree for that section.
- **View Region**: For multi-region deployment, it lists all the regions configured. For single-region deployment, the default-region is displayed by default. To view the sites in a region, select a region from the drop-down list.
- **View Sites:** Lists the site nodes that have been added to the configuration and are currently opened in the Configuration Editor. To view the site configuration, select a site from the frop-down list.
- **Network Map:** Provides a schematic view of the SD-WAN network. Hover the mouse cursor over the sites or the path to view more details. Click the sites to view report options.
- **Audit Status Bar**: The dark grey bar at the bottom of the Configuration Editor page, and spanning the entire width of the Configuration Editor page. The **Audits** status bar is available only when the **Configuration Editor** is open. An Audit Alert icon (red dot or goldenrod delta) at the far left of the status bar indicates one or more errors present in the currently opened configuration. Click the status bar to display a complete list of all unresolved audit alerts for that configuration.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Change Management Wizard

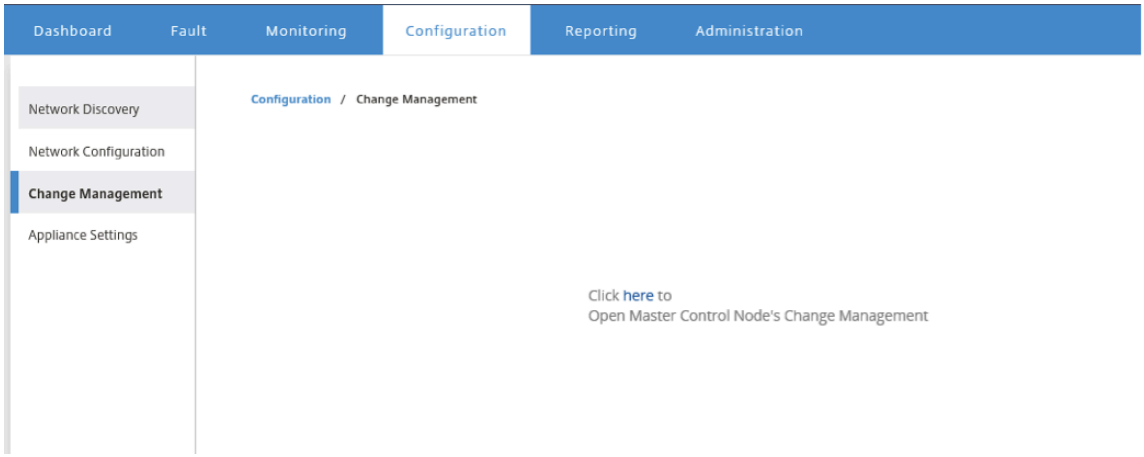
March 12, 2021

The Change Management wizard guides you through the process of uploading, downloading, staging, and activating the Citrix SD-WAN software and configuration on the Master Control Node (MCN) appliance and client appliances.

The Change Management wizard is a component of the Citrix SD-WAN Management Web Interface running on the MCN, and is not part of the Citrix SD-WAN Center. However, you can use the Citrix SD-WAN Center to connect to the specified MCN, and access the Change Management wizard.

To open the Change Management Wizard:

1. In the Citrix SD-WAN Center web interface, click the **Configuration** tab.
2. Click **Change Management**.



3. At the **Click here to Open Master Control Node's Change Management** prompt, click the **here** link.

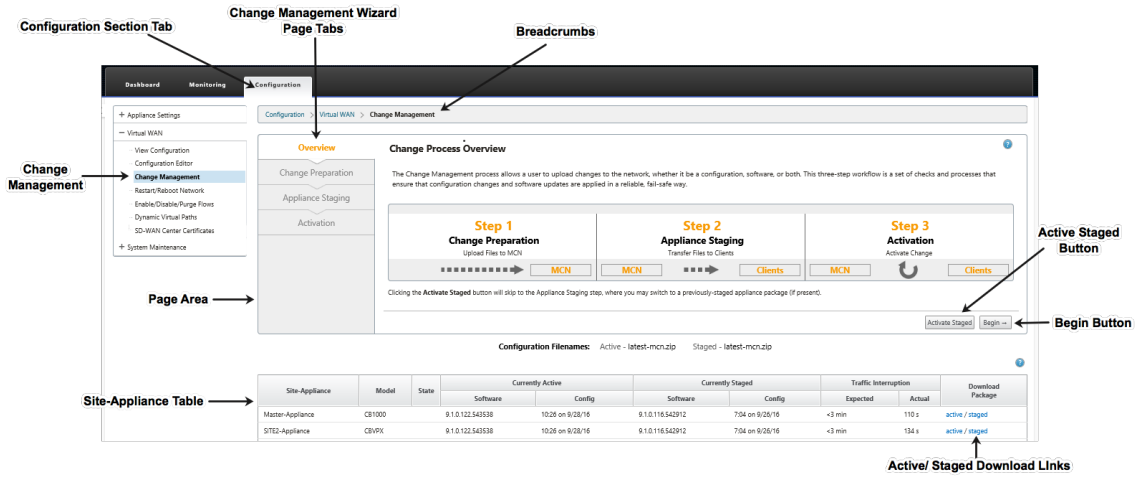
   You will be automatically logged in into the MCN GUI.

   > **Note**
   >
   > You do not have to login into the MCN GUI using the MCN credentials, the auto-login feature enables single sign on.

4. In the MCN management web interface, click the **Configuration** tab.
5. In the navigation tree (left pane), click **+** next to the **Virtual WAN** branch to expand that branch.
6. Click **Change Management**.

   This displays the first page of the **Change Management** wizard, the **Change Process Overview** page, as shown in the figure below.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



7. To start the wizard, click **Begin**.

> **Note**
>
> For complete instructions on using the wizard to upload, stage, and activate the SD-WAN software and configuration on the appliances, please see the SD-WAN 9.1.0 User Guide.

The **Change Management** wizard has the following navigation elements:

- **Page area**: Displays the forms, tables, and activity buttons for each page of the **Change Management** wizard.
- **Change Management wizard page tabs**: On the left side of the page area, on each page of the wizard, tabs are listed in the order in which the corresponding steps occur in the wizard process. When a tab is active, you can click it to return to a previous page in the wizard. An active tab displays its name displays in a blue font. A gray font indicates an inactive tab. Tabs are inactive until all dependencies (previous steps) have been fulfilled without error.
- **Appliance-Site table**: At the bottom of the wizard page area, this table contains information about each configured appliance site, and links for downloading the active or staged appliance packages for that appliance model and site. A package in this context is a zip-file bundle containing the appropriate SD-WAN software package for that appliance model, and the specified configuration package. The Configuration Filenames section above the table shows the package name for the current active and staged packages on the local appliance.
- **Active/Staged download links**: In the **Download Package** field (far right column) of each entry in the **Appliance-Site** table, you can click a link in an entry to download the active or staged package for that appliance's site.
- **Begin button**: Click **Begin** to initiate the **Change Management** wizard process and proceed to the **Change Preparation** tab page.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- **Activate Staged button**: If this is not an initial deployment, and you want to activate the currently staged configuration, you have the option of proceeding directly to the **Activation** step. Click **Activate Staged** to proceed directly to the **Activation** page and initiate activation of the currently staged configuration.

Appliance settings

March 12, 2021

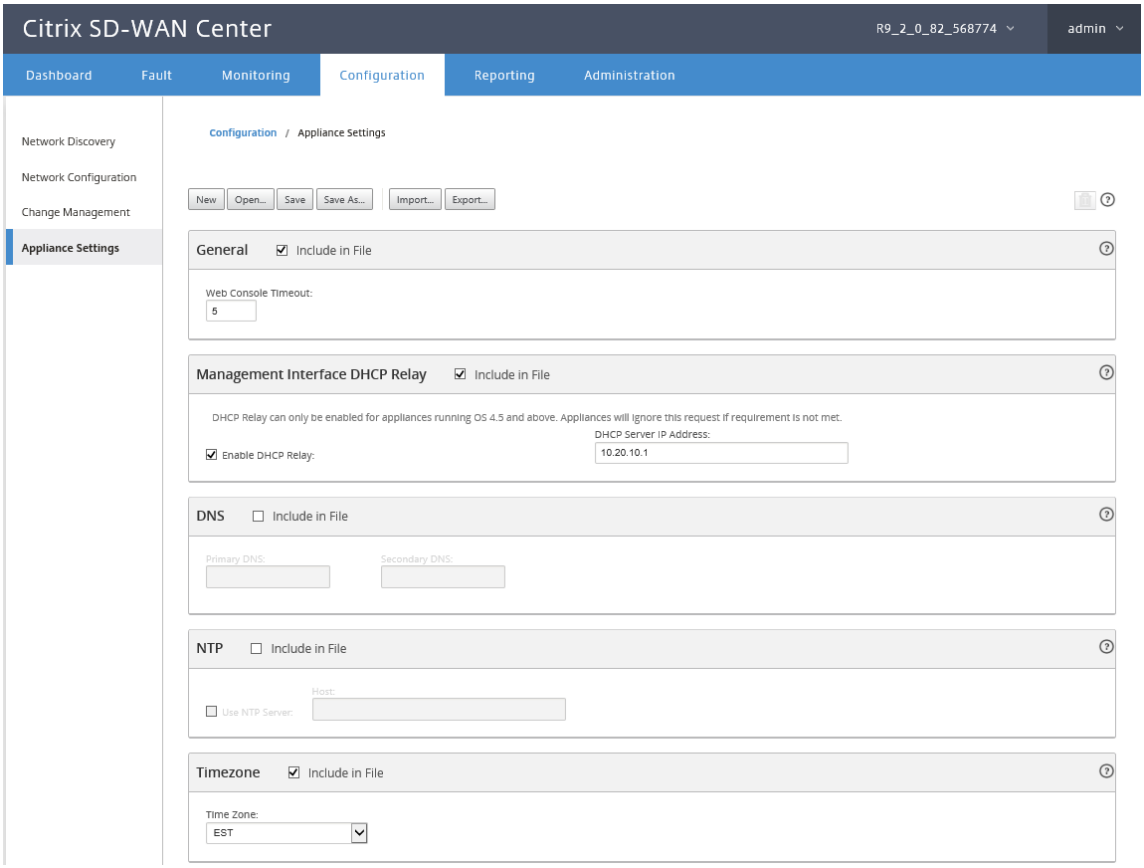
You can configure appliance setting on Citrix SD-WAN Center and export it to a set of managed Citrix SD-WAN appliances in your SD-WAN network. The **Appliance Settings** page allows you to perform the following actions:

- Create a new appliance settings file.
- Open and edit an existing appliance settings file.
- Import an appliance settings file from your local computer.
- Download an appliance settings file to your local computer.
- Export an appliance settings file to the managed appliances.

To create an appliance settings file and export it to managed appliances:

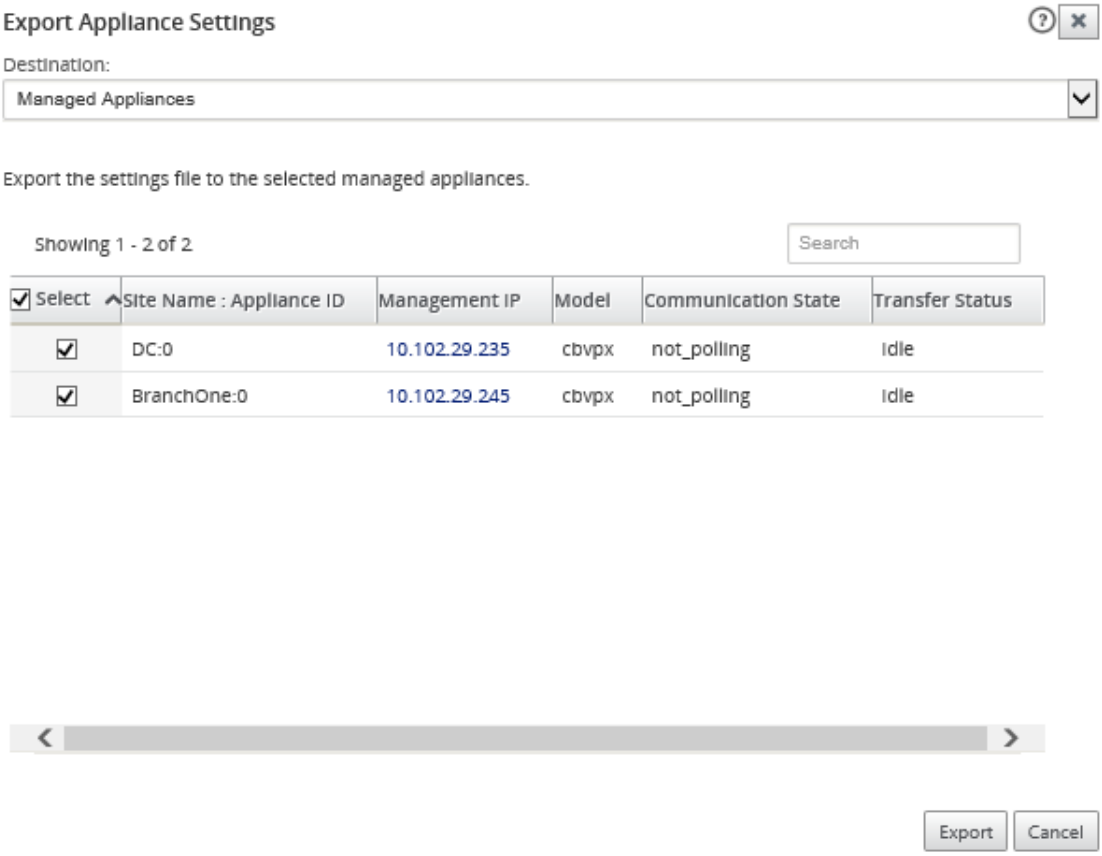
1. In the Citrix SD-WAN Center web interface, click the **Configuration** tab.
2. Click **Appliance Settings** and then click **New**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



3. Select **Include in file** for the required settings and specify the parameter values for the settings. For more information, see appliance settings table.
4. Click **Export**. In the **Save as** dialog box, enter a name for the appliance settings file and click **Save**. The **Export Appliance Settings** dialog box appears.
5. In the **Destination** field select **Managed Appliances** and select the appliances for which you want to export the appliance settings to.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



> **Note**
>
> To download the appliance settings to your local computer, in the **Destination** field select **File Download**.

6. Click **Export**.

Remote LTE site management

July 16, 2021

Citrix SD-WAN Center allows you to remotely view and manage all the LTE sites in your network. It includes appliances connected through an internal LTE modem or external USB LTE modem.

The Citrix SD-WAN appliances such as Citrix SD-WAN 210 SE LTE and 110 LTE Wi-Fi appliances have a built-in internal LTE modem. You can also connect an external 3G/4G USB modem on the following Citrix SD-WAN appliances.

- Citrix SD-WAN 210 SE

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- Citrix SD-WAN 210 SE LTE
- Citrix SD-WAN 110 SE
- Citrix SD-WAN 110 LTE Wi-Fi SE

CDC Ethernet, MBIM, and NCM are the three types of external USB modems supported. You can configure the APN settings and Enable/Disable modem through the new Citrix SD-WAN GUI and Citrix SD-WAN Center. Mobile broadband operations are not supported on CDC Ethernet USB modems.

Perquisites for external LTE modem:

- Use the supported USB LTE dongles. The supported dongle hardware models are Verizon USB730L and AT&T USB800.
- Ensure that a SIM card is inserted into the USB LTE dongle. The CDC Ethernet LTE dongles are pre-configured with a static IP address, this interferes with the configuration and cause connection failure or intermittent connection, if the SIM card is not inserted.
- Before inserting a CDC Ethernet LTE dongle into the SD-WAN appliance, connect the external USB stick to a Windows/Linux machine and ensure that the internet is working properly with proper APN and Mobile Data Roaming configuration. Ensure that the Connection mode of the USB dongle is changed from the default value Manual to Auto.

> **Note**
>
> - The Citrix SD-WAN appliances support only one USB LTE dongle at a time. If more than one USB dongle is plugged in, unplug all the dongles and plug in only one dongle.
> - The Citrix SD-WAN appliances do not support user name and password for USB modems. Ensure that the user name and password feature is disabled on the modem during setup.
> - Un-plugging or rebooting an external MBIM dongle impacts the internal LTE modem data session. This is an expected behaviour.
> - When an external LTE modem is plugged-in, the SD-WAN appliance takes about 3 minutes to recognize it.

Operations that are supported on internal and external modems:

Operations	Internal modem	External modem - CDC Ethernet	External modem - MBIM and NCM
SIM preference	Yes - For appliances that support dual SIM	No	No
SIM PIN	Yes	No	No
APN settings	Yes	No	Yes
Network settings	Yes	No	No
Roaming	Yes	No	No

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

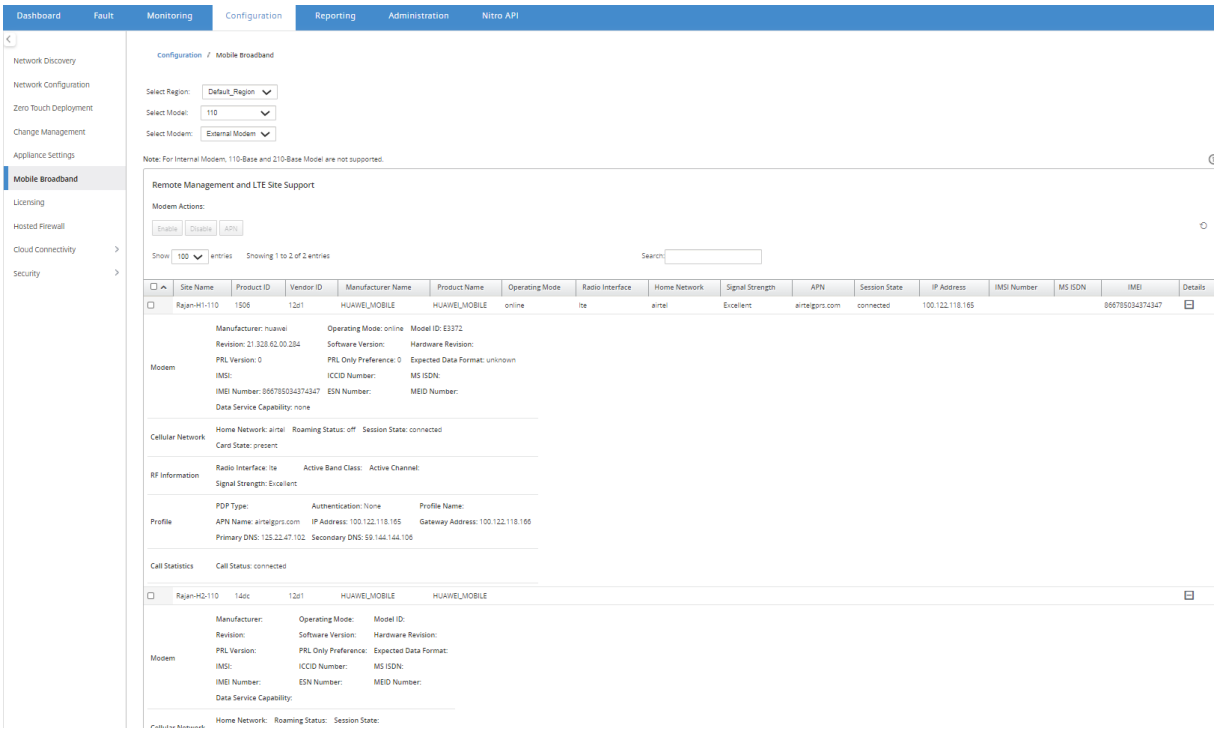
Operations	Internal modem	External modem - CDC Ethernet	External modem - MBIM and NCM
Manage firmware	Yes	No	No
Enable/Disable modem	Yes	No	Yes
Reboot modem	Yes	No	No
Refresh SIM	Yes	No	No

To remotely manage the LTE sites in your network, in the SD-WAN Center UI, navigate to **Configuration > Mobile Broadband**. All the LTE appliances, across sites, managed by the SD-WAN Center is listed here.

For a multi-region deployment, you can select a region for which you want to manage the LTE sites. The Default_Region is selected by default.

You can also select the LTE appliance model and modem type.

To list out the appliances using an external modem, navigate to **Configuration** > **Mobile Broadband**. Select **External Modem** as the modem type.



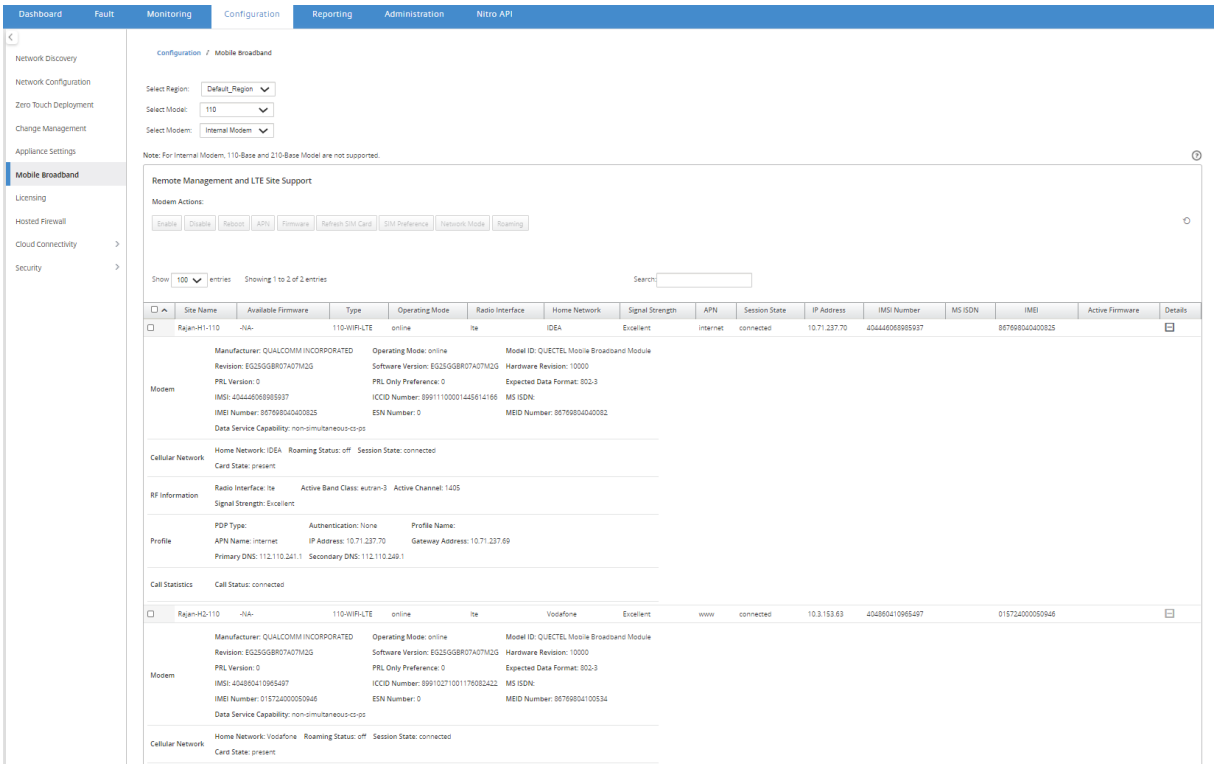
> **Note**
>
> The SIM PIN and other LTE modem configurations are currently not supported for external

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> modems.

To list out the appliances using an internal modem, navigate to **Configuration** > **Mobile Broadband**. Select **Internal Modem** as the modem type.

> **Note**
>
> The LTE operations are different for different LTE models.



You can select either a single appliance or multiple appliances to perform the following LTE modem operation:

- **Enable**: Enable the modem at the selected sites.
- **Disable**: Disable the modem at the selected sites.
- **Reboot**: Reboot the modem at the selected sites.
- **APN**: Configure the APN settings for the selected sites. For more information, see Configure APN settings.
- **Firmware**: This option is applicable for 210 LTE appliance only. Browse and select the required firmware. You can choose to upload only or upload and apply the firmware file on the selected sites. From the list of available firmware you can choose to apply it or delete it.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> **Note**
>
> In multi-region deployment, the firmware operations for non-default region sites cannot be done from the SD-WAN Center Headend. You can perform Firmware operations from the specific region's Collector SD-WAN Center.

- **Refresh SIM card**: Refresh the SIM card by turning it OFF and turning it back ON at the selected sites. This operation is performed to detect the new SIM card inserted into the 210 SE LTE modem.
- **SIM Preference**: This option is applicable for the 110 LTE appliance only. The 110 LTE appliance support dual SIM and you can set the SIM preference.
- **Network Mode**: You can select the mobile network on Citrix SD-WAN appliances that support internal LTE modem. The supported networks are 3G, 4G, or both. For 110 LTE appliances, select the SIM on which to apply the changes.
- **Roaming**: The roaming option is enabled by default on your LTE appliances, you can choose to disable it. For 110 LTE appliances, select the SIM on which to apply the changes.

You can also configure LTE functionality on individual LTE appliances. For more information, see Configure LTE functionality on 210 SE LTE.

For information about configuring a 110-LTE-WIFI appliance, see Configure LTE functionality on 110 LTE Wi-Fi.

APN settings

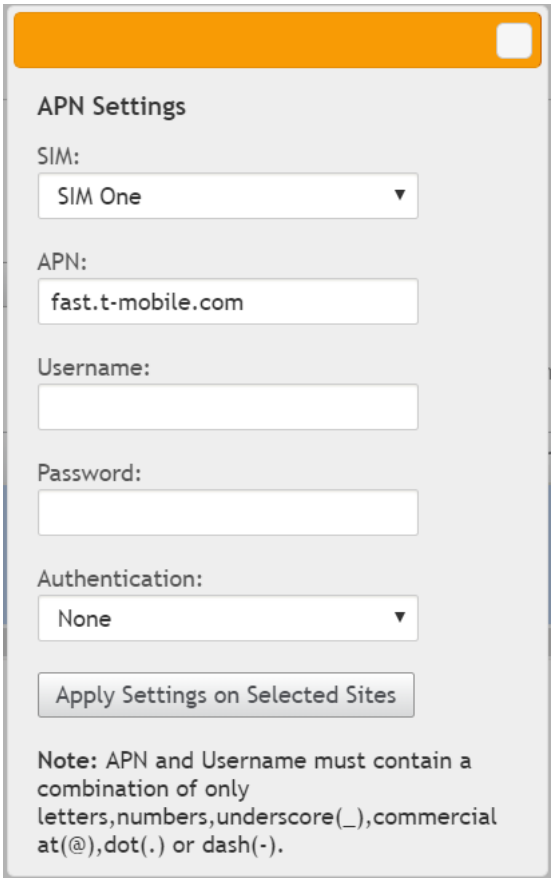
APN is the name of the settings your appliance reads to set up a connection to the gateway between the carrier's cellular network and the public internet. You can obtain the APN information from the carrier and remotely configure the **APN** settings on one or more LTE appliances.

> **Note**
>
> APN settings vary from carrier to carrier.

To configure APN settings:

1. In the SD-WAN Center UI navigate to **Configuration > Mobile Broadband**. Select the LTE sites for which you want to configure APN settings and click **APN**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



2. For a 110 LTE appliance, select the SIM on which the APN settings is applied.
3. Enter the **APN name**, **Username**, **Password**, and **Authentication** provided by the carrier. You can choose from PAP, CHAP, PAPCHAP authentication protocols. If the carrier has not provided any authentication type, set it to **None**.
4. Click **Apply Settings on Selected Sites**.

Citrix SD-WAN Center as a license server

March 12, 2021

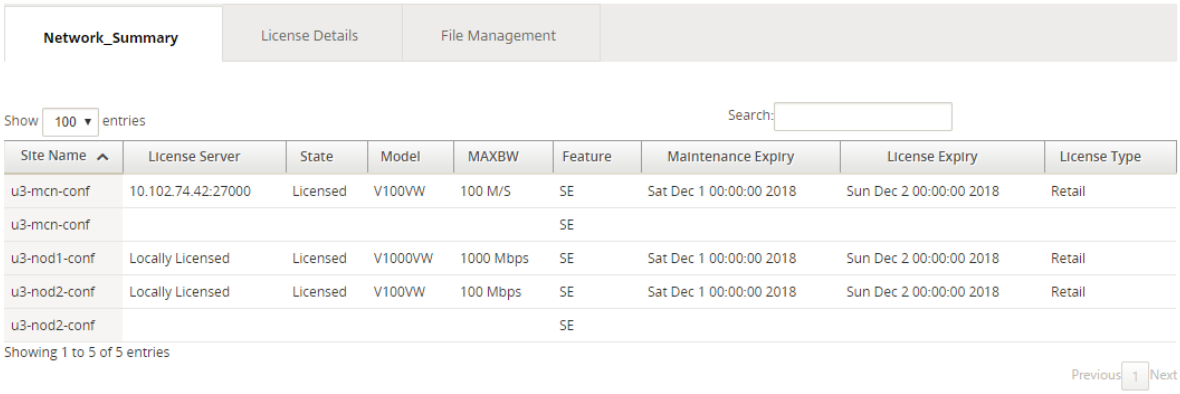
You can acquire the licenses for the appliances in your network, upload and install it in SD-WAN Center. To use SD-WAN Center as the remote license server, configure the IP address of SD-WAN Center as the remote server for centralized license management. For more information see, Centralized License Management.

After you push the network configuration to the sites through the change management process, and once the configuration is activated, the branch appliances automatically obtain the licenses from the

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

SD-WAN Center.
For these licenses to be used one must assign the licenses to the host of the SD-WAN Center itself.

To view the license details of all the appliances discovered by SD-WAN Center navigate to **Configuration** > **Licensing** > **Network Summary.**



The following parameters are displayed:

- **Site Name**: The name of the Site.
- **License Server**: The IP Address and port number of the license server. If the license was installed locally on the appliance, it is displayed as "Locally Licensed".
- **State**: The current license state of the appliance, Licensed or Unlicensed.
- **Model**: The appliance model that the license supports.
- **MAXBW**: The maximum bandwidth permitted by the license.
- **Feature**: The Citrix SD-WAN edition that the license supports.
- **Maintenance Expiry**: The expiry date of Citrix Subscription Advantage.

  > **Note**
  >
  > During Software upgrade, if the software build date is higher than the Maintenance Expiry date then the software upgrade is not allowed.

- **License Expiry**: The expiry date of the license.
- **License Type**: The type of license.

To upload and install license files in SD-WAN Center:

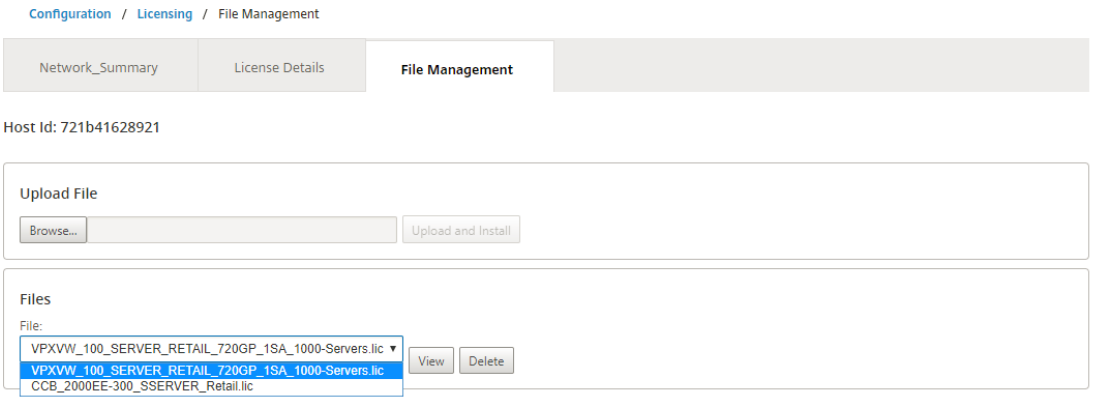
1. Obtain the license for the Citrix SD-WAN appliances and save it on your local computer.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> **Note**
>
> For instructions on obtaining a Citrix SD-WAN software license, contact Citrix SD-WAN Customer Support.

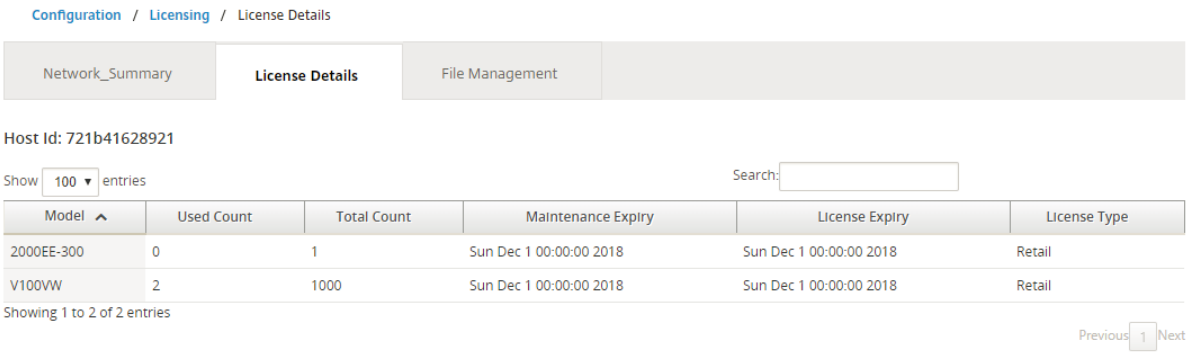
2. In the SD-WAN Center GUI, navigate to **Licensing** > **File Management**.
3. In the **Upload File** section, click **Browse**. Select the license file from your local computer and click **Upload and Install**.

   The installed license files are listed in the **Files** drop-down menu, you can choose to view or delete the license files.



> **Note**
>
> The Host ID is the SD-WAN Center host ID, used to generate the license files. The license files generated using a different host ID cannot be uploaded and installed on Citrix SD-WAN Center.

You can view the details of all the license files uploaded and installed on Citrix SD-WAN Center, at a glance, by navigating to **Configuration** > **Licensing** > **License Details.**



The following parameters are displayed:

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- **Model:** The appliance model that the license supports.
- **Used Count:** The number of appliances on which this license is installed.
- **Total Count:** The total number of appliances on which this license can be installed.
- **Maintenance Expiry**: The expiry date of Citrix Subscription Advantage.
- **License Expiry**: The expiry date of the license.
- **License Type**: The type of license.

Deploy Citrix SD-WAN on Azure from Citrix SD-WAN Center

March 12, 2021

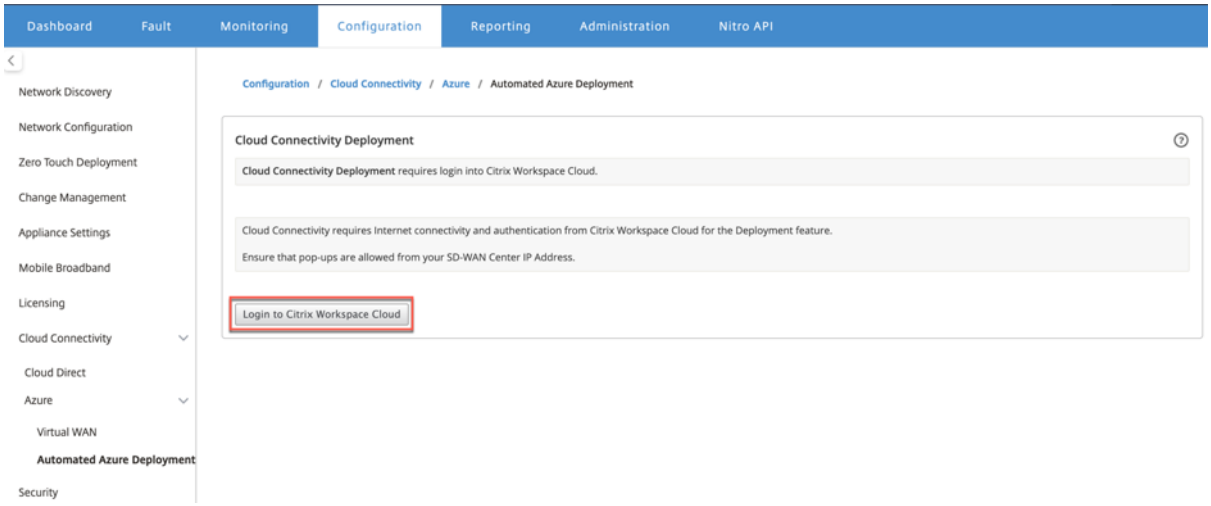
Citrix SD-WAN for Azure enables organizations to have a direct secure connection from each branch to the applications hosted in Azure eliminating the need to backhaul cloud bound traffic through a data center.

Prerequisites

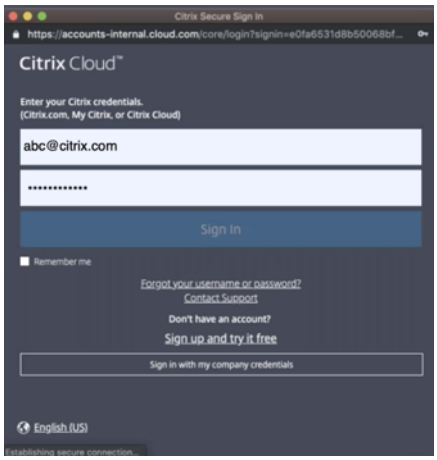
- Citrix Workspace Cloud credentials.
- Azure subscription credentials
- Azure application and service principal with the role-based access control, see How to: Use the portal to create an Azure AD application and service principal that can access resources.
- Once the service principal is created, make a note of the following details:
  - Azure Subscriber ID
  - Tenant ID
  - Application ID
  - Secret Key
- Perform the change management on the MCN/SD-WAN Center using the ctx-sdw-sw-xxxxxxx.zip.
- From Citrix SD-WAN Center, discover the MCN and pull the active config.

To deploy Citrix SD-WAN on Azure from SD-WAN Center, navigate to **Configuration > Cloud Connectivity > Azure > Automated Azure Deployment**.

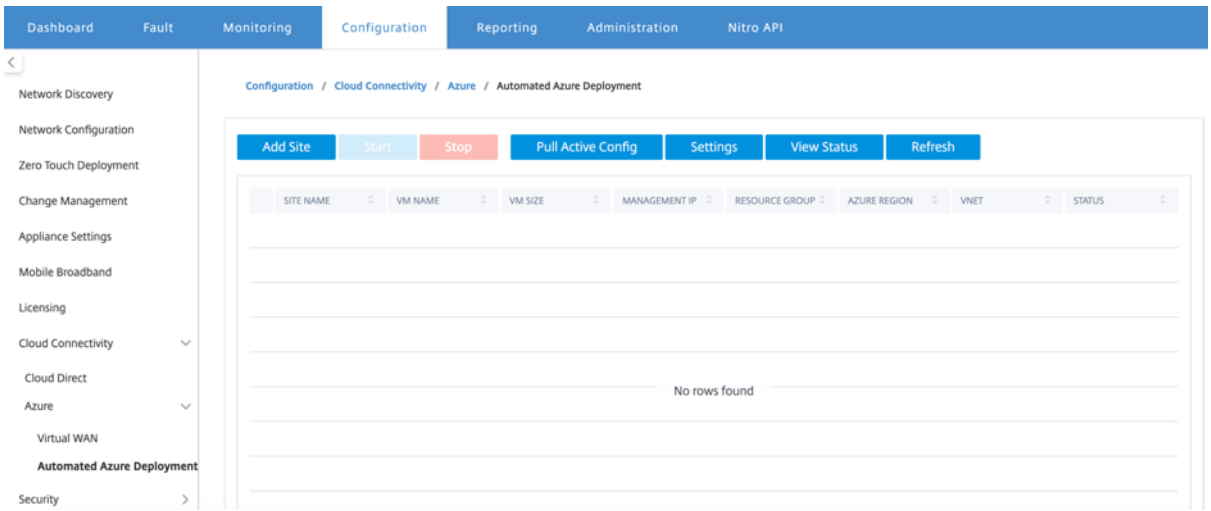
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Log in with Citrix Cloud credentials.

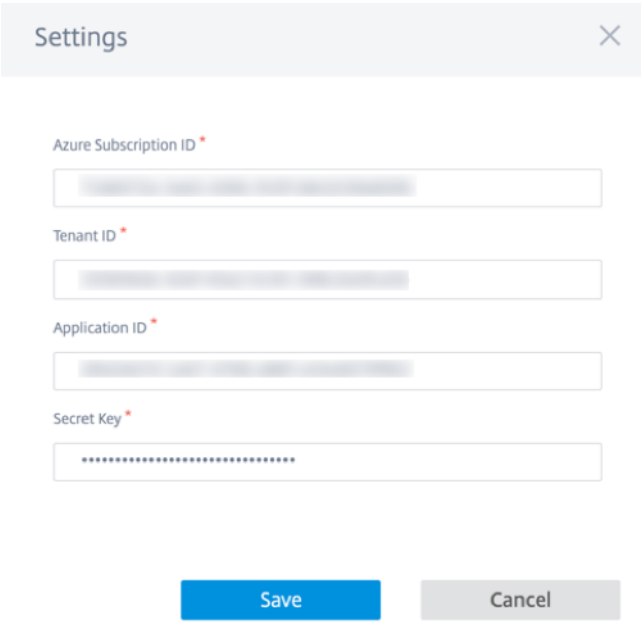


Automated Azure deployment



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Click **Settings** option and provide the Azure subscription details. Click Pull Active Config option to retrieve the active running config from the MCN.



Deploy Citrix SD-WAN in Azure

To deploy the Citrix SD-WAN in Microsoft Azure:

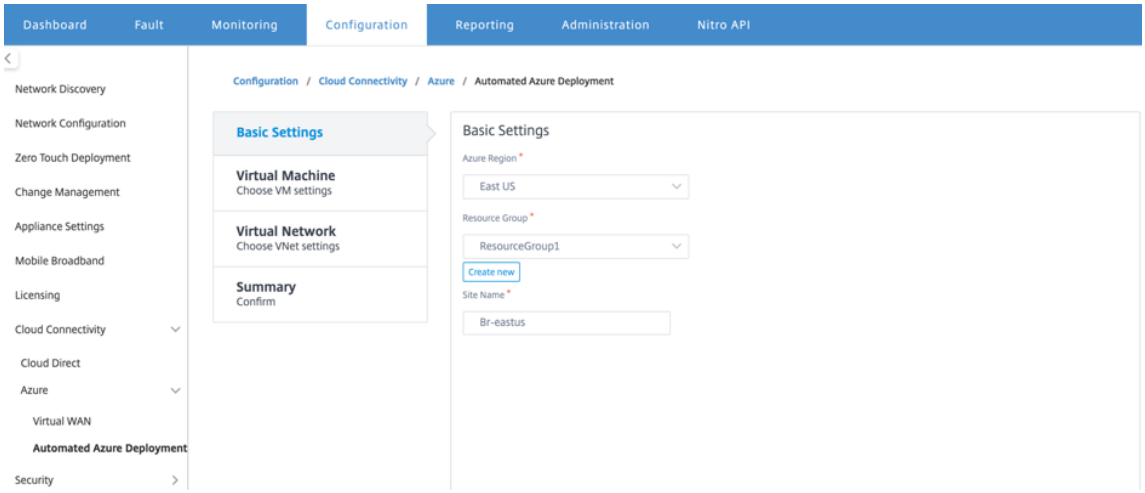
1. Click **Add a Site** to add a new SD-WAN instance. It initiates the creation of an SD-WAN virtual machine on Azure under your current subscription.

   As part of this deployment, it also:

   - Automatically adds SD-WAN configuration for the newly added site to the current active configuration on MCN.
   - Performs the change management.
   - Apply the MCN's software version and configuration to this new site.

   Complete the **Basic settings, Virtual Machine,** and **Virtual Network** settings.

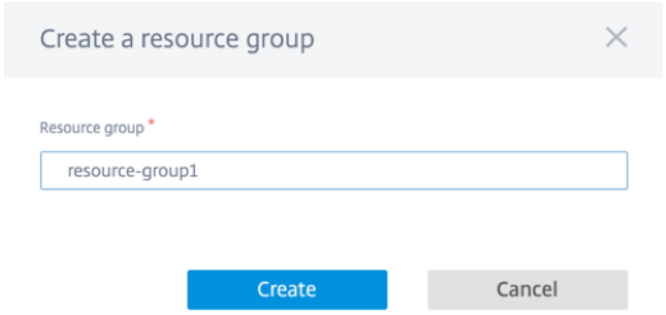
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Under Basic Settings, select the region and resource group from the drop-down list. Once the region is selected, the resource group drop-down list shows all the existing resource groups in this region under this subscription.

> **NOTE:**
>
> To add a site, the resource group must be empty.

You can choose an existing empty resource group or click **Create New** option to create a new one.

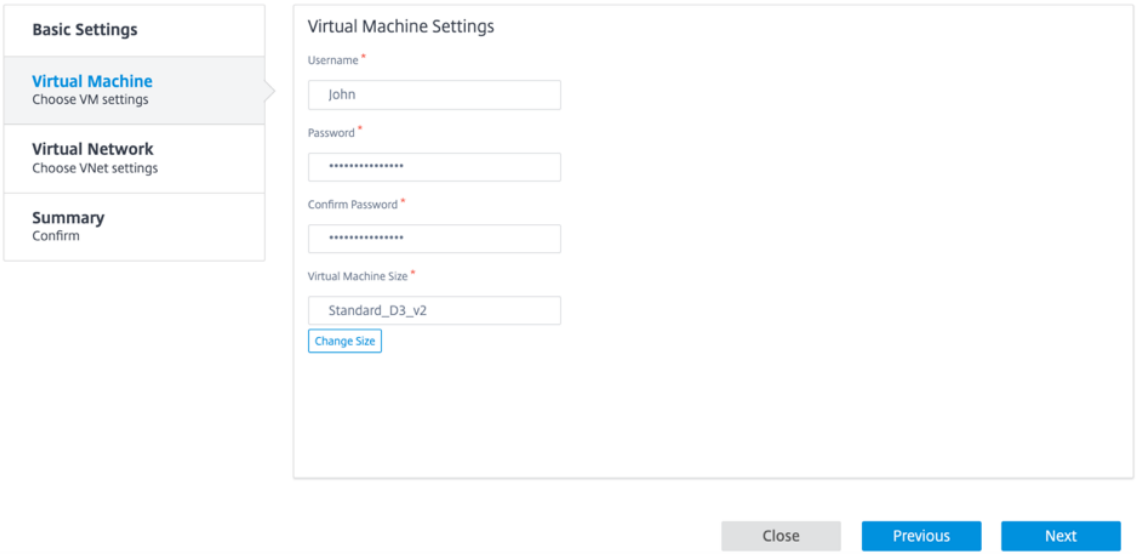


2. Site name is auto generated with the region name. You can still edit the site name as needed.

> **NOTE:**
>
> Ensure that the site name maintains the SD-WAN site name requirements and is unique in the SD-WAN network.
>
> The Azure VM name is generated from the site name in **AZ-regionname-sitename** format.

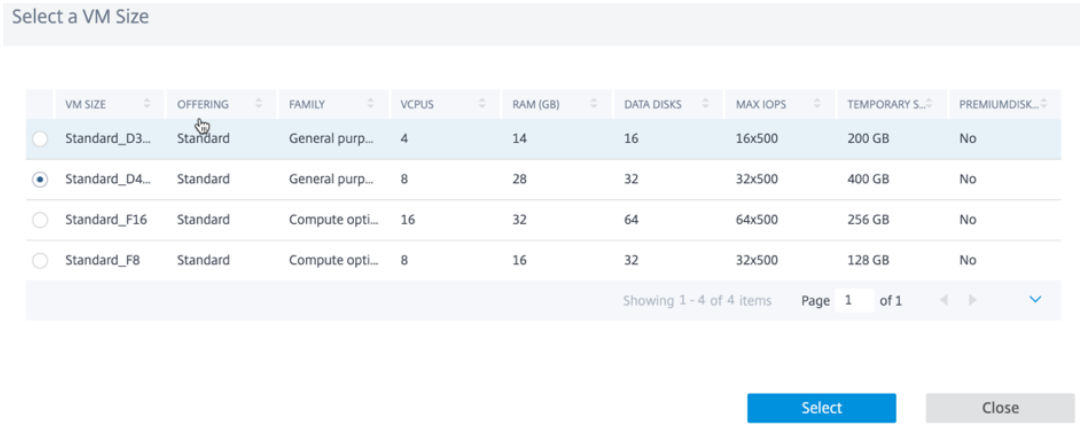
3. Click **Next** to configure the virtual machine.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



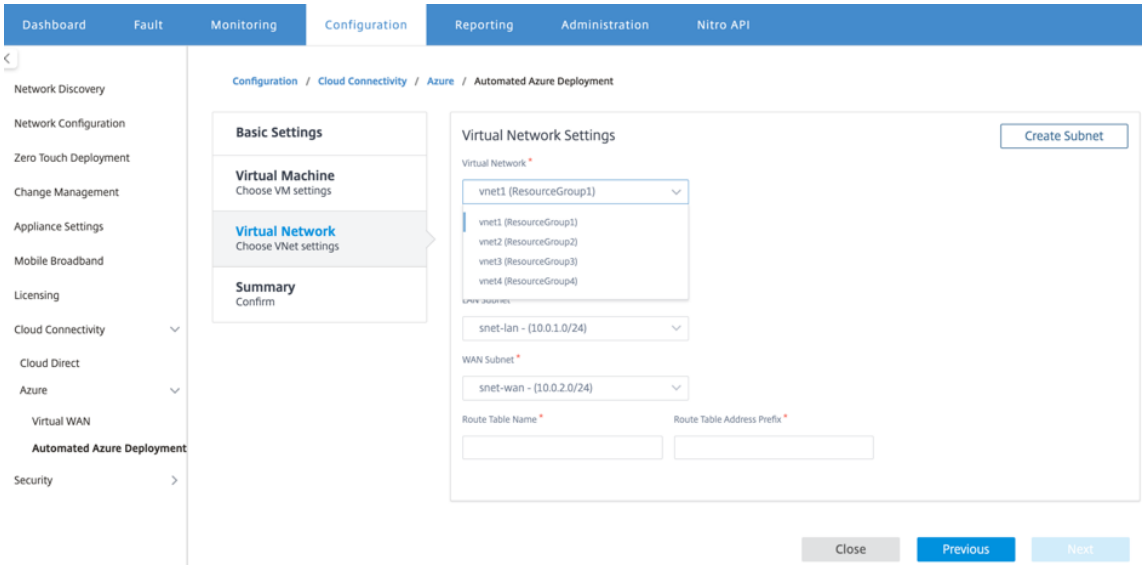
Provide a User name, Password, and Confirm password. By default, the VM size is auto filled with the standard size. Click **Change Size** to select a different VM size if needed.

> **NOTE:**
>
> This user credential provided during deployment has read-only access to the Azure SD-WAN. For administrative privileges, use admin credentials.

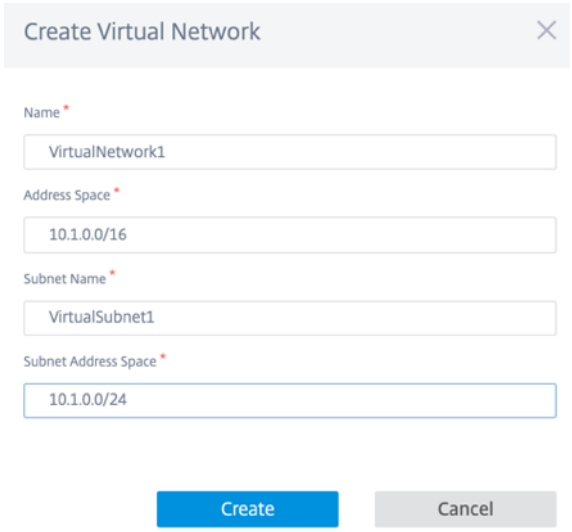


4. Click **Next** to perform the virtual network settings.
5. Select virtual network from the drop-down list. The list contains all the virtual network in the chosen Azure region.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

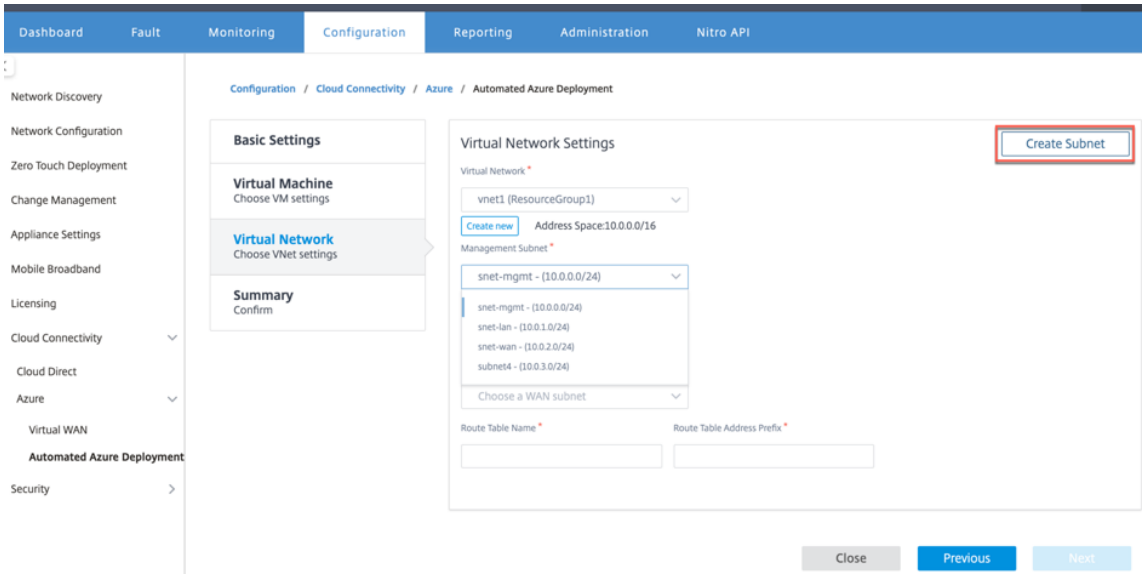


You can deploy the site on an existing virtual network or create a new virtual network. Click **Create New** to create a new virtual network. Provide the Virtual network name, Address space (specify a custom private IP address space), Subnet name, and Subnet address space.

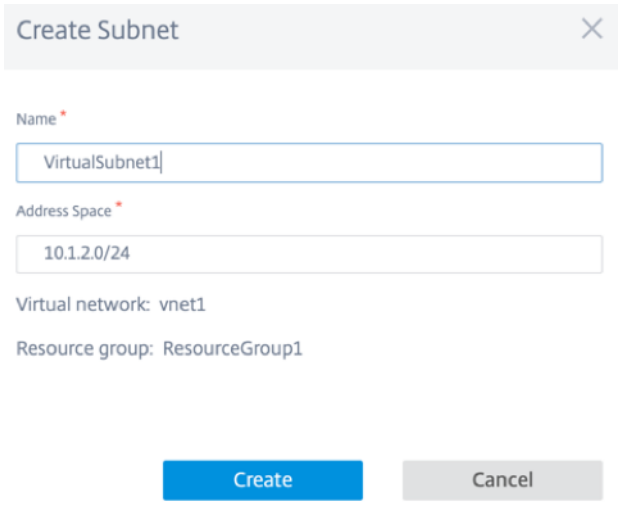


6. Select a subnet for management.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



7. You can also create a subnet using the **Create a Subnet** option (from the top right corner).

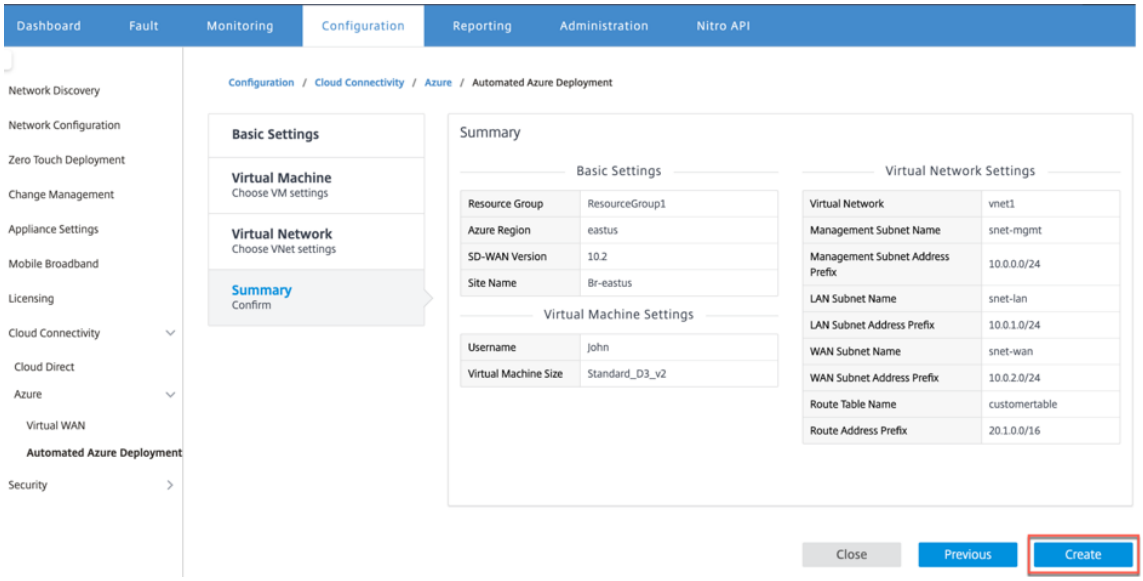


8. From the drop-down list, choose different subnet for LAN and WAN and provide the **Routing Table Name** along with the **Routing Table Address Prefix**. The **Routing Table Address Prefix** is the destination address space that is redirected to this SD-WAN appliance. Other target address will be redirected by Azure routing.

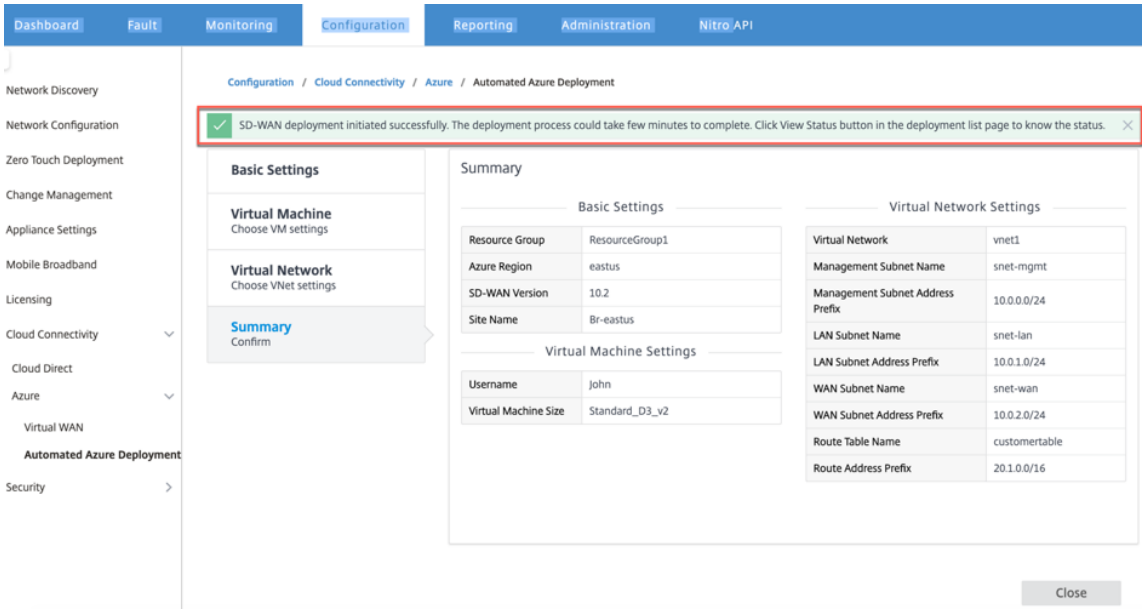
> **NOTE:**
>
> The Routing Table is associated with the LAN subnet. If the chosen LAN subnet already has an associated route table, then that route table will be displayed and cannot be modified. Otherwise you can specify the routing table name.

9. Click **Next** to review and confirm the setting detail and click **Create**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



A status message appears on the top stating that the deployment initiated successfully.



The deployment might take time to complete so it is recommended that you click **View Status** to get the latest update about the deployment status.

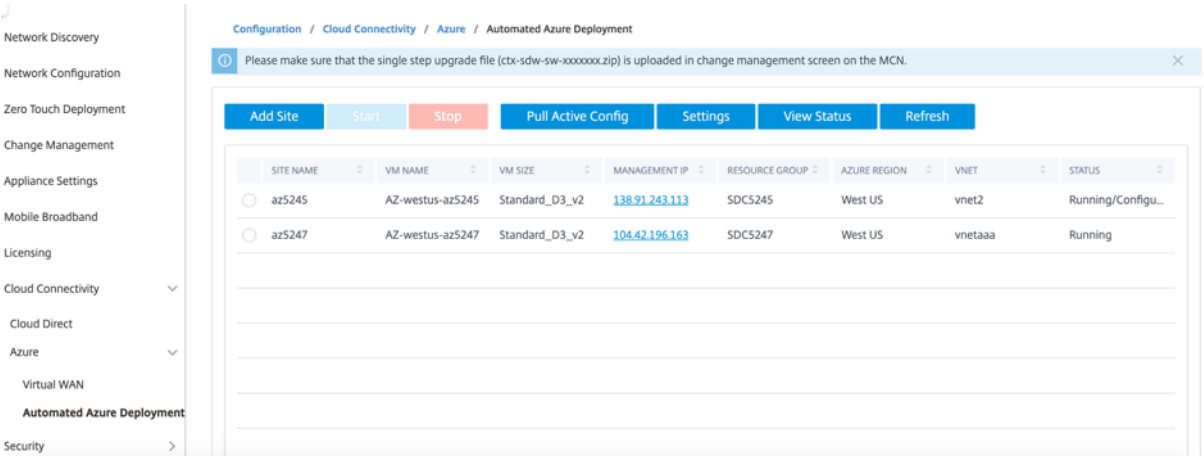
As part of the deployment:

- The virtual machine is created in the selected Azure region.
- A site is automatically added to the active SD-WAN configuration in the SD-WAN.
- Change management is performed on the newly provisioned Azure VM.

Once the deployment is succeeded, the virtual paths are formed between the MCN and Azure site. If the deployment encounters error, the process is rolled back and all the auto-created resources are reverted.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

By default, the site is placed as part of the default routing domain. It belongs to the default region using the default auto path group.



- **Site Name**: Name of the Citrix SD-WAN site. This site name is used in the Citrix SD-WAN configuration.
- **VM Name**: Name of the Virtual Machine (VM) that is provisioned in Azure.
- **VM Size**: The VM size that was selected while creating the site.
- **Management IP**: Management IP address that was assigned to the newly created SD-WAN VM.
- **Resource Group**: Resource groups are logical constructs and data exchange across resource groups is always possible. The Azure virtual machine belongs to this resource group. The new resources created during the deployment of the Citrix SD-WAN, are grouped under this resource group. If there is any error during the deployment, the resources created in this resource group will be deleted.
- **Azure Region**: Represents the location of the resource group and its resources.
- **VNet**: Virtual network that is being used by the site.
- **Status**: Provides the VM's status.

Click **Refresh** button to get the latest site status. You can **Start** or **Stop** the VM anytime for the selected site. You can select only one site at a time.

When the deployment is complete, login to MCN or Citrix SD-WAN Center to view the status of virtual paths.

Zero Touch Deployment

March 12, 2021

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> **Note**
>
> The Zero Touch Deployment service is supported only on select Citrix SD-WAN appliances:
>
> - SD-WAN 110 Standard Edition
> - SD-WAN 210 Standard Edition
> - SD-WAN 410 Standard Edition
> - SD-WAN 2100 Standard Edition
> - SD-WAN 1000 Standard Edition (reimage required)
> - SD-WAN 1000 Enterprise Edition (Premium Edition) (reimage required)
> - SD-WAN 1100 Standard Edition
> - SD-WAN 1100 Premium (Enterprise) Edition
> - SD-WAN 2000 Standard Edition (reimage required)
> - SD-WAN 2000 Enterprise Edition (Premium Edition(reimage required)
> - SD-WAN AWS VPX instance

Zero Touch Deployment (ZTD) Service is a Citrix operated and managed cloud service which allows discovery of new appliances in the Citrix SD-WAN network, and automates the deployment process for branch offices. The ZTD Cloud Service is accessible from any node in the network via Internet, and over Secure Socket Layer (SSL) protocol.

The ZTD Cloud Service securely communicates with backend Citrix Network services storing identification of customers who have purchased Zero Touch capable devices (e.g. SD-WAN 410-SE, 2100-SE). The backend services are in place to authenticate any Zero Touch Deployment request, properly validating association between the Customer Account and the Serial Numbers of Citrix SD-WAN appliances.

ZTD High-Level Architecture and Workflow

Data Center Site

Citrix SD-WAN Administrator –A user with Administration rights of the SD-WAN environment with the following primary responsibilities:

- Configuration creation using Citrix SD-WAN Center Network Configuration tool, or import of configuration from the Master Control Node (MCN) SD-WAN appliance
- Citrix Cloud Login to initiate the Zero Touch Deployment Service for new site node deployment.

> **Note**
>
> If your SD-WAN Center is connected to the internet through a proxy server, you have to configure the proxy server settings on the SD-WAN Center. For more information, see Proxy Server Settings

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> for Zero Touch Deployment.

Network Administrator –A user responsible for Enterprise network management (DHCP, DNS, internet, firewall, etc.)

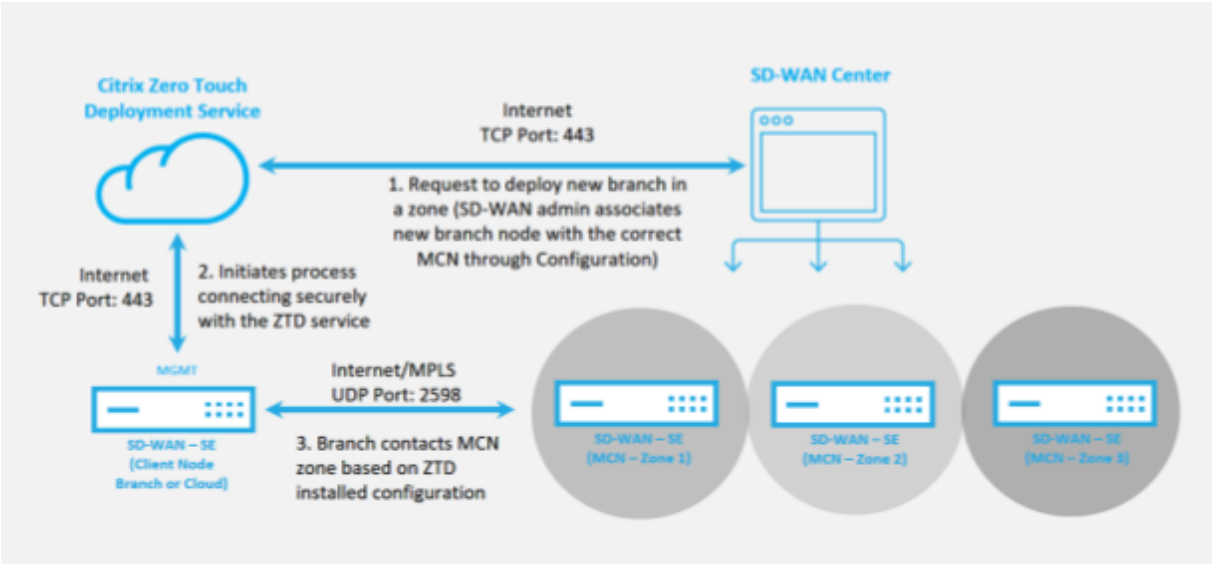
- If necessary, configure firewalls for outbound communication to FQDN ***sdwanzt.citrixnetworkapi.net*** from SD-WAN Center.

Remote Site

Onsite Installer –A local contact or hired installer for on-site activity with the following primary responsibilities:

- Physically unpack the Citrix SD-WAN appliance.
- Reimage non-ZTD ready appliances.
  - Required for: SD-WAN 1000-SE, 2000-SE, 1000-EE, 2000-EE
  - Not required for: SD-WAN 410-SE, 2100-SE
- Power cable the appliance.
- Cable the appliance for internet connectivity on the Management interface (e.g. MGMT, or 0/1).
- Cable the appliance for WAN link connectivity on the Data interfaces (e.g. apA.WAN, apB.WAN, apC.WAN, 0/2, 0/3, 0/5, etc).

> **Note**
>
> The interface layout is different each model, so please reference the documentation for identification of data and management ports.

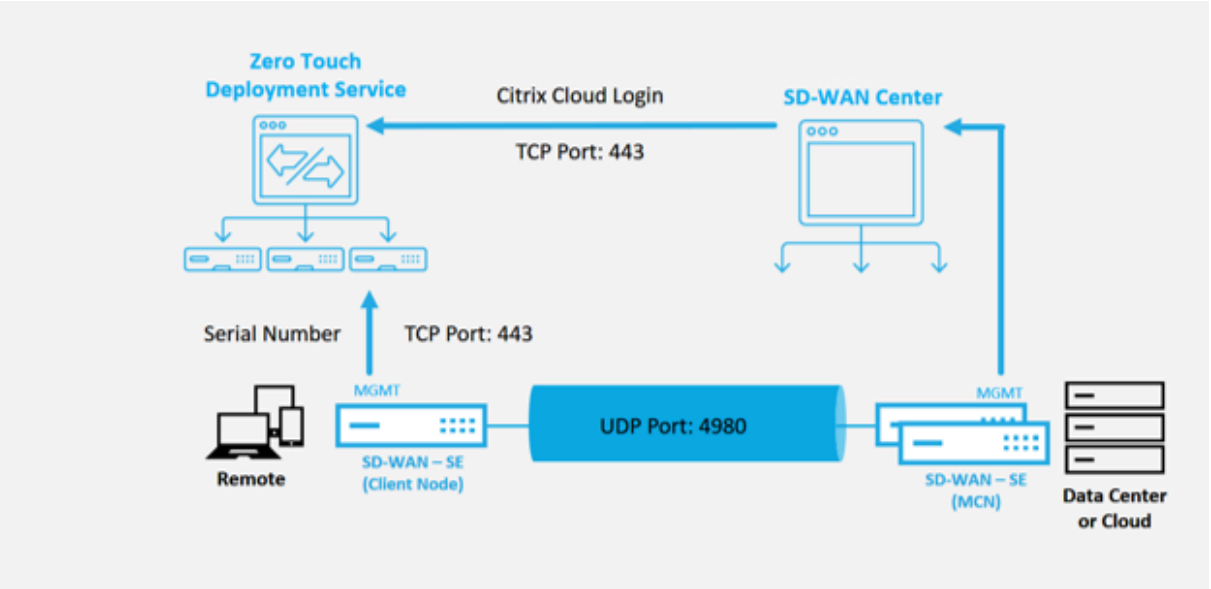


© 1999–2025 Cloud Software Group, Inc. All rights reserved.

The following prerequisites are required before starting any Zero Touch Deployment service:

- Actively running SD-WAN promoted to Master Control Node (MCN).
- Actively running SD-WAN Center with connectivity to the MCN through Virtual Path.
- Citrix Cloud Login credentials created on https://onboarding.cloud.com (reference the instruction below on account creation).
- Management network connectivity (SD-WAN Center and SD-WAN Appliance) to the Internet on port 443, either directly or through a proxy server.
- Internet connectivity on port 443 to access the SD-WAN Center web portal for the ZTD initial setup.
- (optional) At least one actively running SD-WAN appliance operating at a branch office in Client Mode with valid Virtual Path connectivity to MCN to help validate successful path establishment across the existing underlay network.

The last prerequisite is not a requirement, but allows the SD-WAN Administrator to validate that the underlay network allows Virtual Paths to be established when the Zero Touch Deployment is complete with any newly added site. Primarily, this validates that the appropriate Firewall and Route policies are in place to either NAT traffic accordingly or confirm ability for UDP port 4980 can successfully penetrate the network to reach the MCN.



Zero Touch Deployment Service Overview

The Zero Touch Deployment Service works in tandem with the SD-WAN Center to provide an easier deployment of branch office SD-WAN appliances. SD-WAN Center is configured and used as the central management tool for the SD-WAN Standard and Enterprise (Premium) Edition appliances. To utilize the Zero Touch Deployment Service (or ZTD Cloud Service), an Administrator must begin by deploying

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

the first SD-WAN device in the environment, then configure and deploy the SD-WAN Center as the central point of management. When the SD-WAN Center, release 9.1 or later, is installed with connectivity to the public internet on port 443, SD-WAN Center automatically initiates the Cloud Service and install necessary components to unlock the Zero Touch Deployment features and to make the Zero Touch Deployment option available in the GUI of SD-WAN Center. Zero Touch Deployment is not available by default in the SD-WAN Center software. This is purposely designed to make sure the proper preliminary components on the underlay network are present before allowing an Administrator to initiate any on-site activity involving Zero Touch Deployment.

After a working SD-WAN environment is up and running registration into the Zero Touch Deployment Service is accomplished through creating a Citrix Cloud account login. With SD-WAN Center able to communicate with the ZTD service, the GUI exposes the Zero Touch Deployment options under the Configuration tab. Logging into the Zero Touch Service authenticates the Customer ID associated with the particular SD-WAN environment and registers the SD-WAN Center, in addition to unlocking the account for further authentication of ZTD appliance deployments.

Using the Network Configuration tool in SD-WAN Center, the SD-WAN Administrator will then need to utilize the templates or clone site capability to build out the SD-WAN Configuration to add new sites. The new configuration is used by the SD-WAN Center to initiate the deployment of ZTD for the newly added sites. When the SD-WAN Administrator initiates a site for deployment using the ZTD process, he or she has the option to pre-authenticate the appliance to be used for ZTD by pre-populating the serial number, and initiating email communication to on-site installer to begin on-site activity.

The Onsite Installer receives email communication that the site is ready for Zero Touch Deployment and can begin the installation procedure of powering on and cabling the appliance for DHCP IP address assignment and internet access on the MGMT port. Also, cabling in any LAN and WAN ports. Everything else is initiated by the ZTD Service and progress is monitored by the utilizing the activation URL. In the event the remote node to be installed is a cloud instance, opening up the activation URL begins the workflow to automatically install the instance in the designated cloud environment, no action is needed by a local installer.

The Zero Touch Deployment Cloud Service automates the following actions:

Download and Update the ZTD Agent if new features are available on the branch appliance.

- Authenticate the branch appliance by validating the serial number.
- Authenticate that the SD-WAN Administrator accepted the site for ZTD using the SD-WAN Center.
- Pull the configuration file specific for the targeted appliance from the SD-WAN Center.
- Push the configuration file specific for the targeted appliance to the branch appliance.
- Install the configuration file on the branch appliance.
- Push any missing SD-WAN software components or required updates to the branch appliance.
- Push a temporary 10 Mbps license file for confirmation of Virtual Path establishment to the

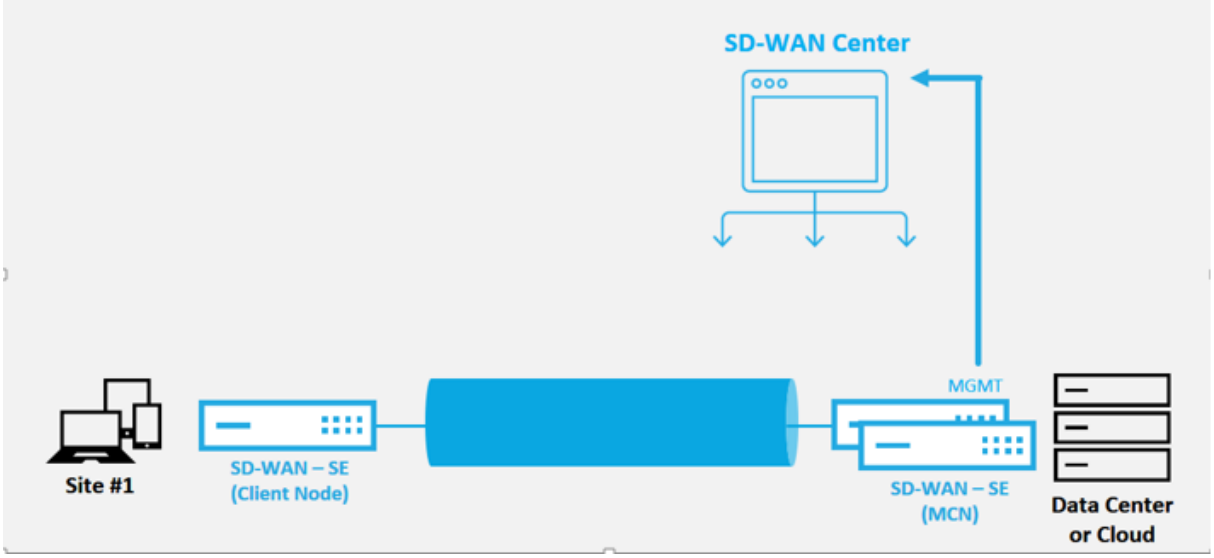
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

branch appliance.
- Enable the SD-WAN Service on the branch appliance.

More steps are required of the SD-WAN Administrator to install a permanent license file on the appliance.

Zero Touch Deployment Service Procedure

The following procedure detail the steps required to deploy a new site using the Zero Touch Deployment Service. Have a running MCN and one client node already working with proper communication to SD-WAN Center, as well as established Virtual Paths confirming connectivity across the underlay network. The following steps are required of the SD-WAN Administrator to initiate the deployment of zero touch:



How to Configure Zero Touch Deployment Service

The SD-WAN Center has the functionality to accept requests from newly connected appliances to join the SD-WAN Enterprise network. The request is forwarded to the web interface through the zero touch deployment service. Once the appliance connects to the service, configuration and software upgrade packages are downloaded.

Configuration workflow:

- Access **SD-WAN Center** > **Create New site configuration** or Import existing configuration and save it.
- Log in to Citrix Workspace Cloud to enable ZTD service. The Zero Touch Deployment menu option is now displayed in the SD-WAN center web management interface.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- In SD-WAN Center, navigate to **Configuration** > **Zero Touch Deployment** > **Deploy New Site**.
- Select an appliance, click Enable, and click **Deploy**.
- Installer receives activation email > Enter the serial number > **Activate** > Appliance is deployed successfully.

To configure Zero Touch Deployment service:

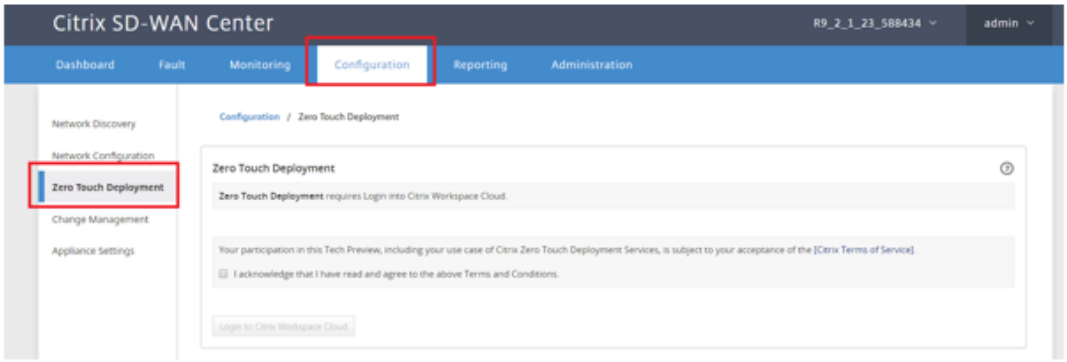
1. Install SD-WAN Center with enabled Zero Touch Deployment capabilities.

   a) Install SD-WAN Center with DHCP assigned IP address.

   b) Verify that SD-WAN Center is assignment a proper management IP address and network DNS address with connectivity to the public internet across the management network.

   c) Upgrade the SD-WAN Center to the latest SD-WAN software release version.

   d) With proper internet connectivity, the SD-WAN Center initiates the Zero Touch Deployment (ZTD) Cloud Service and automatically download and install any firmware updates specific to ZTD, if this call home procedure fails the following Zero Touch Deployment option will not be available in the GUI.



   e) Read the Terms and Conditions, and then select "**I acknowledge that I have read and agree to the above Terms and Conditions**."

   f) Click the "**Login to Citrix Workspace Cloud**"button if a Citrix Cloud account has already been created.

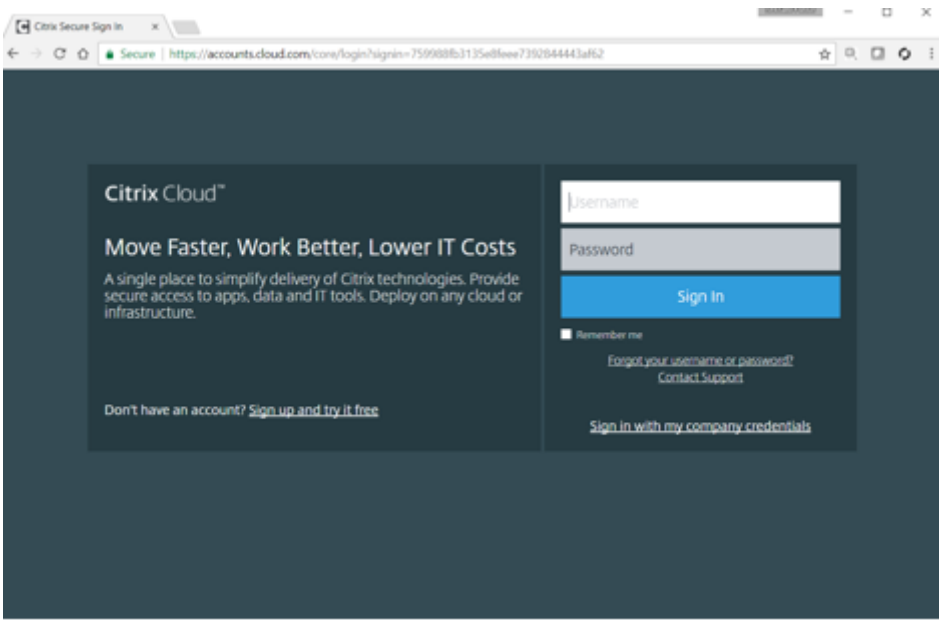
   g) Login into the Citrix Cloud account, and upon receiving the following message of successful login, **PLEASE DO NOT CLOSE THIS WINDOW UP, THE PROCESS REQUIRES ANOTHER ~20 SECONDS FOR THE SD-WAN CENTER GUI TO BE REFRESHED.** The window should close on its own when it is complete.**

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

h) To create a Cloud Login account follow the below procedure:

- Open a web browser to https://onboarding.cloud.com
- Click on the link for "**Wait, I have a Citrix.com account**."

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



i) Sign-in with an existing Citrix account.

j) Once logged into SD-WAN Center Zero Touch Deployment page, you may notice that no sites are available for ZTD deployment because of the following reasons:

- The active configuration has not been selected from the Configuration drop-down menu
- All the sites for the current active configuration have already been deployed
- The configuration was not built using the SD-WAN Center, but rather the Configuration Editor available on the MCN
- Sites were not built in the configuration referencing zero touch capable appliances (e.g. 410-SE, 2100-SE, Cloud VPX)

2. Update the configuration to add a **new remote** site with a **ZTD capable SD-WAN appliance** using SD-WAN Center Network Configuration.

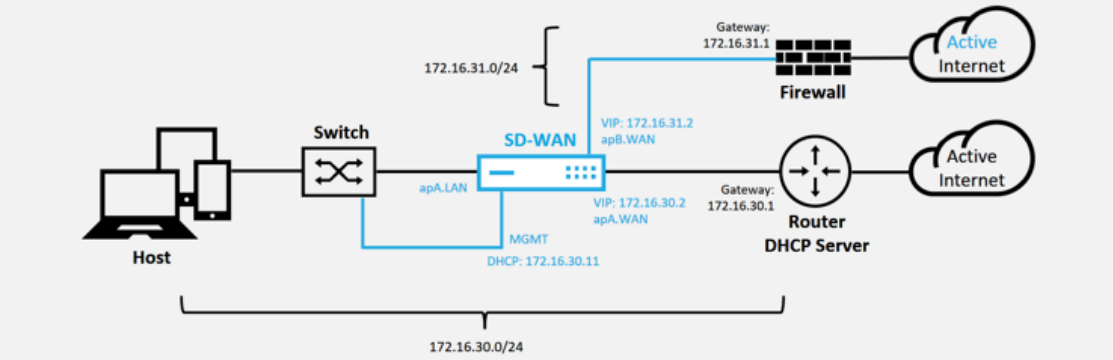
   If the SD-WAN configuration was not built using the SD-WAN Center Network Configuration, import the active configuration from the MCN and begin modifying the configuration using SD-WAN Center. For Zero Touch Deployment capability, the SD-WAN Administrator must build the configuration using SD-WAN Center. The following procedure should be used to add a new site targeted for zero touch deployment.

   Design the new site for SD-WAN appliance deployment by first outlining the details of the new site (that is, Appliance Model, Interface Groups usage, Virtual IP Addresses, WAN Links with bandwidth and their respective Gateways).

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> **Important**
>
> You may notice any site node that has VPX selected as the model is also listed, but currently ZTD support is only available for the AWS VPX instance.
>
> **Note**
>
> - Make sure that you are using a support web browser for Citrix SD-WAN Center
> - Make sure the web browser is not blocking any pop-up windows during the Citrix Workspace Login

Branch Office Topology

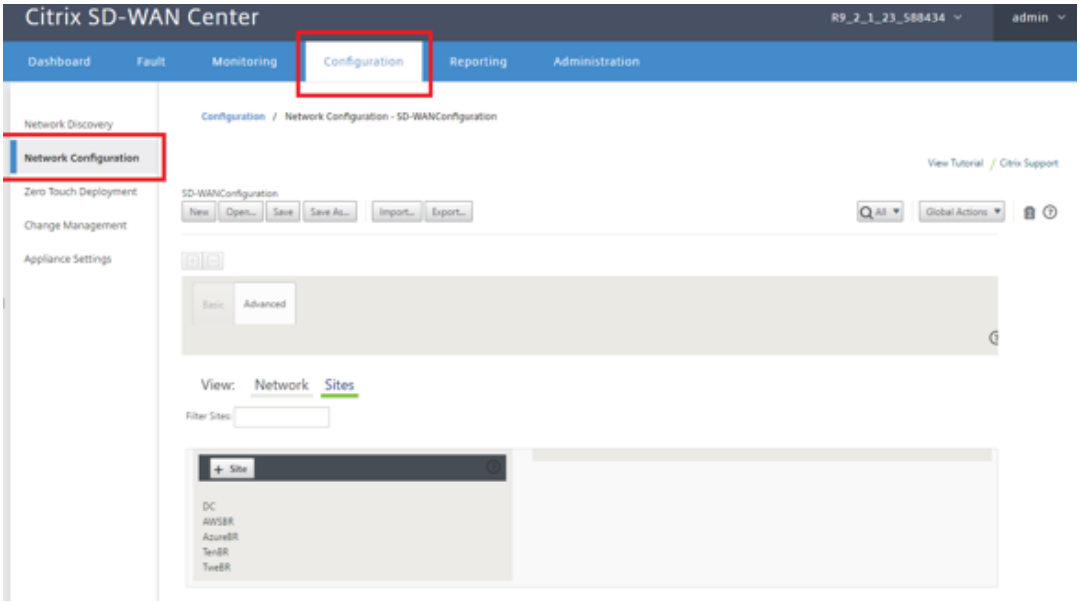


This is an example deployment of a branch office site, the SD-WAN appliance is deployed physically in path of the existing MPLS WAN link across a 172.16.30.0/24 network, and using an existing backup link by enabling it into an active state and terminating that second WAN link directly into the SD-WAN appliance on a different subnet 172.16.31.0/24.

> **Note**
>
> The SD-WAN appliances automatably assign a default IP address of 192.168.100.1/16. With DHCP enabled by default, the DHCP Server in the network may provide the appliance a second IP address in a subnet that overlaps the default. This can possibly result in a routing issue on the appliance where the appliance may fail to connect to the ZTD Cloud Service. Configure the DHCP server to assign IP addresses outside of the range of 192.168.0.0/16.
>
> There are various different deployment modes available for SD-WAN product placement in a network. In the above example, SD-WAN is being deployed as an overlay on top of existing networking infrastructure. For new sites, SD-WAN Administrators may choose to deploy the SD-WAN in Edge or Gateway Mode deployment, eliminating the need for a WAN edge router and firewall, and consolidating the network needs of edge routing and firewall onto the SD-WAN solution.

a) Open the **SD-WAN Center web management interface** and navigate to the **Configuration** > **Network Configuration** page.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



b) Make sure a working configuration is already in place, or import the configuration from the MCN.

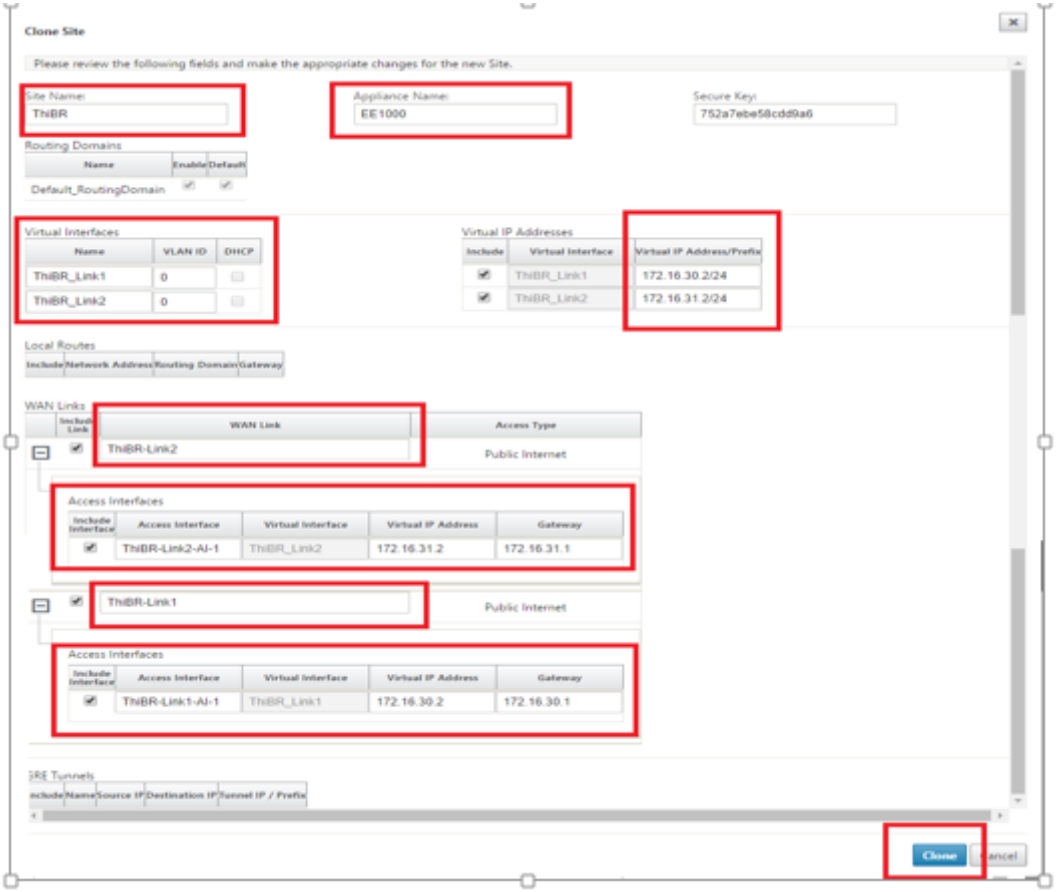
c) Navigate to the Advanced tab to create a site.

d) Open the Sites tile to display the currently configurated sites.

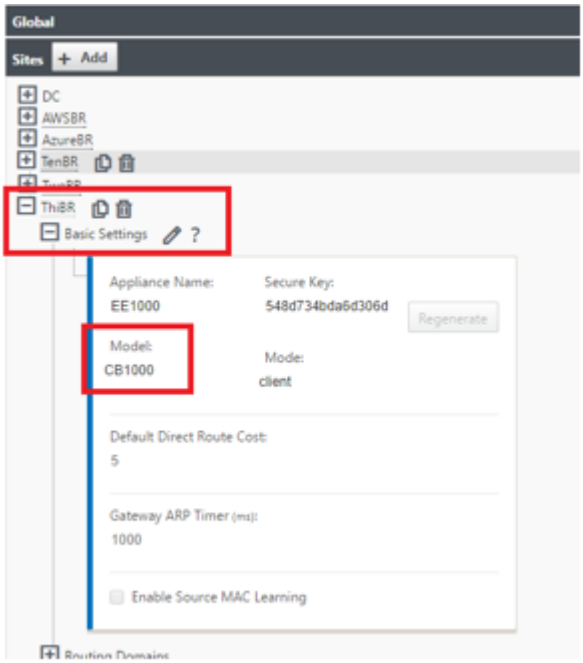
e) Quickly built the configuration for the new site by utilizing the clone feature of any existing site.

f) Populate all the required fields from the topology designed for this new branch site

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



g) After cloning a new site, navigate to the site's **Basic Settings**, and verify that the Model of SD-WAN is correctly selected which would support the zero touch service.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

h) The SD-WAN model for the site can be updated, but do be aware that the Interface Groups may have to be redefined since the updated appliance may have a new interface layout then what was used to clone.

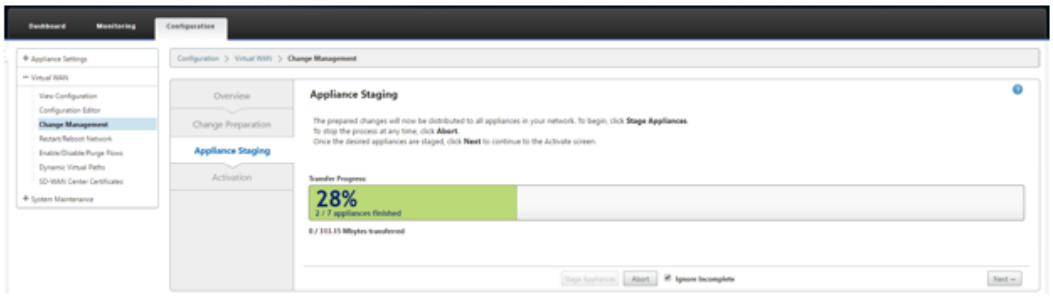
i) Save the new configuration on SD-WAN Center, and use the export to the "**Change Management inbox**"option to push the configuration using Change Management.

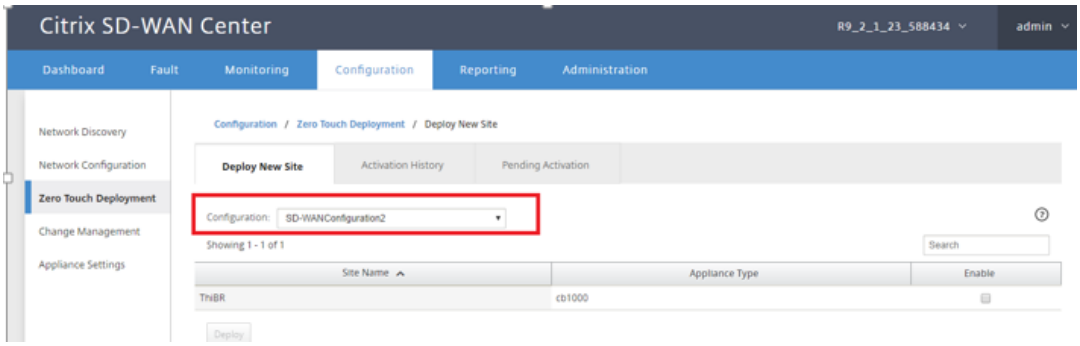
j) Follow the Change Management procedure to properly stage the new configuration, which makes the existing SD-WAN devices aware of the new site to be deployed via zero touch, you need to utilize the "Ignore Incomplete"option to skip attempting to push the configuration to the new site that still needs to go through the ZTD workflow.

3. Navigate back to the SD-WAN Center Zero Touch Deployment page, and with the new active configuration running, the new site is available for deployment.

a) In the Zero Touch Deployment page, under the **Deploy New Site** tab, select the running network configuration file

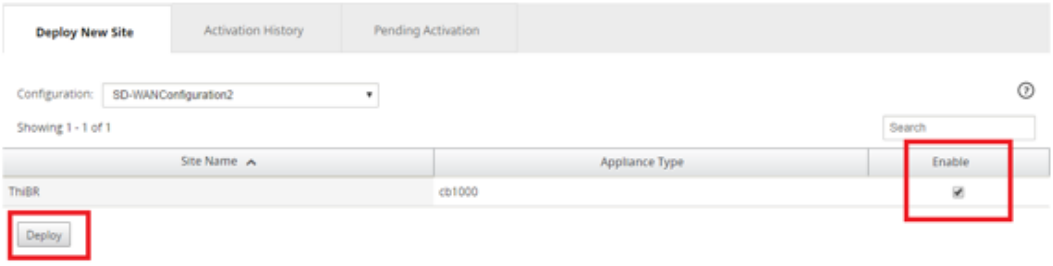
b) After the running configuration file is selected, the list of all the branch sites with undeployed SD-WAN devices that are supported for zero touch will be displayed



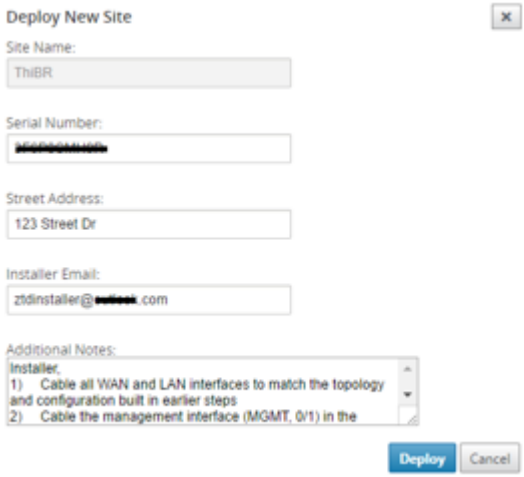


c) Select the branch sites you want to configure for Zero Touch service, click **Enable**, and then **Deploy**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



d) A Deploy New Site pop-up window appears, where the Admin can provide the Serial Number, branch site Street Address, Installer Email address, and more Notes, if necessary.



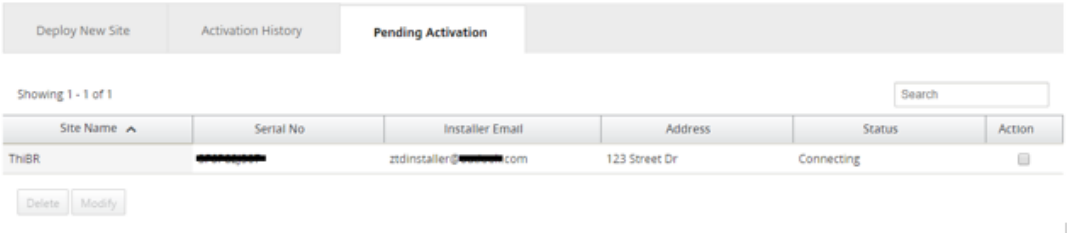
> **Note**
>
> The Serial Number entry field is optional and depending if it is populated or not, will result in a change in on-site activity the Installer is responsible for.
>
> - If Serial Number field is populated –The installer in not required to enter serial number into the activation URL generated with the deploy site command
> - If Serial Number field is left black –The installer will be responsible for entering in the correct serial number of the appliance into the activation URL generated with the deploy site command

a) After clicking the **Deploy** button, a message will appear indicating that "The Site configuration has been deployed."

b) This action triggers the SD-WAN Center, which was previously registered with the ZTD Cloud Service, to share the configuration of this particular site to be temporality stored in the ZTD Cloud Service.

c) Navigate to the Pending Activation tab to confirm that the branch site information populated successfully and was put into a pending installer activity status.

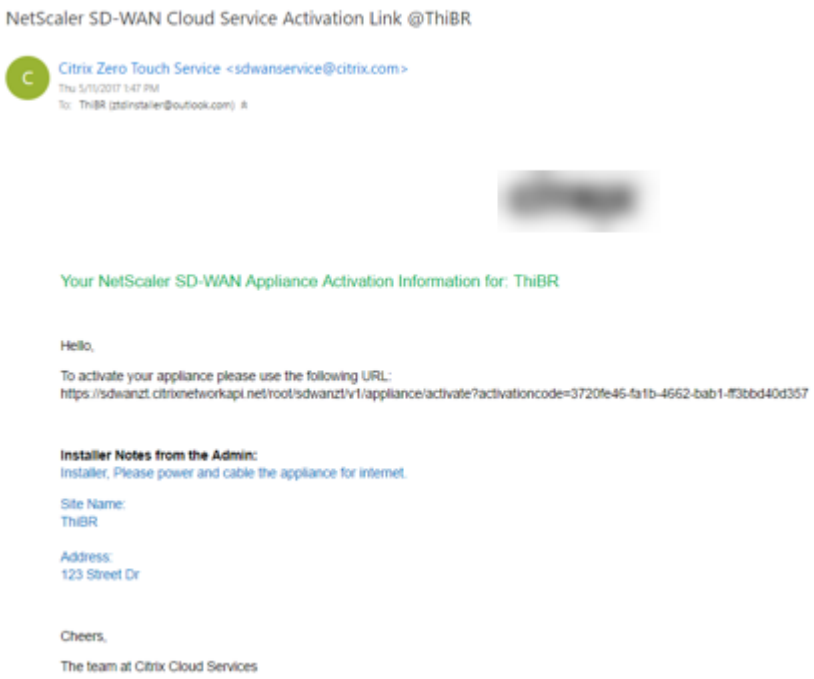
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



> **Note**
>
> A zero touch deployment in the Pending Activation state can optionally be chosen to Delete or Modify, if information is incorrect. If a Site is deleted from the pending activation page, it becomes available to be deployed in the Deploy New Site tab page. Once you choose to delete the branch site from Pending activation, the activation link send to the installer becomes invalid.
>
> If the Serial Number field was not populated by the SD-WAN Administrator, the Status Field indicates "Waiting for Installer"instead of "Connecting."

4. The next series of activities is performed by the On-site Installer.

   a) The Installer verifies the mailbox for the email address that the SD-WAN Administrator used when deploying the site.



   b) Open the zero touch deployment Activation URL in an internet browser window.

   c) If the SD-WAN Administrator did not pre-populate the serial number in the deploy site step, then the Installer would be responsible for locating the serial number on the physical ap-

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

pliance and entering the serial number manually into the activation URL, then click the **Activate** button.

d) If the Admin pre-populating the Serial Number information, the Activation URL will have already progressed to the next step.

e) The installer must physically be on-site to perform the following actions:

- Cable all WAN and LAN interfaces to match the topology and configuration built in earlier steps.
- Cable the management interface (MGMT, 0/1) in the segment of the network that provides DHCP IP address and connectivity to the Internet with DNS and FQDN to IP address resolution.
- Power cable the SD-WAN appliance.
- Turn on the power switch of the appliance.

> **Note**
>
> Most appliances will automatically power on when the power cable is attached. Some appliance may have to be powered on using the power switch on the front of the appliance, others may have the power switch on the rear of the appliance. Some power switches require holding the power button until the unit powers up.

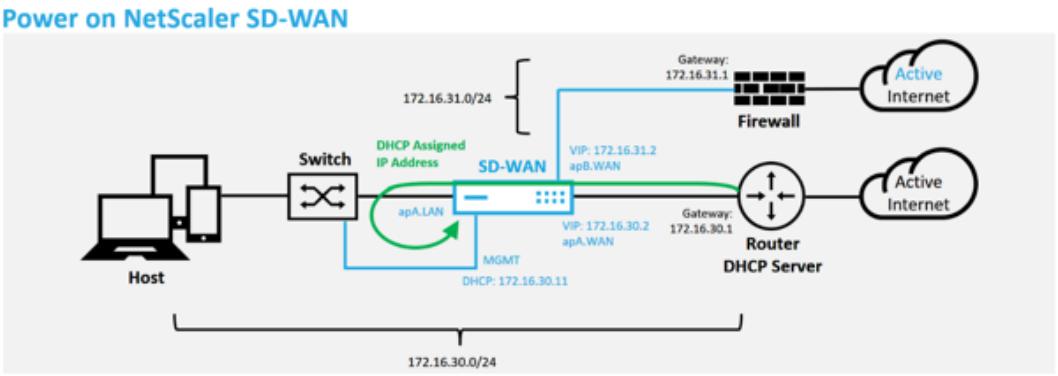
5. The next series of steps are automated with the help of the Zero Touch Deployment service, but requires that the following pre-requisites are available.

- The branch appliance should be powered up
- DHCP must be available in the existing network to assign management and DNS IP address
- Any DHCP assigned IP address requires connectivity to the internet with ability to resolve FQDNs

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- IP assignment can be configured manually, as long as the other pre-requisites are meet

a) The appliance obtains an IP address from the networks DHCP Server, in this example topology this is achieved through the bypassed data interfaces of a factory default state appliance.



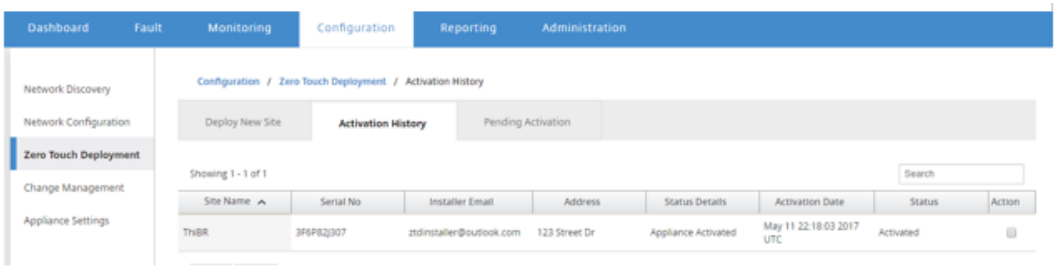
b) As the appliance obtains the web management and DNS IP addresses from the underlay network DHCP Server, the appliance initiates the Zero Touch Deployment Service and download any ZTD related software updates.

c) With successful connectivity to the ZTD Cloud Service, the deployment process automatically perform the following:

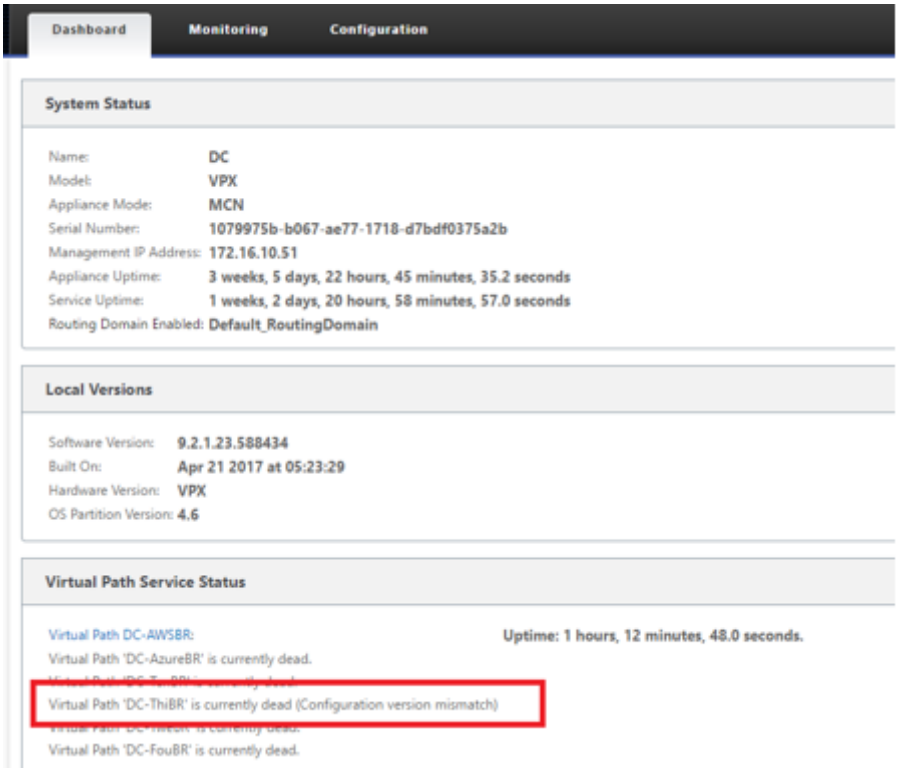
- Download the Configuration File that is stored earlier by the SD-WAN Center
- Applying the Configuration to the local appliance
- Download and Install a temporary 10 MB license file
- Download and Install any software updates if needed
- Activate the SD-WAN Service

d) Further confirmation can be done in the SD-WAN Center web management interface, the Zero Touch Deployment menu displays successfully activated appliances in the **Activation History** tab.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

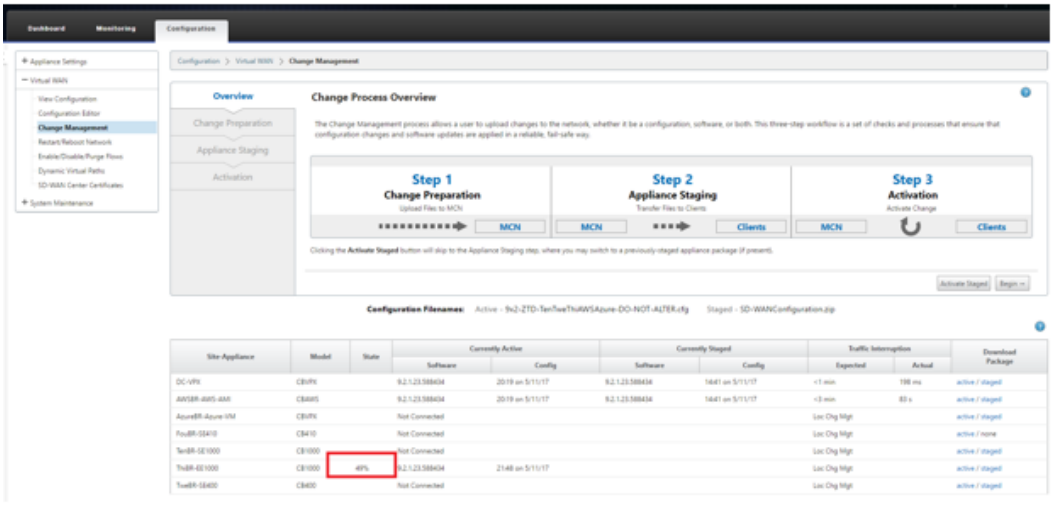


e) The Virtual Paths may not immediately show in a connected state because the MCN may not trust the configuration handed down from the ZTD Cloud Service, and reports "Configuration version mismatch"in the MCN Dashboard.

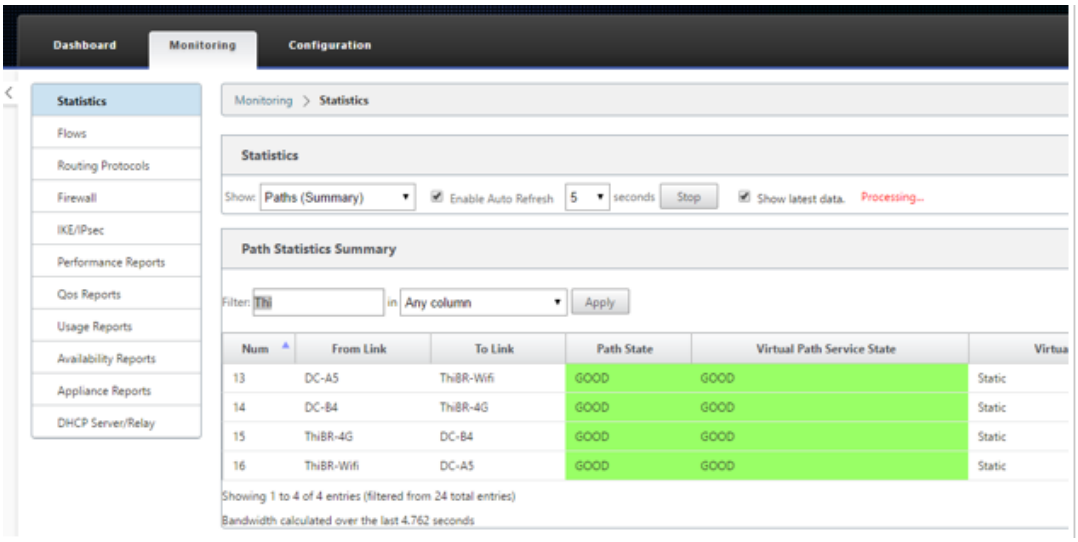


f) The configuration is redelivered to the newly installed branch office appliance and the status is monitored on the **MCN** > **Configuration** > **Virtual WAN** > **Change Management** page (this process can take several minutes to complete).

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

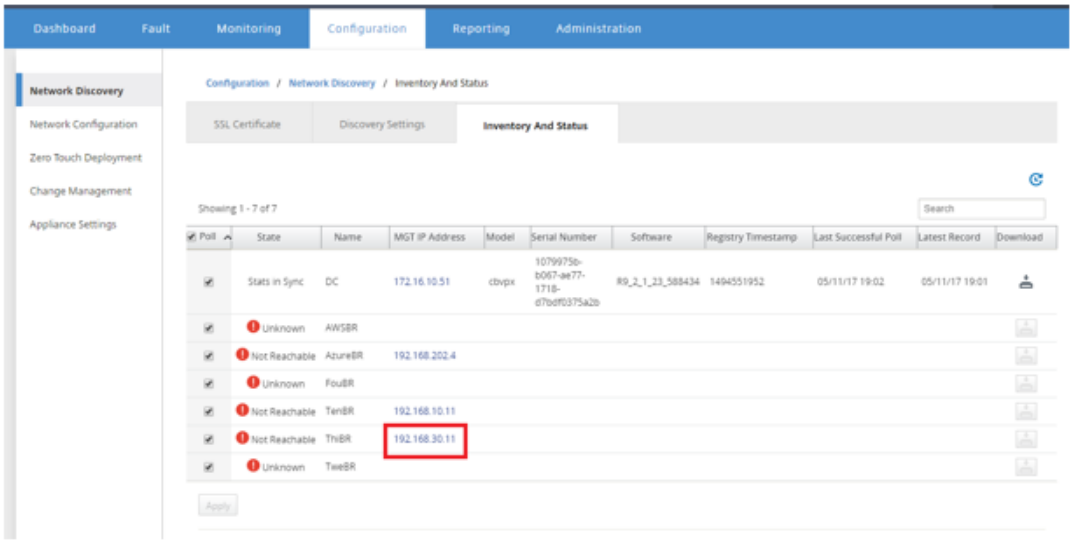


g) The SD-WAN Administrator can monitor the head-end MCN web management page for the established Virtual Paths of the remote site.

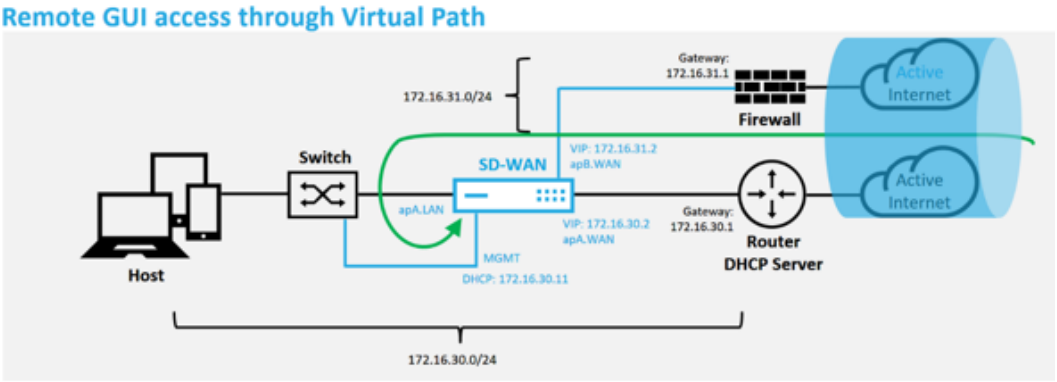


h) SD-WAN Center can also be utilized to identify the DHCP assigned IP address of the on-site appliance from the **Configuration** > **Network Discovery** > **Inventory and Status** page.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

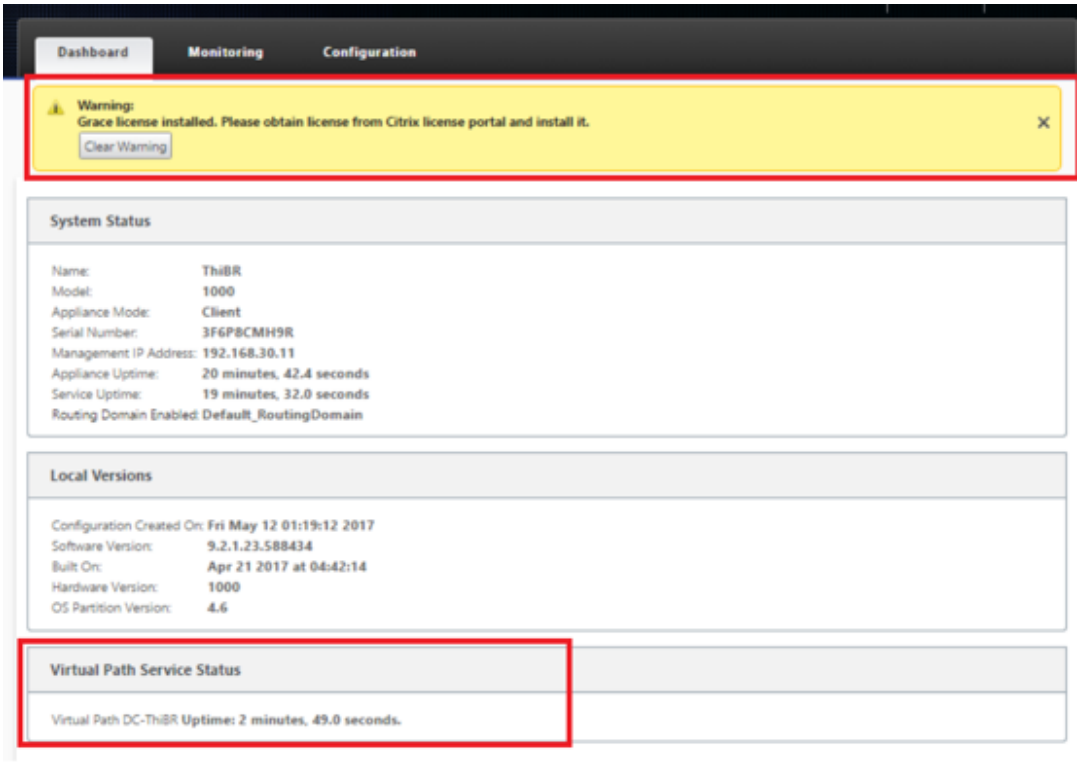


i) At this point the SD-WAN Network Administrator can gain web management access to on-site appliance utilizing the SD-WAN overlay network.



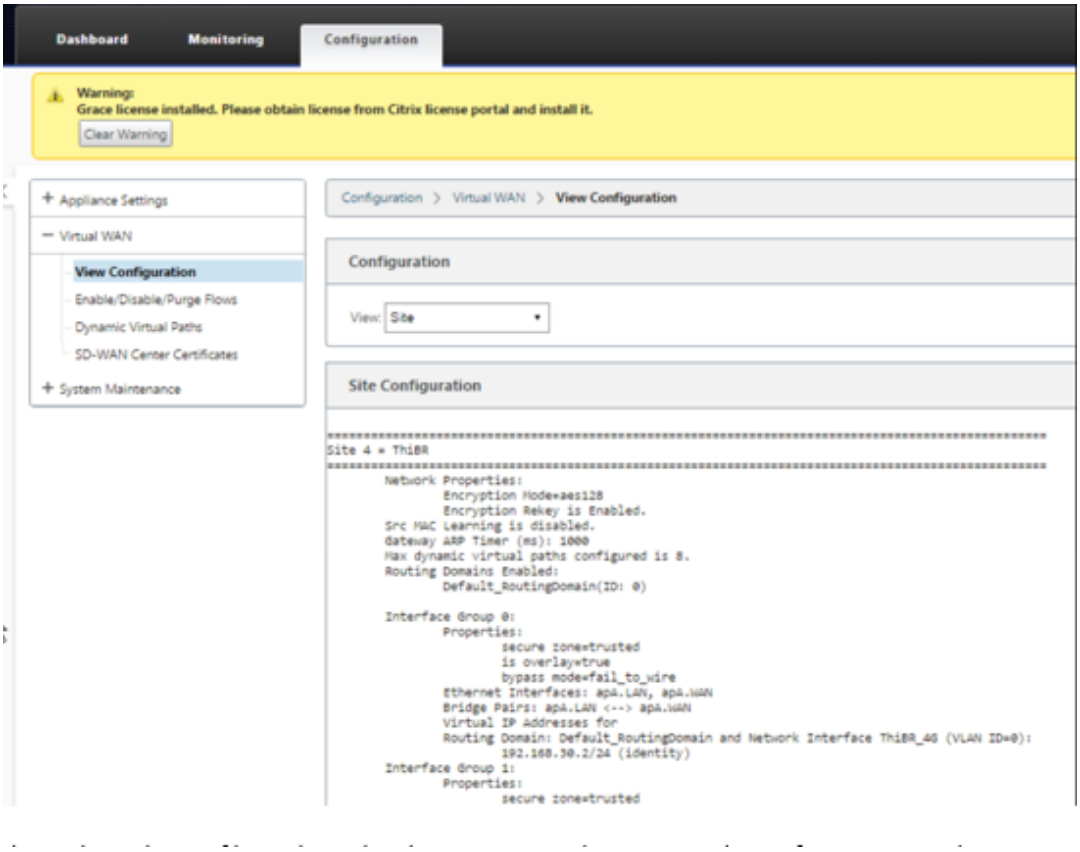
j) Web management access to the remote site appliance indicates that the appliance has been installed with a temporary Grace License at 10 Mbps, which enables the ability for the Virtual Path Service Status to report as active.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

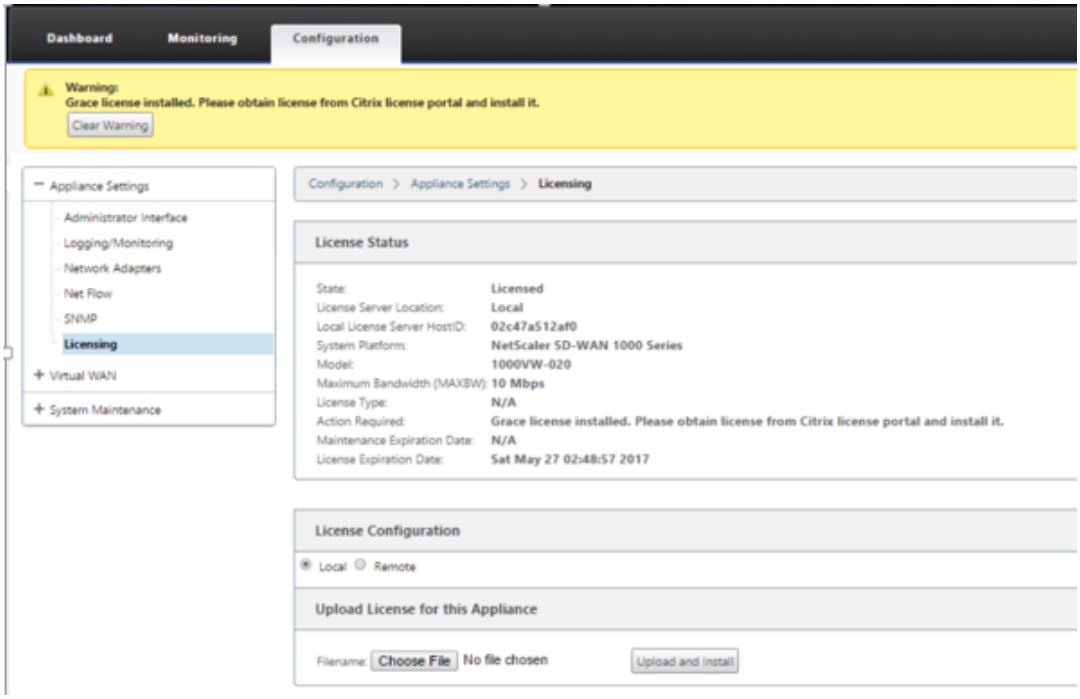


k) The appliance configuration can be validated using the **Configuration** > **Virtual WAN** > **View Configuration** page.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



l) The appliance license file can be updated to a permanent license using the **Configuration** > **Appliance Settings** > **Licensing** page.



m) After uploading and installing the permanent license file, the Grace License warning ban-

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

ner disappears and during the license install process no loss in connectivity to the remote site will occur (zero pings are dropped).

On-prem zero touch

March 12, 2021

For instructions about how to deploy an SD-WAN appliance with Zero Touch Service, see the topic; How to Configure Zero Touch Deployment Service.

AWS

March 12, 2021

Deploying in AWS

With SD-WAN release 9.3, zero touch deployment capabilities have extended to Cloud instances. The procedure to deploy zero touch deployment process four cloud instances is slightly different from appliance deployment for zero touch service.

1. Update the configuration to add a new remote site with a ZTD capable SD-WAN cloud device using SD-WAN Center Network Configuration.

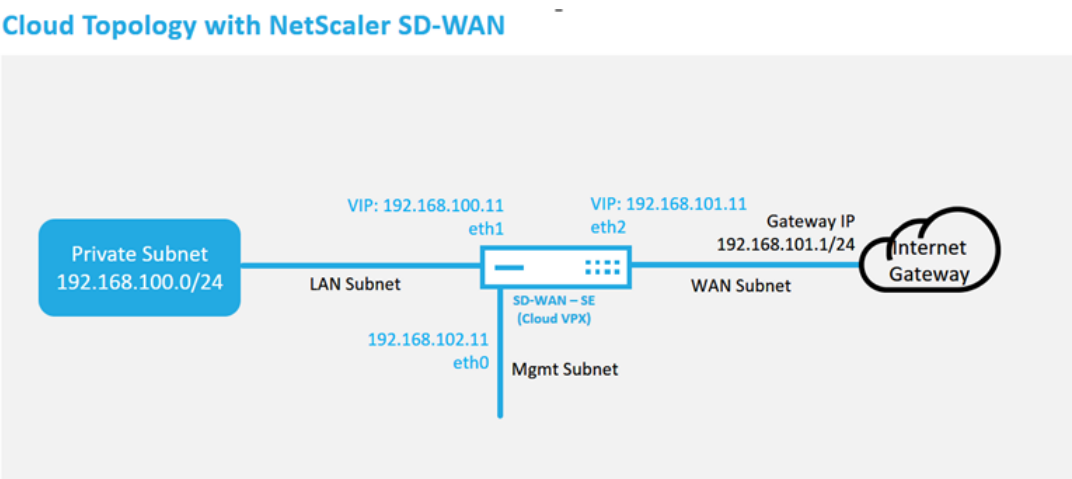
   If the SD-WAN configuration was not built using the SD-WAN Center Network Configuration, import the active configuration from the MCN and begin modifying the configuration using SD-WAN Center. For Zero Touch Deployment capability, the SD-WAN Administrator must build the configuration using SD-WAN Center. The following procedure should be used to add a new cloud node targeted for zero touch deployment.

   a) Design the new site for SD-WAN cloud deployment by first outlining the details of the new site (i.e. VPX size, Interface Groups usage, Virtual IP Addresses, WAN Link(s) with bandwidth and their respective Gateways).

   > **Note**
   >
   > - Cloud deployed SD-WAN instances must be deployed in Edge/Gateway mode.
   > - The template for the cloud instance is limited to three interfaces; Management, LAN, and WAN (in that order).
   > - The available cloud templates for SD-WAN VPX are currently hard-set to obtain

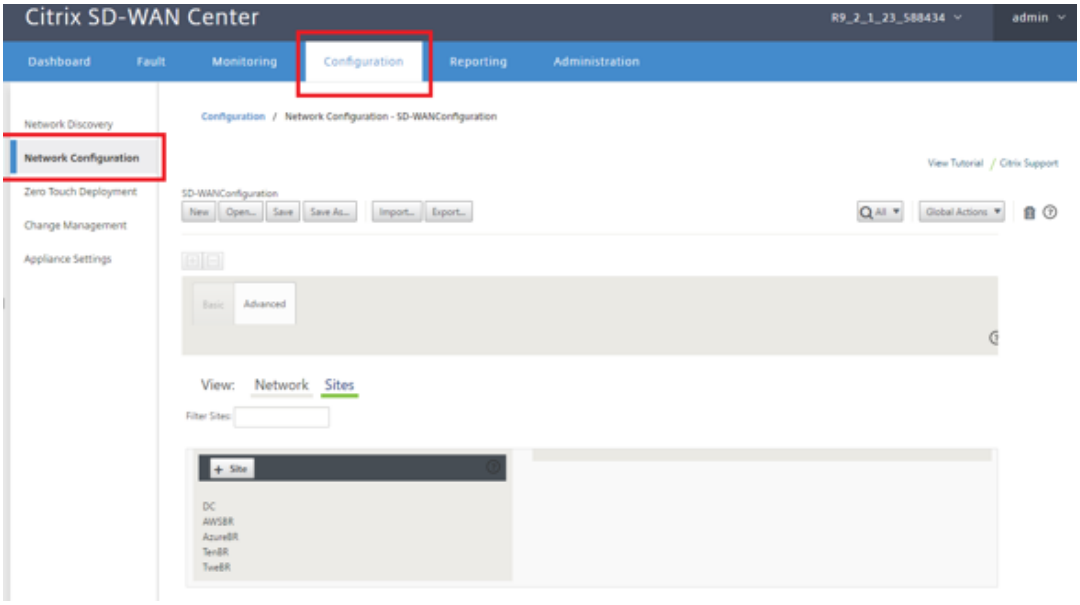
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> the #.#.#.#.11 IP address of the available subnets in the VPC .



This is an example deployment of a SD-WAN cloud deployed site, the Citrix SD-WAN device is deployed as the edge device servicing a single Internet WAN link in this cloud network. Remote sites will be able to leverage multiple distinct Internet WAN links connecting into this same Internet Gateway for the cloud, providing resiliency and aggregated bandwidth connectivity from any SD-WAN deploy site to the cloud infrastructure. This provides cost effective and highly reliable connectivity to the cloud.

b) Open the SD-WAN Center web management interface and navigate to the **Configuration** > **Network Configuration** page.



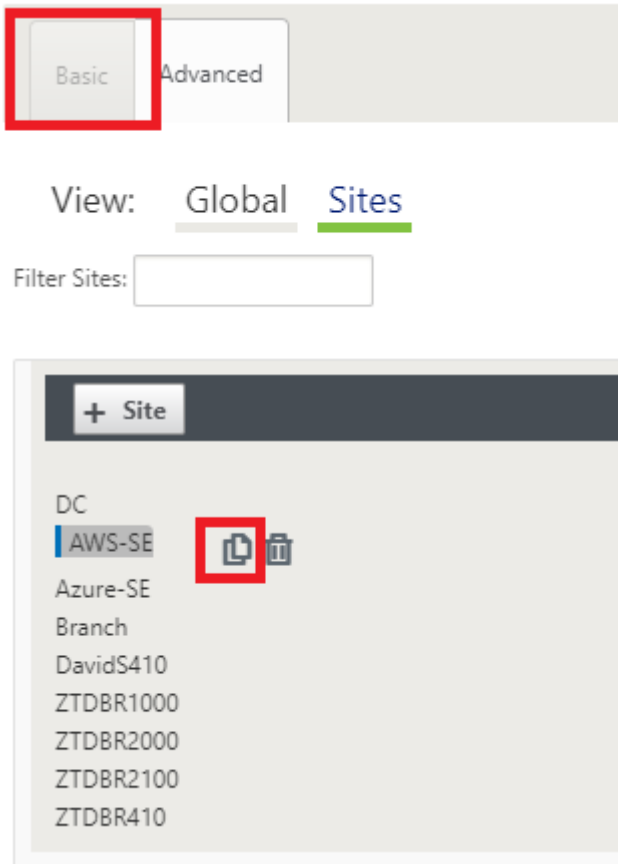
c) Make sure a working configuration is already in place, or import the configuration from the MCN.

d) Navigate to the Basic tab to create a new site.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

e) Open the Sites tile to display the currently configured sites.

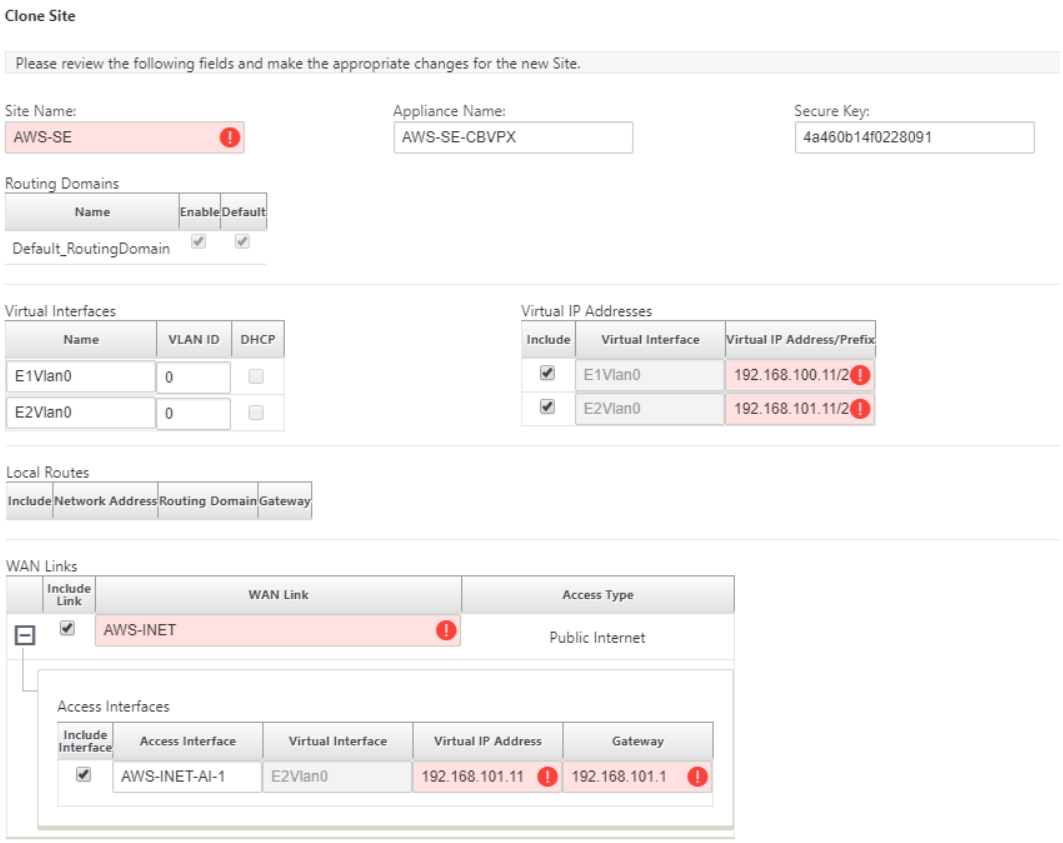
f) Quickly built the configuration for the new cloud site by utilizing the clone feature of any existing site, or manually build a new site.



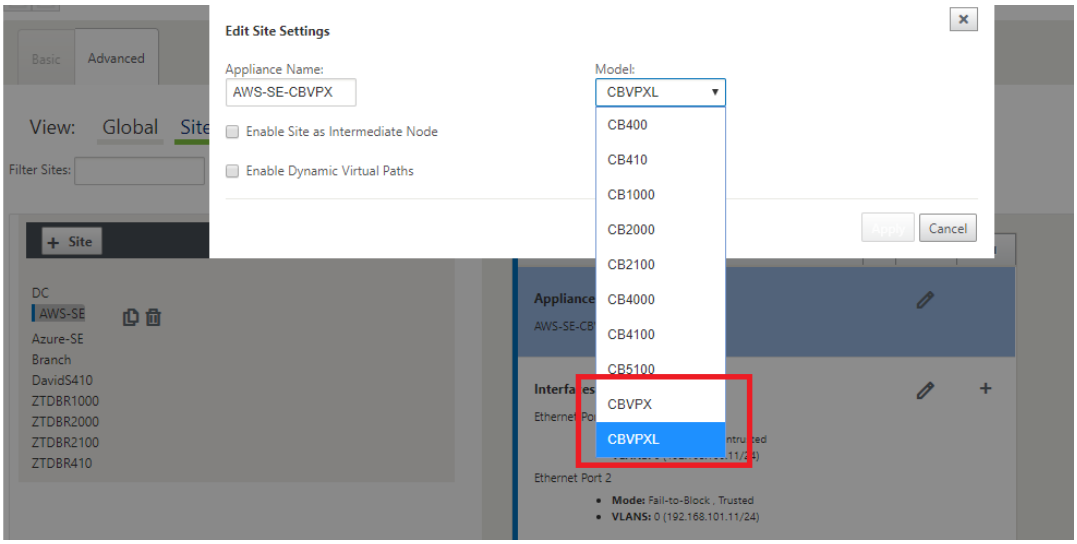
g) Populate all the required fields from the topology designed earlier for this new cloud site

Keep in mind that the template available for cloud ZTD deployments are hard-set to utilize the #.#.#.11 IP address for the Mgmt, LAN, and WAN subnets. If the configuration is not set to match the expected .11 IP host address for each interface, then the device will not be able to properly establish ARP to the cloud environment gateways and IP connectivity to the Virtual Path of the MCN.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



h) After cloning a new site, navigate to the site's **Basic Settings**, and verify that the Model of SD-WAN is correctly selected which would support the zero touch service.

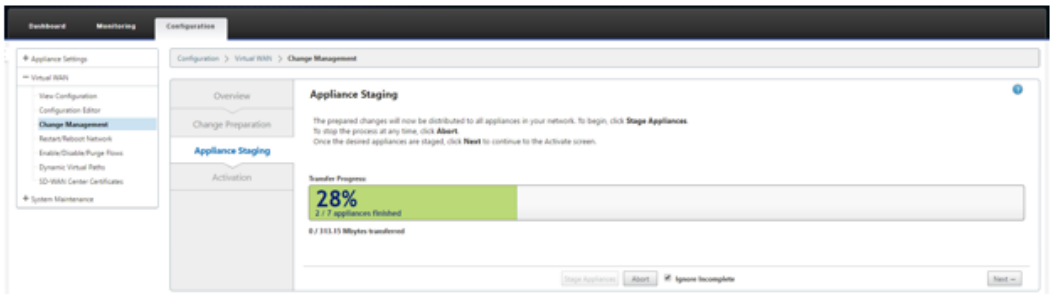


i) Save the new configuration on SD-WAN Center, and use the export to the "**Change Management inbox**"option to push the configuration using Change Management.

j) Follow the Change Management procedure to properly stage the new configuration, which

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

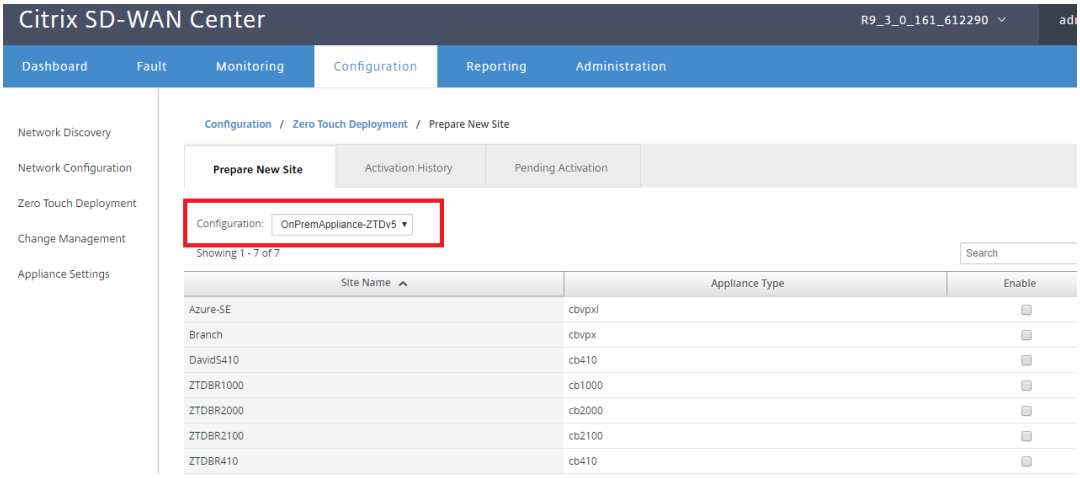
makes the existing SD-WAN devices aware of the new site to be deployed via zero touch, you will need to utilize the "*Ignore Incomplete*"option to skip attempting to push the configuration to the new site that still needs to go through the ZTD workflow.



2. Navigate back to the SD-WAN Center Zero Touch Deployment page, and with the new active configuration running, the new site will be available for deployment.

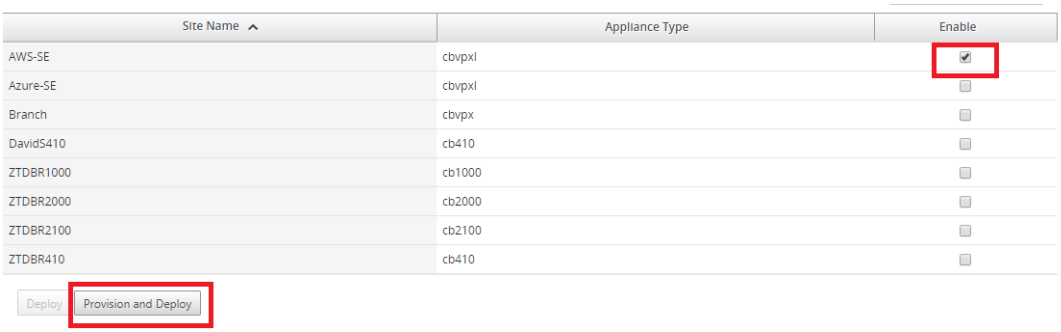
   a) In the Zero Touch Deployment page, under the **Deploy New Site** tab, select the running network configuration file.

   b) After the running configuration file is selected, the list of all the branch sites with undeployed Citrix SD-WAN devices that are supported for zero touch will be displayed.



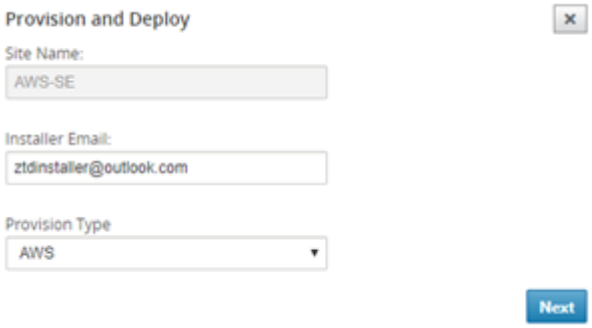
   c) Select the target cloud site you want to deploy using the Zero Touch service, click **Enable**, and then **Provision and Deploy**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

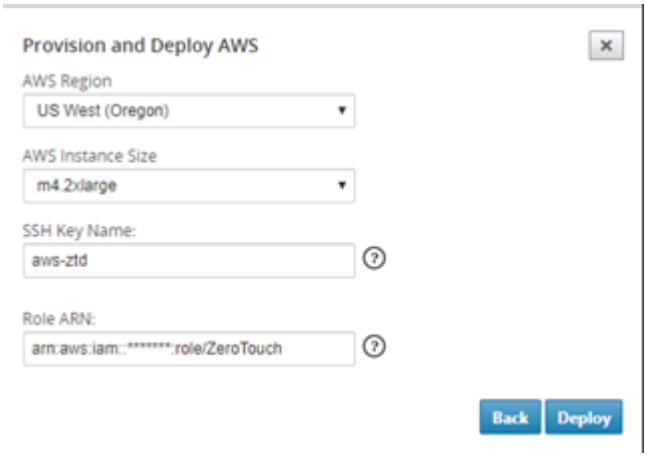


d) A pop-up window will appear, where the Citrix SD-WAN Admin can initiate the deployment for Zero Touch.

Populate an email address where the activation URL can be delivered, and select the **Provision Type** for the desired Cloud.



e) After clicking **Next**, Select the appropriate Region, Instance size, populate the SSH Key name and Role ARN fields appropriately.



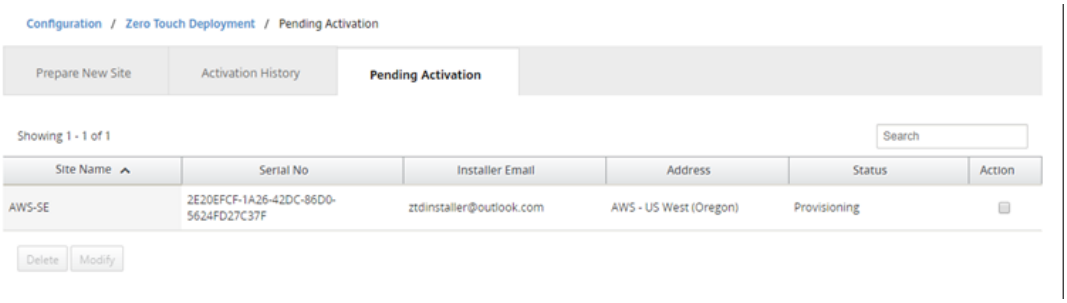
> **Note**
>
> Make use of the help links for guidance on how to setup the SSH Key and Role ARN on the Cloud account. Also make sure the select region matches what is available on the account and that the selected Instance Size matches VPX or VPXL as the selected

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> model in the SD-WAN configuration.

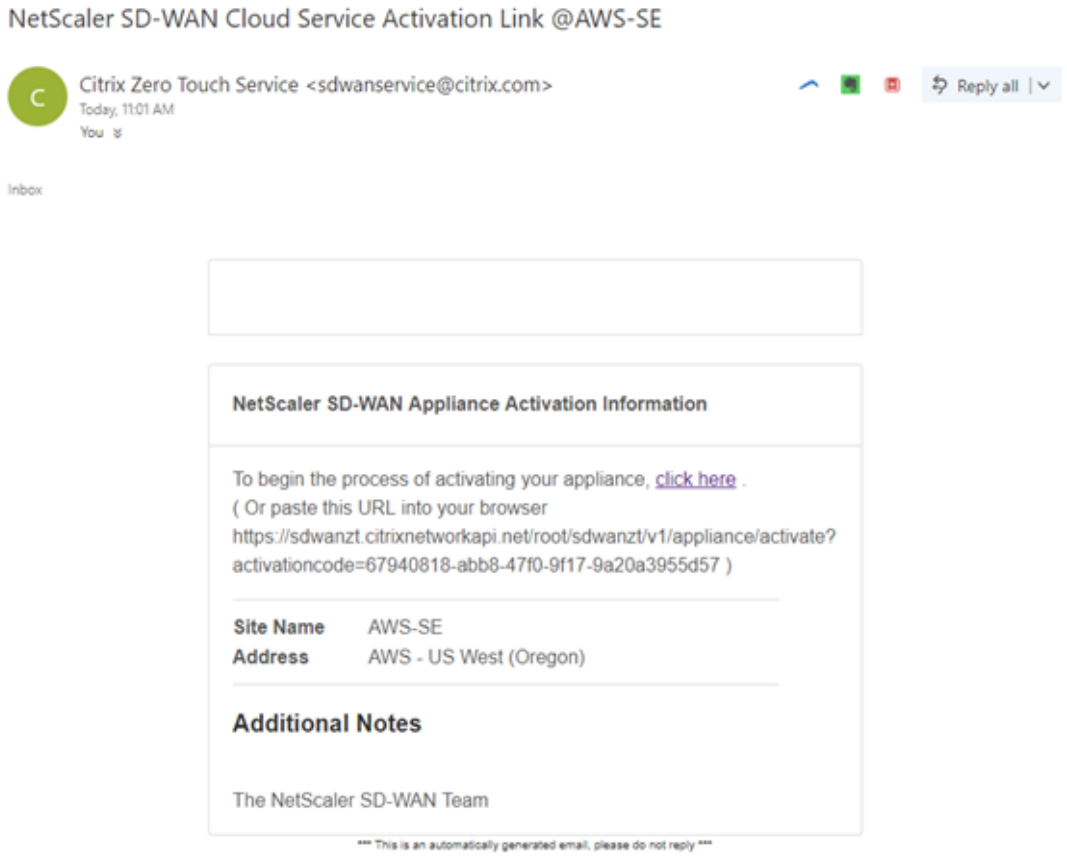
f) Click **Deploy**, triggering the SD-WAN Center, which was previously registered with the ZTD Cloud Service, to share the configuration of this site to be temporality stored in the ZTD Cloud Service.

g) Navigate to the **Pending Activation** tab to confirm that the site information populated successfully and was put into a provisioning status.



3. Initiate the Zero Touch Deployment process as the Cloud Admin.

a) The Installer will need to check the mailbox of the email address the SD-WAN Administrator used when deploying the site.

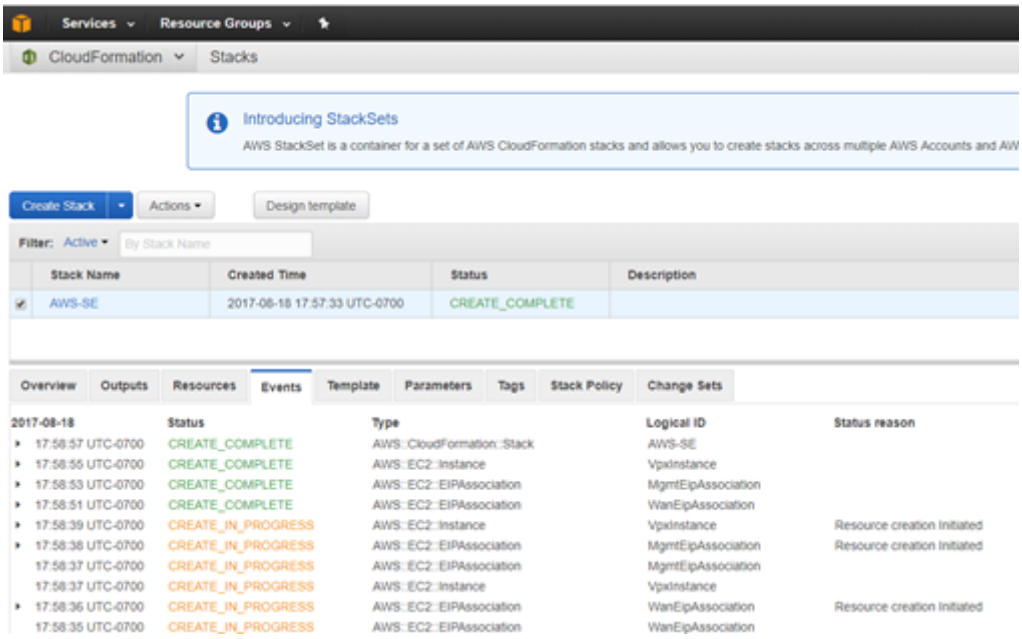


© 1999–2025 Cloud Software Group, Inc. All rights reserved.

b) Open the activation URL found in the email in an internet browser window.

c) If the SSH Key and Role ARN are properly inputted, the Zero Touch Deployment Service will immediately start provisioning the SD-WAN instance, otherwise connections errors will immediately be displayed.

d) For additional troubleshooting on the AWS console, the Cloud Formation service can be utilized to catch any events that occur during the provisioning process.

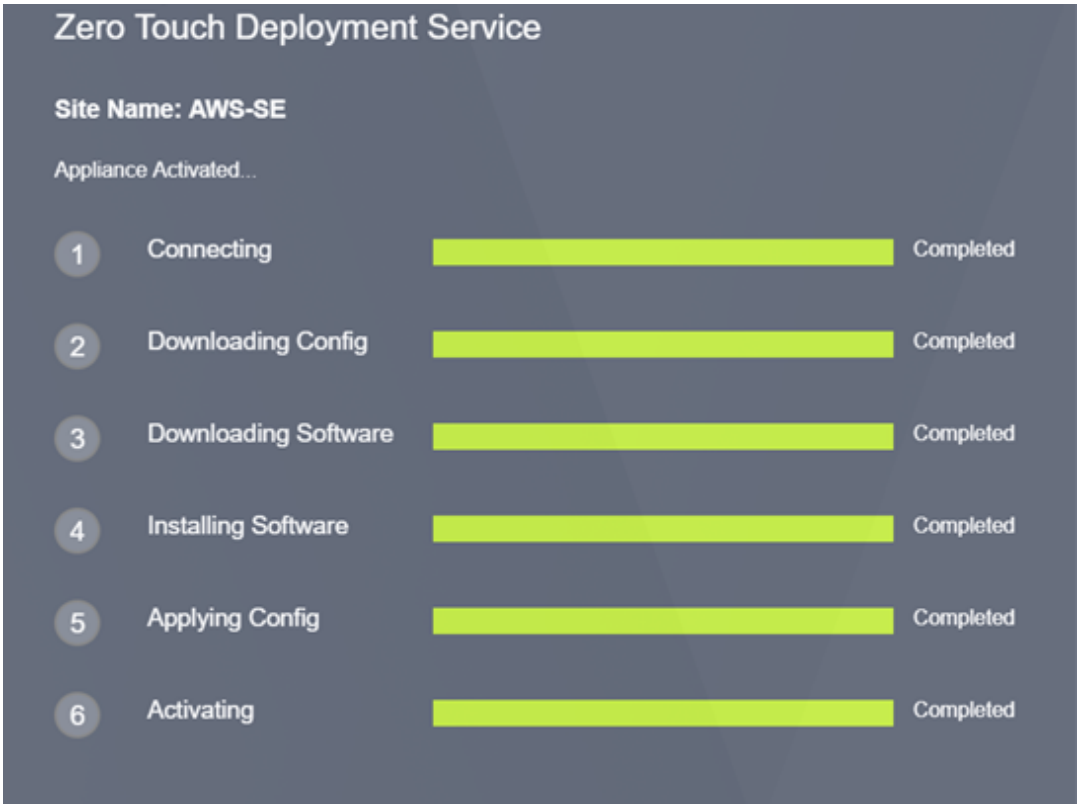


© 1999–2025 Cloud Software Group, Inc. All rights reserved.

e) Allow the provisioning process ~8-10 minutes and activation another ~3-5 minutes to fully complete.

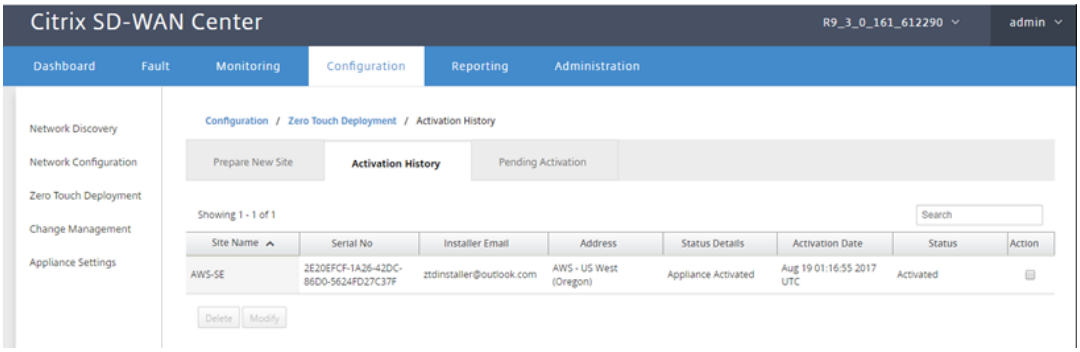
f) With successful connectivity of the SD-WAN cloud instance to the ZTD Cloud Service, the service will automatically perform the following:

- Download the site-specific Configuration File that was stored earlier by the SD-WAN Center
- Applying the Configuration to the local instance
- Download and Install a temporary 10 MB license file
- Download and Install any software updates if needed
- Activate the SD-WAN Service

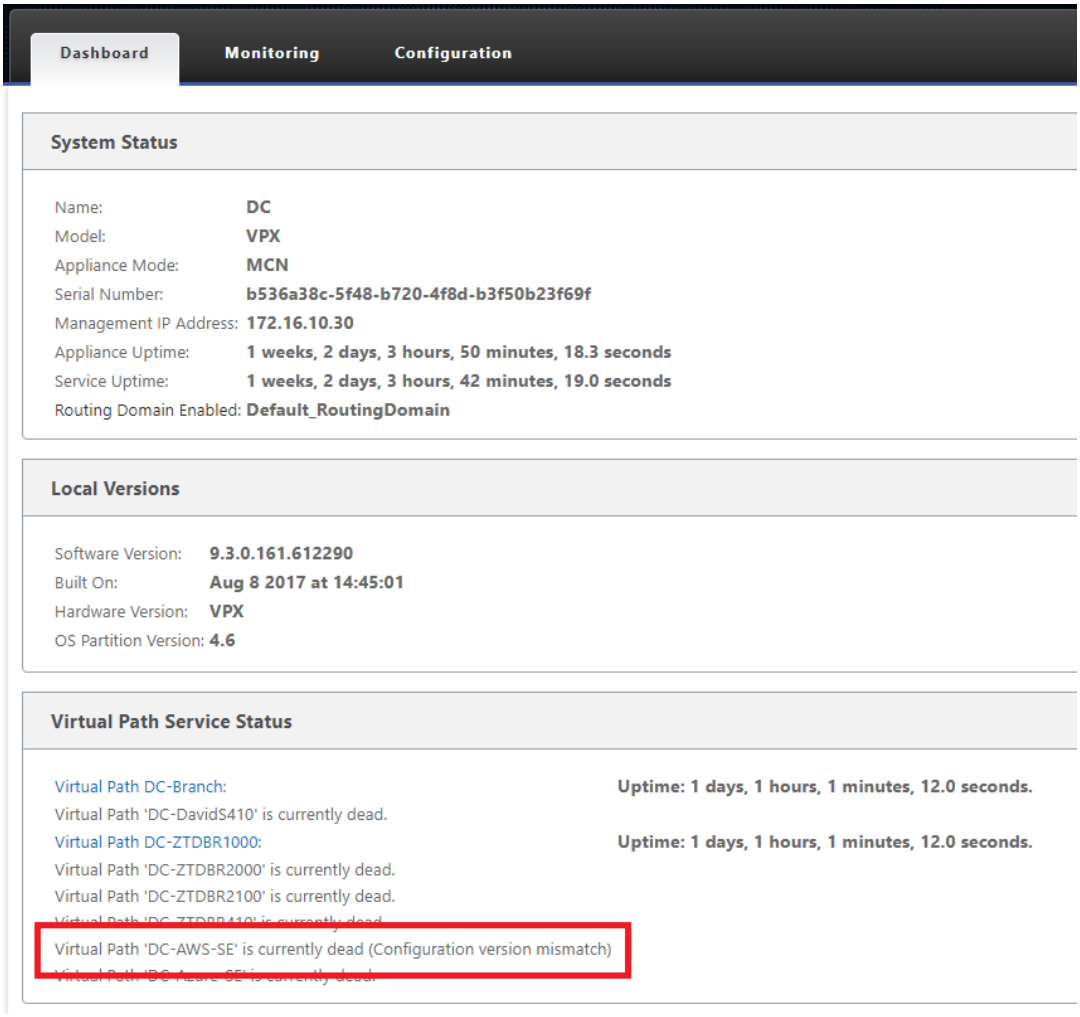


g) Further confirmation can be done in the SD-WAN Center web management interface; the Zero Touch Deployment menu will display successfully activated appliances in the **Activation History** tab.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

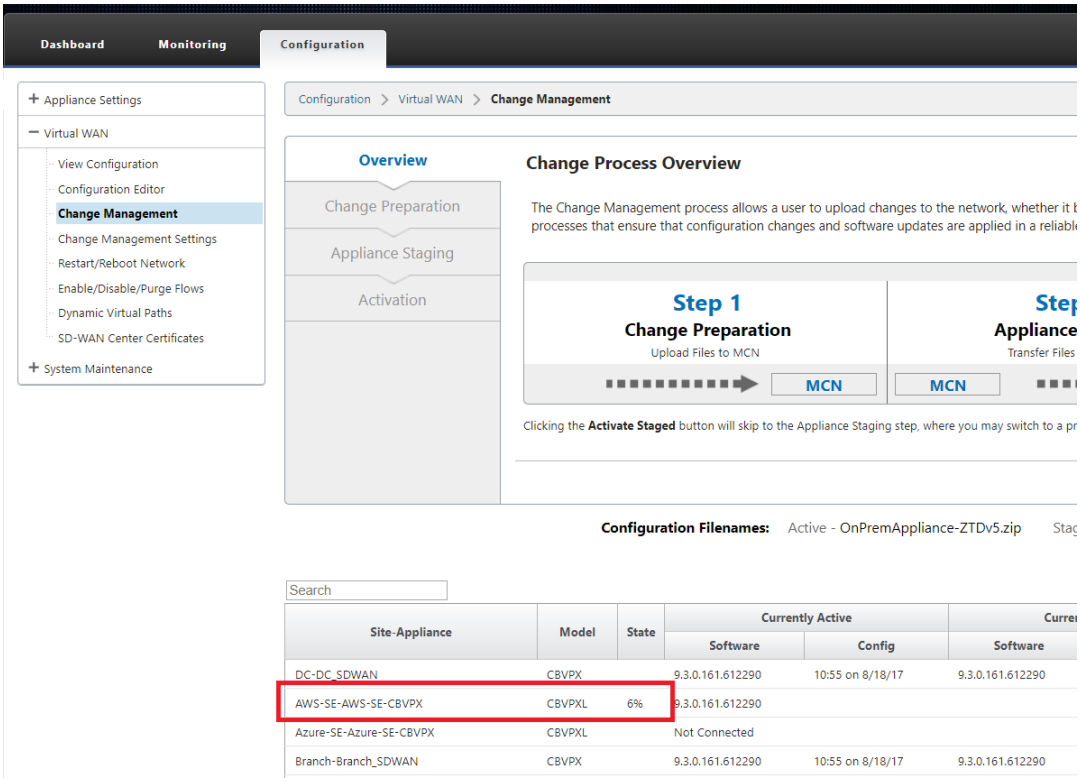


h) The Virtual Paths may not immediately show in a connected state, this is because the MCN may not trust the configuration handed down from the ZTD Cloud Service, and will report "*Configuration version mismatch*"in the MCN Dashboard.

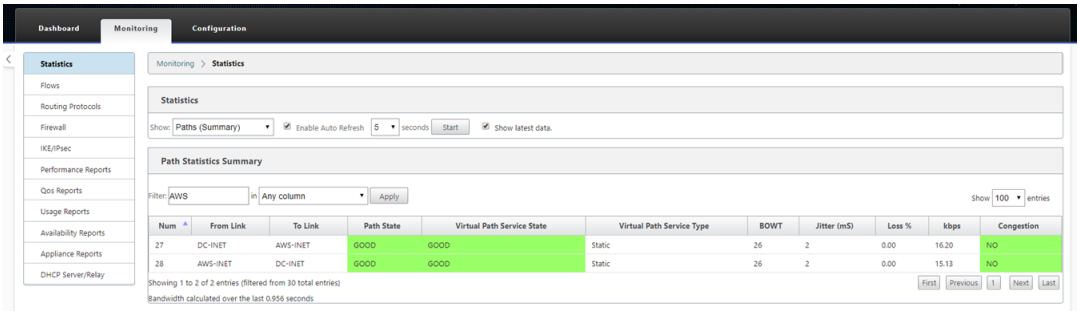


i) The configuration will automatically be redelivered to the newly installed branch office appliance, the status of this can be monitoring on the **MCN** > **Configuration** > **Virtual WAN**> **Change Management** page (depending on the connectivity, this process can take several minutes to complete).

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

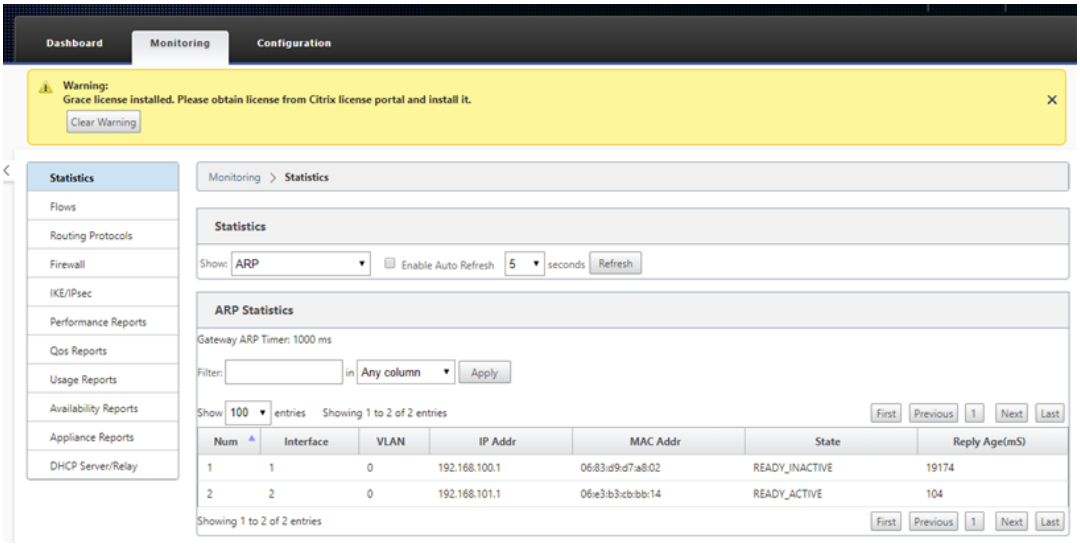


j) The SD-WAN Administrator can monitor the head-end MCN web management page for the established Virtual Paths of the newly added cloud site.



k) If troubleshooting is required, open the SD-WAN instances user interface using the public IP assigned by the cloud environment during provisioning, and utilize the ARP table in the **Monitoring** > **Statistics** page to identify any issues connecting to the expected gateways, or utilize the trace route and packet capture options in diagnostics.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Azure

March 12, 2021

With SD-WAN release 9.3, zero touch deployment capabilities have extended to Cloud instances. The procedure to deploy zero touch deployment process for cloud instances is slightly different from appliance deployment for zero touch service.

Updating the configuration to add a new remote site with a ZTD capable SD-WAN cloud device using SD-WAN Center Network Configuration

If the SD-WAN configuration was not built using the SD-WAN Center Network Configuration, import the active configuration from the MCN and begin modifying the configuration using SD- WAN Center. For Zero Touch Deployment capability, the SD-WAN Administrator must build the configuration using SD-WAN Center. The following procedure should be used to add a new cloud node targeted for zero touch deployment.

1. Design the new site for SD-WAN cloud deployment by first outlining the details of the new site (i.e. VPX size, Interface Groups usage, Virtual IP Addresses, WAN Link(s) with bandwidth and their respective Gateways).

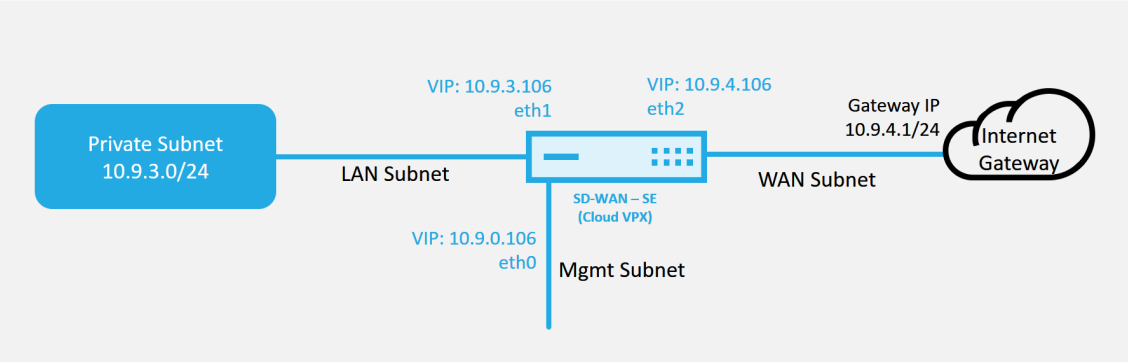
   > **Note**
   >
   > - Cloud deployed SD-WAN instances must be deployed in Edge/Gateway mode.
   > - The template for the cloud instance is limited to three interfaces; Management, LAN,

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

and WAN (in that order).

- The available Azure cloud templates for SD-WAN VPX are currently hard-set to obtain the 10.9.4.106 IP for the WAN, 10.9.3.106 IP for the LAN, and 10.9.0.16 IP for the Management address. The SD-WAN configuration for the Azure node targeted for Zero Touch must match this layout.
- The Azure site name in the configuration must be all lowercase with no special characters (e.g. ztdazure).

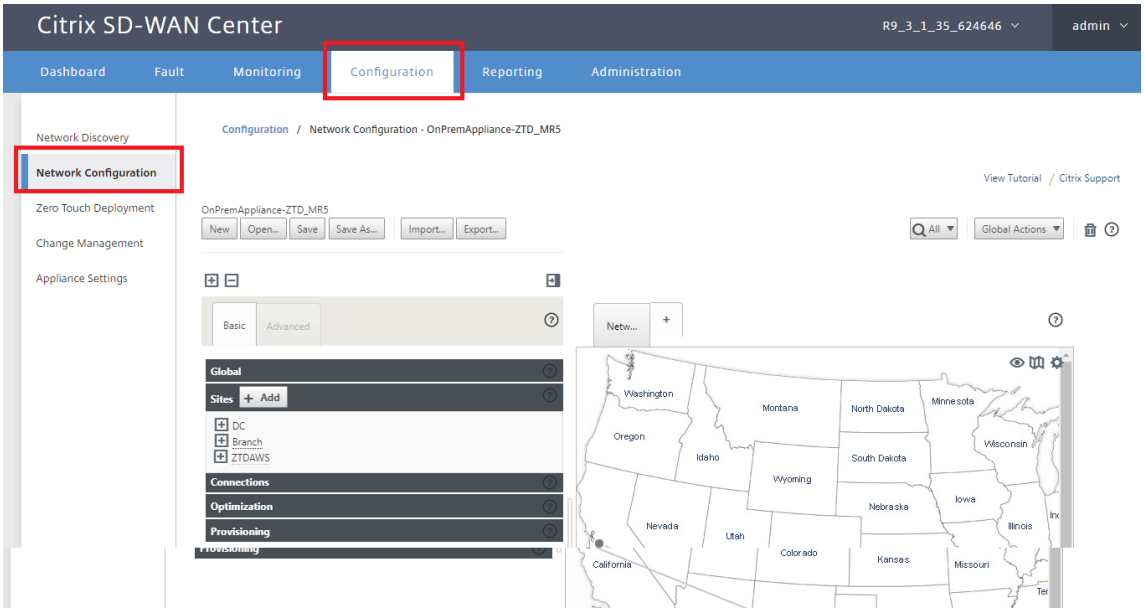
Azure Cloud Topology with NetScaler SD-WAN



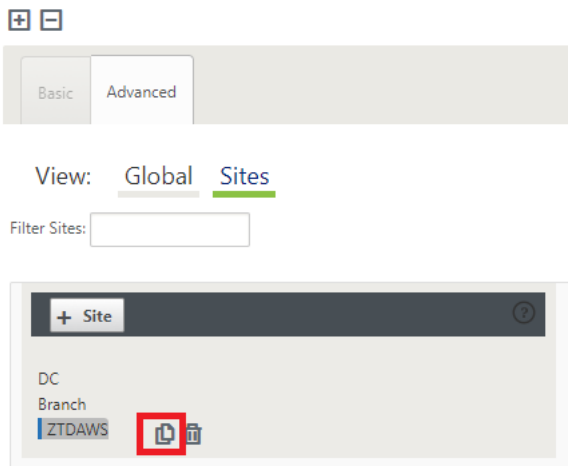
This is an example deployment of a SD-WAN cloud deployed site, the Citrix SD-WAN device is deployed as the edge device servicing a single Internet WAN link in this cloud network. Remote sites will be able to leverage multiple distinct Internet WAN links connecting into this same Internet Gateway for the cloud, providing resiliency and aggregated bandwidth connectivity from any SD-WAN deploy site to the cloud infrastructure. This provides cost effective and highly reliable connectivity to the cloud.

2. Open the SD-WAN Center web management interface and navigate to the **Configuration** > **Network Configuration** page.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



3. Make sure a working configuration is already in place, or import the configuration from the MCN.
4. Navigate to the Basic tab to create a new site.
5. Open the Sites tile to display the currently configured sites.
6. Quickly built the configuration for the new cloud site by utilizing the clone feature of any existing site, or manually build a new site.

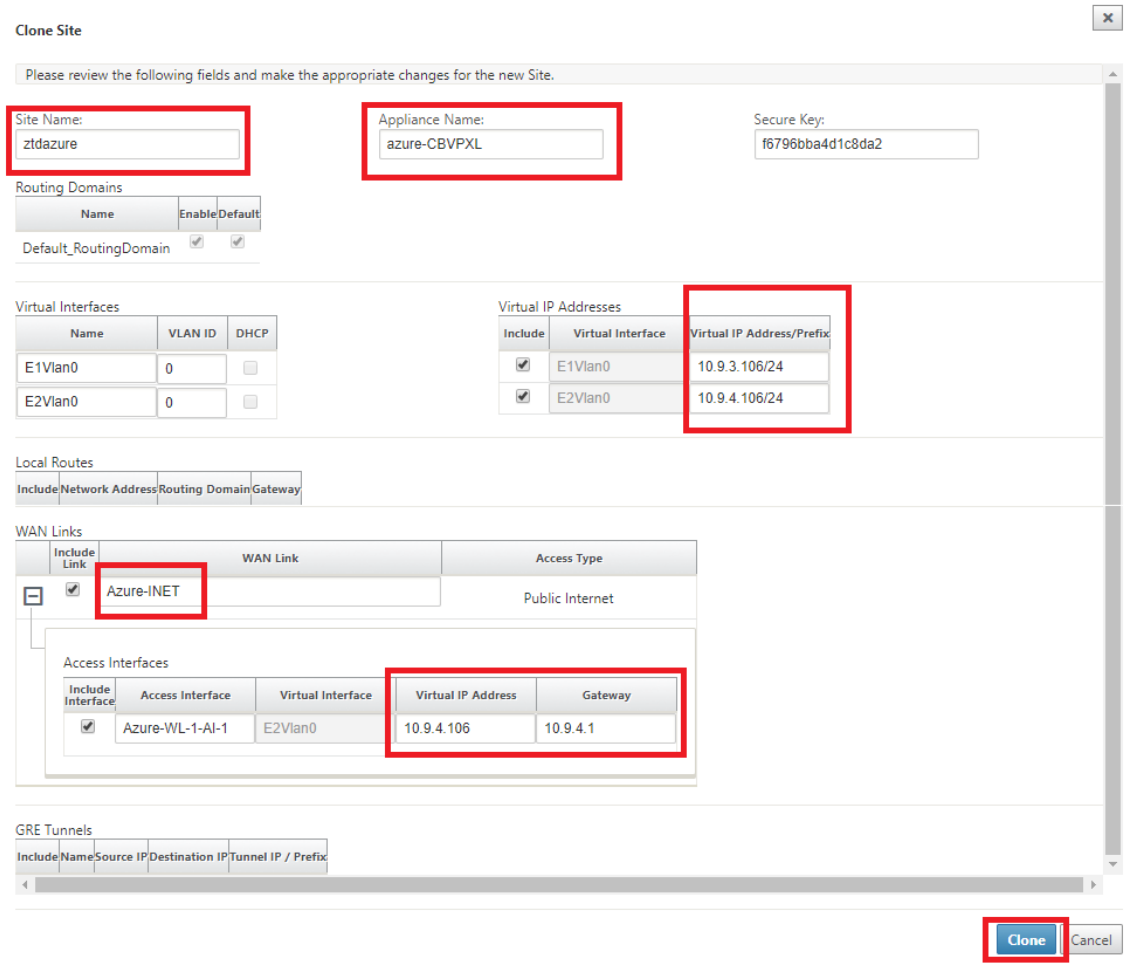


7. Populate all the required fields from the topology designed earlier for this new cloud site.

   Keep in mind that the template available for Azure cloud ZTD deployments is currently hard-set to obtain the 10.9.4.106 IP for the WAN, 10.9.3.106 IP for the LAN, and 10.9.0.16 IP for the Management address. If the configuration is not set to match the expected VIP address for each interface, then the device will not be able to properly establish ARP to the cloud environment gateways and IP connectivity to the Virtual Path of the MCN.

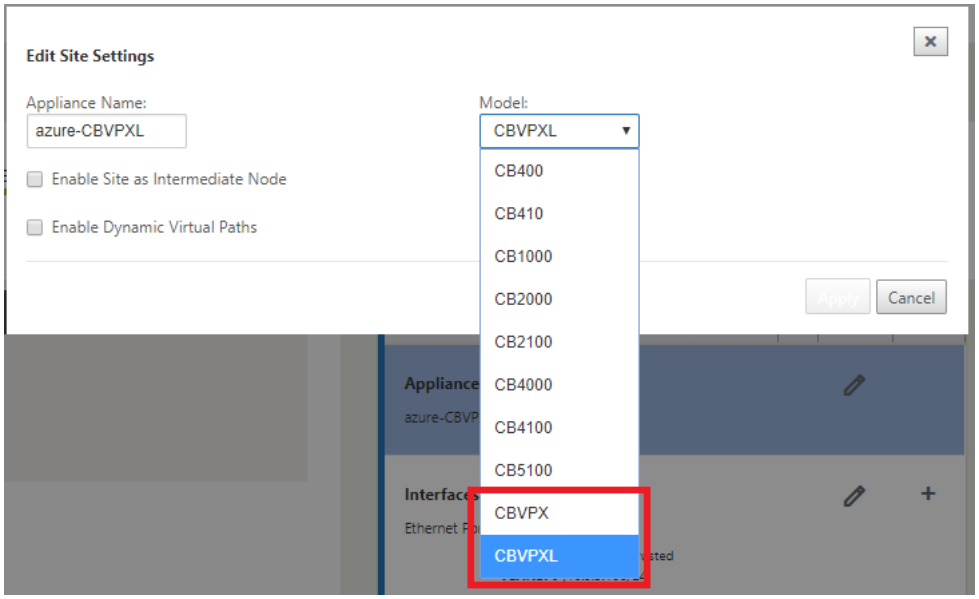
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

It is import that the site name be compliant with what Azure expects. The site name must be in all lower case, at least 6 characters, with no special characters, it must confirm to the following regular expression **^[a-z][a-z0-9-]{1,61}[a-z0-9]$.**

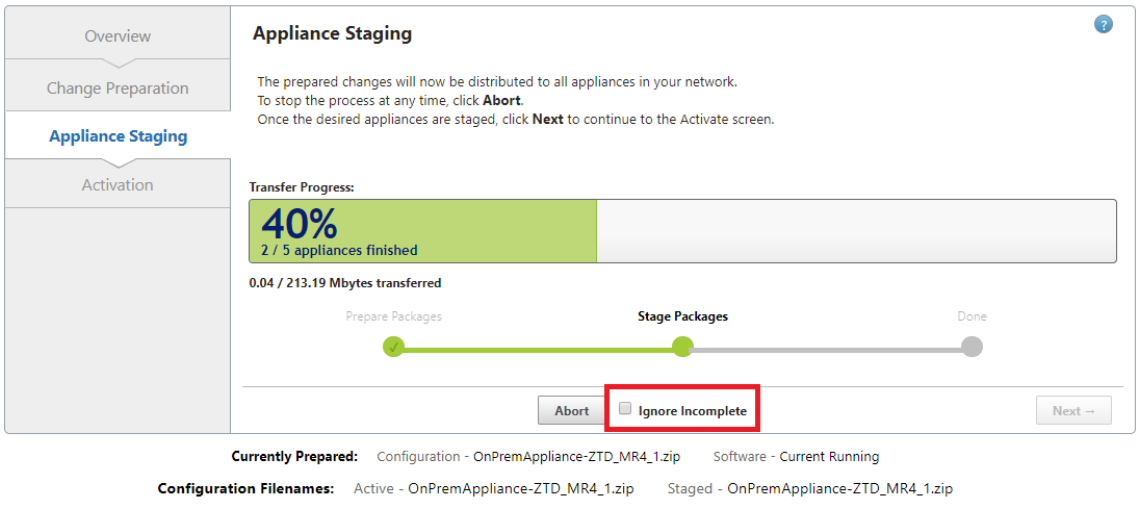


8. After cloning a new site, navigate to the site's **Basic Settings**, and verify that the Model of SD-WAN is correctly selected which would support the zero touch service.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



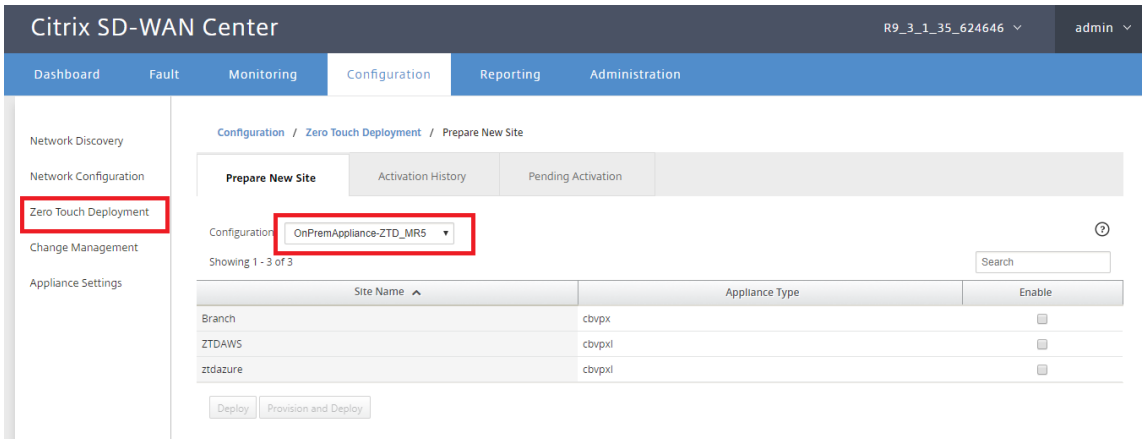
9. Save the new configuration on SD-WAN Center, and use the export to the "**Change Management inbox**"option to push the configuration using Change Management.
10. Follow the Change Management procedure to properly stage the new configuration, which makes the existing SD-WAN devices aware of the new site to be deployed via zero touch, you will need to utilize the "*Ignore Incomplete*"option to skip attempting to push the configuration to the new site that still needs to go through the ZTD workflow.



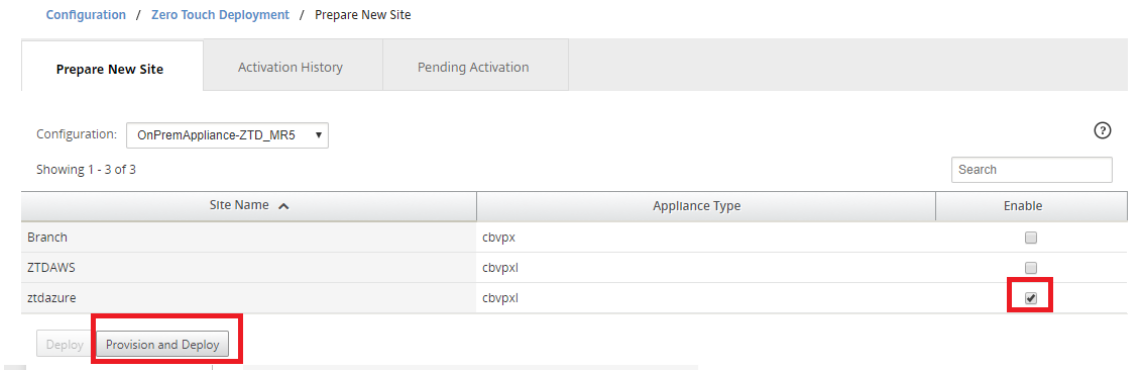
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Navigate to the SD-WAN Center's Zero Touch Deployment page, and with the new active configuration running, the new site will be available for SD-WAN Center Provision and Deploy Azure (Step 1 of 2)

1. In the Zero Touch Deployment page, login with your Citrix account credentials. Under the **Deploy New Site** tab, select the running network configuration file.
2. After the running configuration file is selected, the list of all the branch sites with ZTD capable Citrix SD-WAN devices will be displayed.

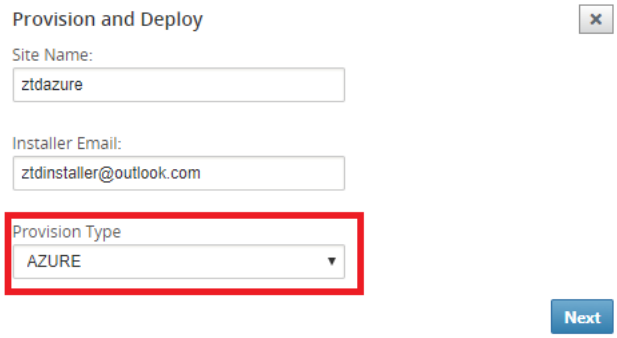


3. Select the target cloud site you want to deploy using the Zero Touch service, click **Enable**, and then click **Provision and Deploy**.



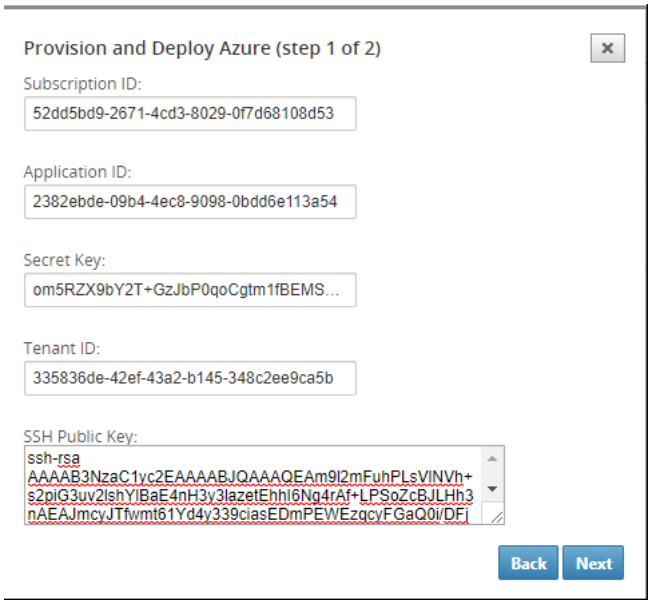
4. A pop-up window will appear, where the Citrix SD-WAN Admin can initiate the deployment for Zero Touch. Validate that the site name complys with the requirements on Azure (lowercase with no special characters). Populate an email address where the activation URL can be delivered, and select Azure as the **Provision Type** for the desired Cloud, before clicking **Next**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



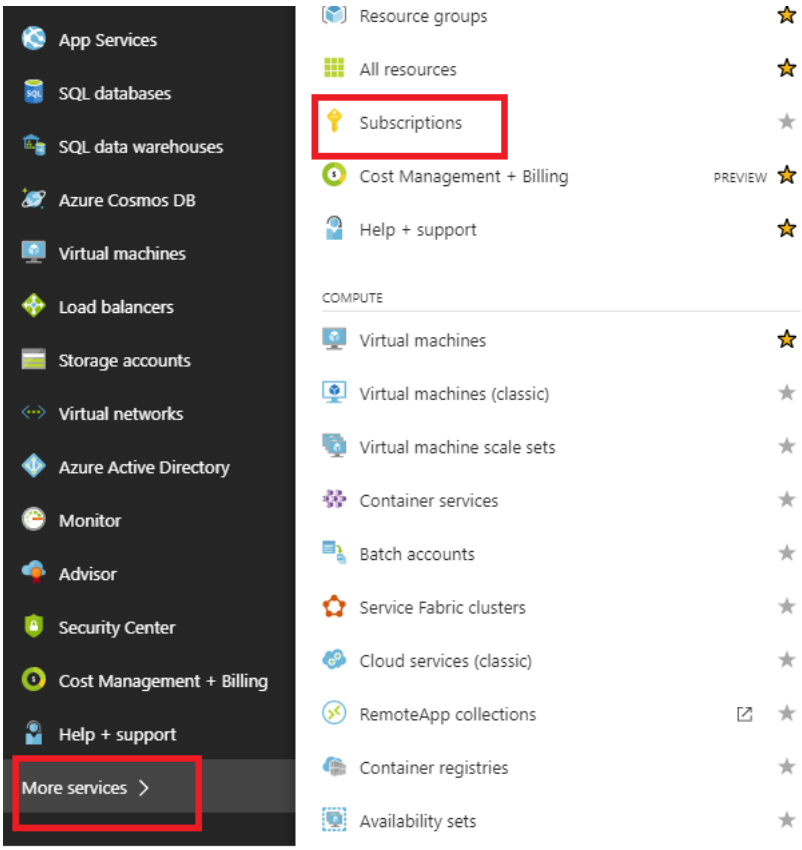
5. After clicking **Next**, the Provision and Deploy Azure (step 1of 2) window will require input of obtained from the Azure account.

   Copy and paste each required field after obtaining the information from your Azure account. The steps below outline how to obtain the required Subscription ID, Application ID, Secret Key, and Tenant ID from your Azure account, then proceed by clicking **Next**.



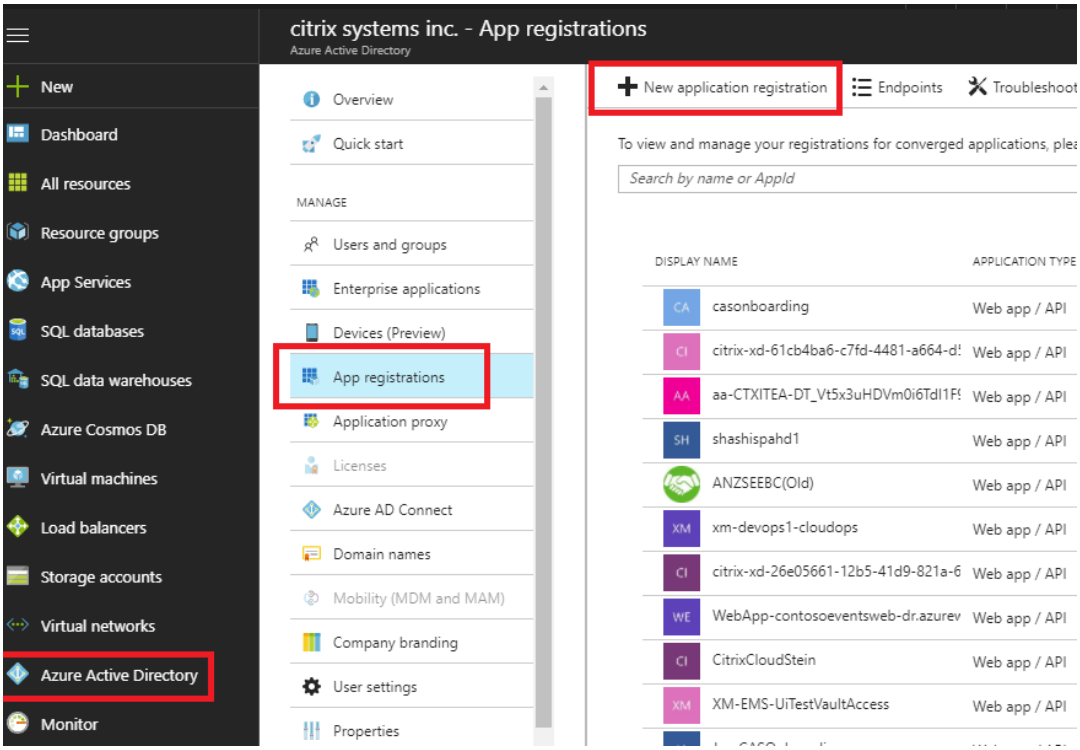
   a) On the Azure account, we can identify the required ***Subscription ID*** by navigating to "More Services"and select **Subscriptions.**

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

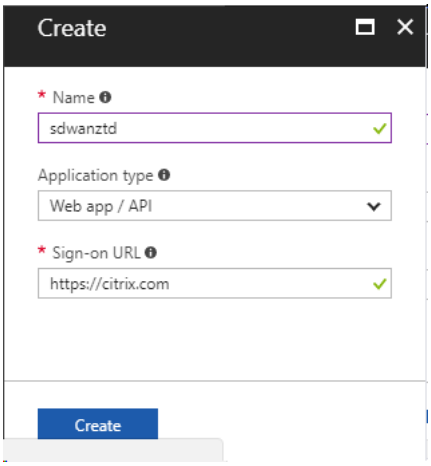


b) To identify the required ***Application ID***, navigate to Azure Active Directory, Application registrations, and click N**ew application registration.**

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

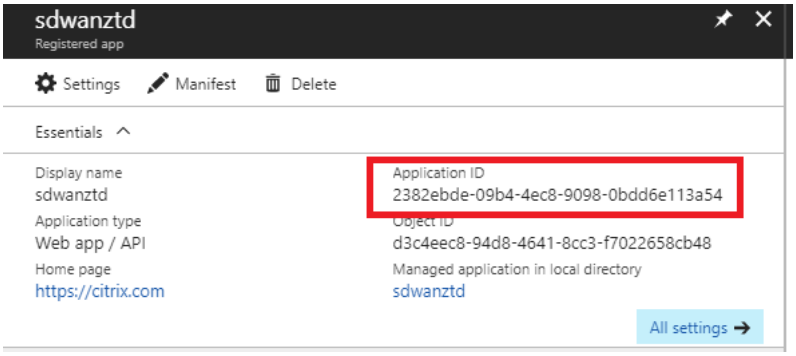


c) In the app registration create menu, enter a Name and a Sign-on URL (this can be any URL, the only requirement is that it must be valid), then click **Create**.

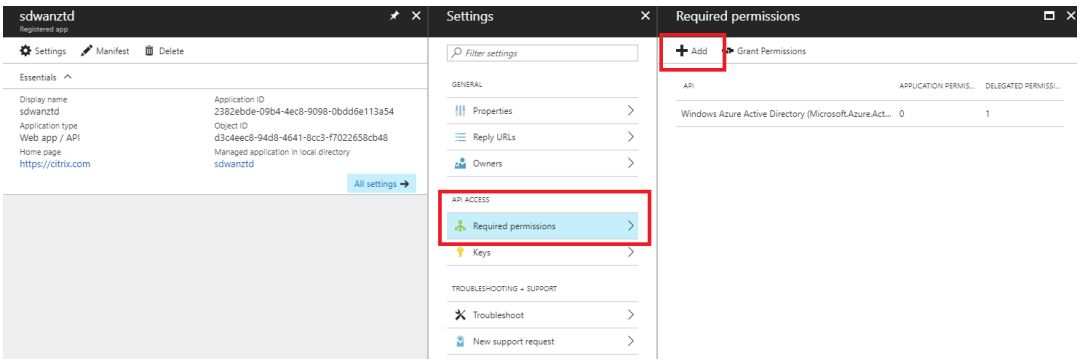


d) Search for and open the newly created Registered App, and note the Application ID.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

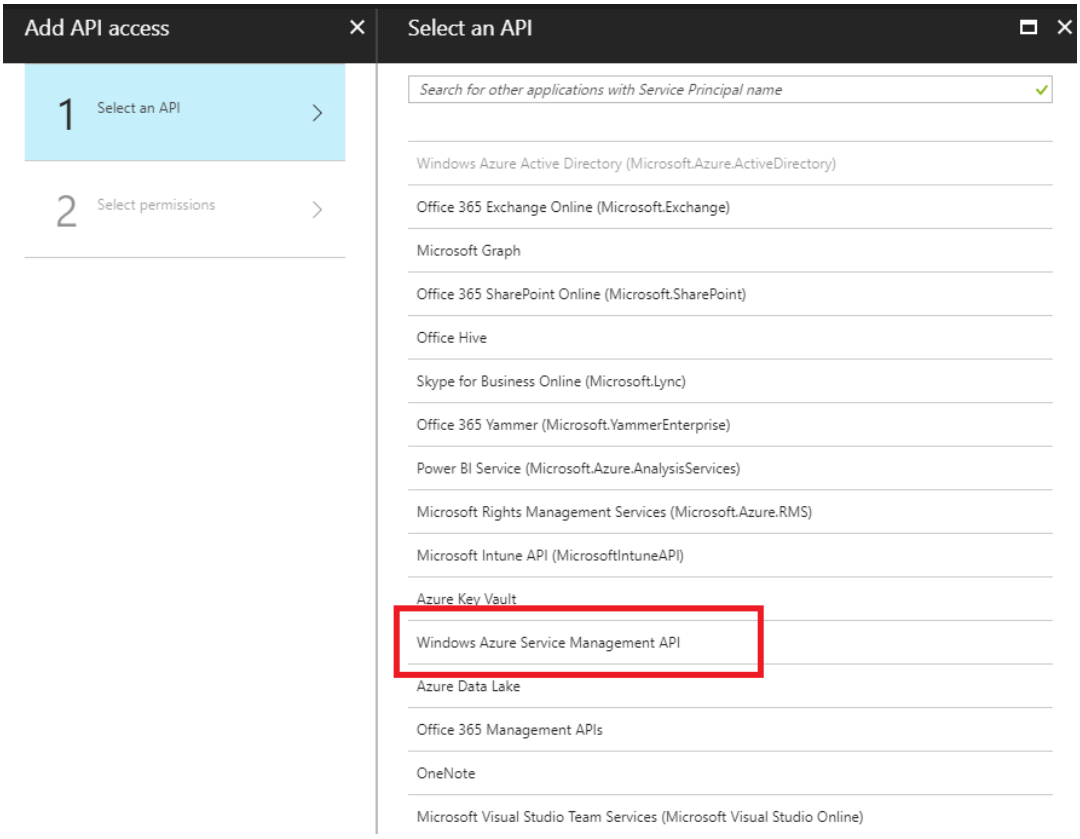


e) Again open the newly created Registration App, and to identify the required *Security Key*, under API Access, select **Required permissions,** to allow a third party to provision and instance. Then select **Add**.

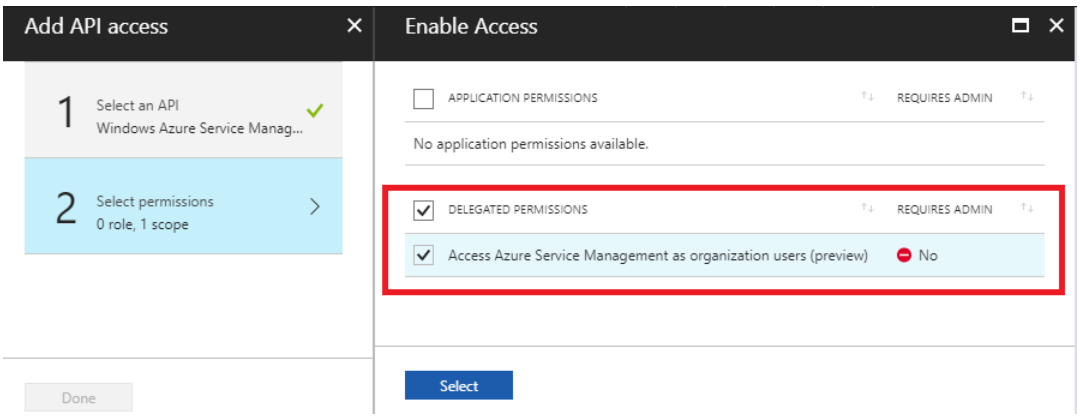


f) When adding the Required permissions, **Select an API,** then highlight **Windows Azure Service Management API.**

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

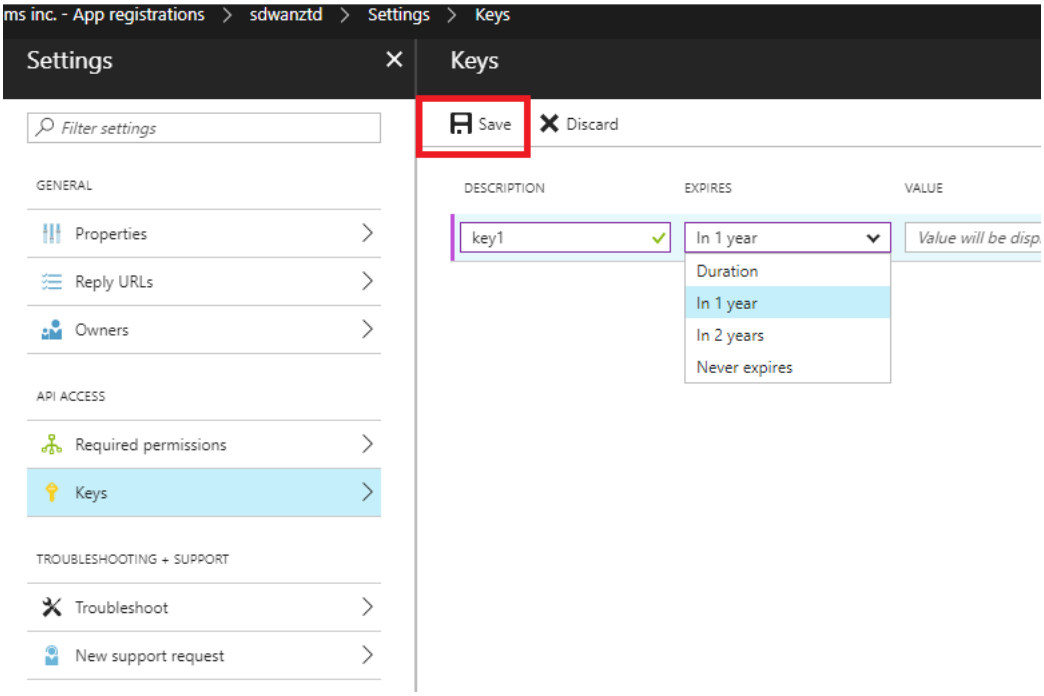


g) Enable **Delegate Permissions** to provision instances, then click **Select** and **Done**.

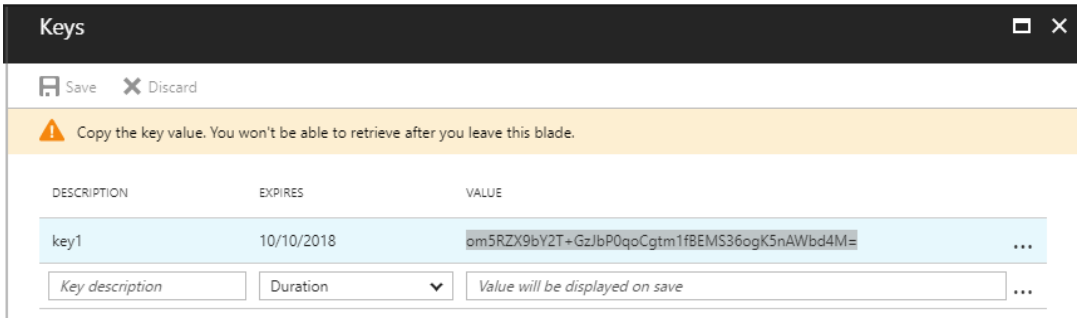


h) For this Registered App, under API Access, select **Keys,** and create a secret **key description** and the desired **duration** for the key to be valid. Then click **Save which** will produce a **secret key** (the key is only required for the provisioning process, it can be deleted after the instance is made available).

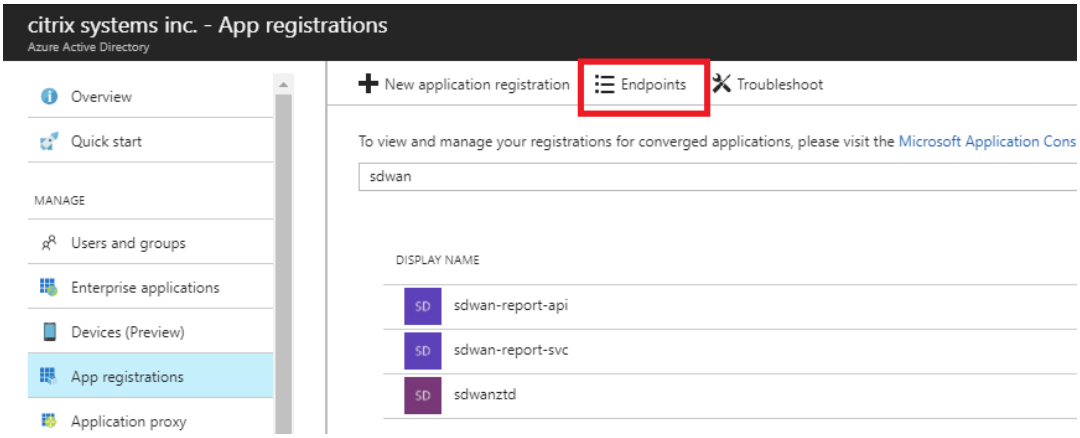
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



i) Copy and save the secret key (note you will not be able to retrieve this later).



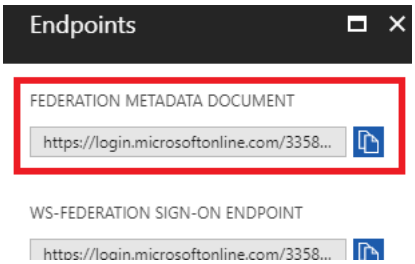
j) To identify the required ***Tenant ID*****, n**avigate back to the App registration pane, and select **Endpoints**.



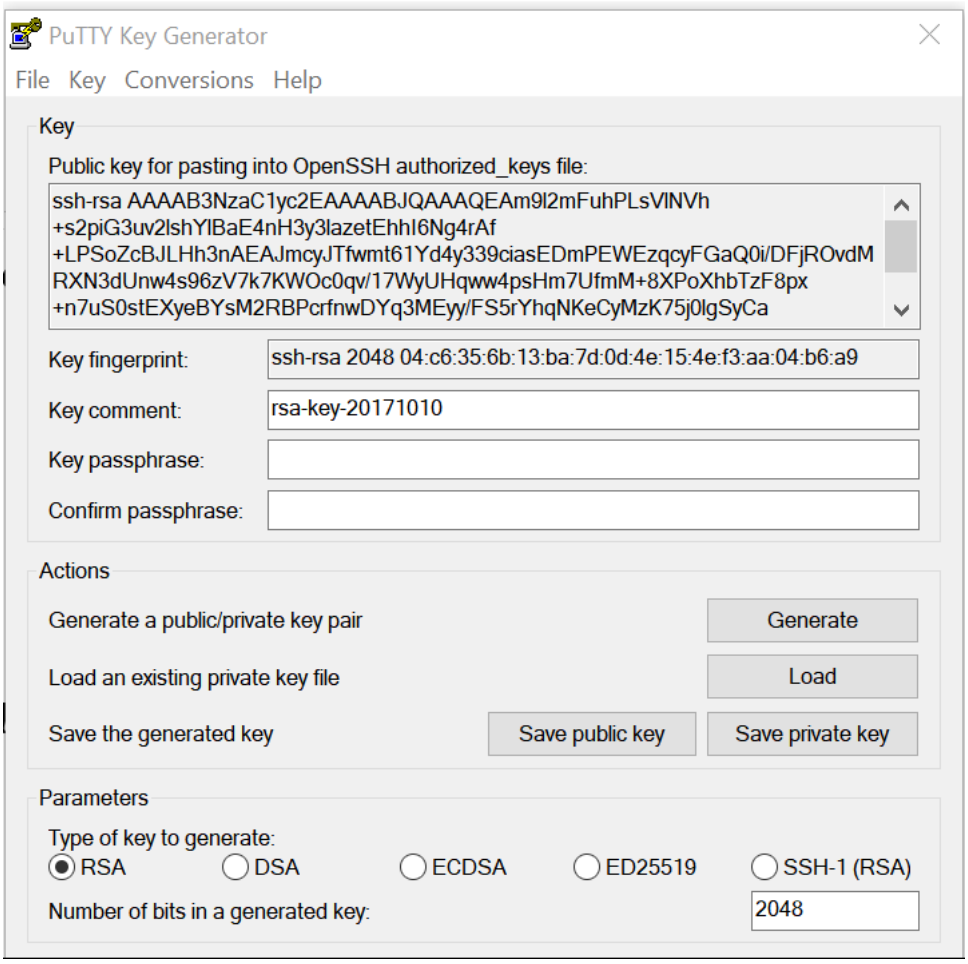
k) Copy the **Federation Metadata Document**, to identify your Tenant ID (note the Tenant ID

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

is 36-character string located between the “online.com/”and the “/federation”in the URL).

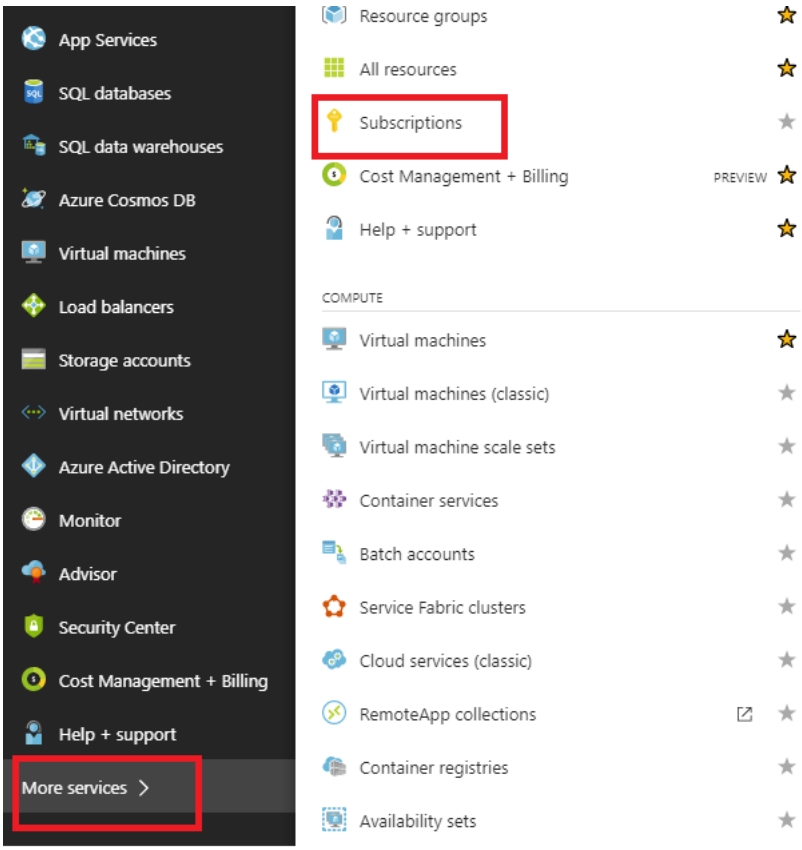


l) The last item required is the ***SSH Public Key***. This can be created using Putty Key Generator or ssh-keygen and will be utilized for authentication, eliminating the need for passwords to log in. The SSH public key can be copied (including the heading ssh-rsa and trailing rsa-key strings). This public key will be shared through SD-WAN Center input to the Citrix Zero Touch Deployment Service.

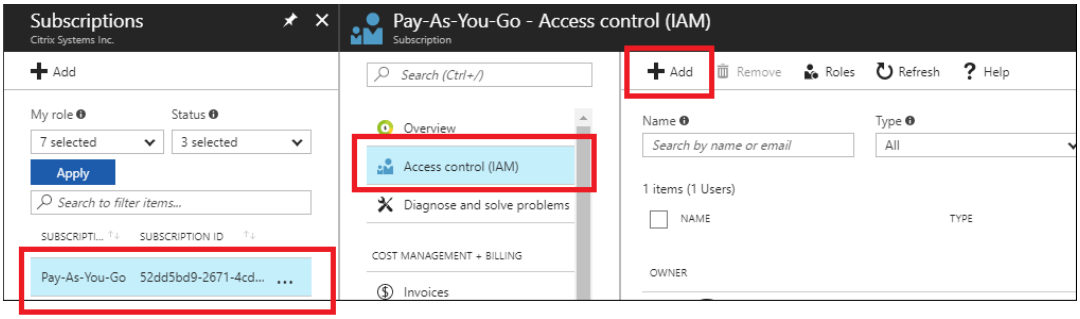


m) Additional steps are required to assign the application a role. Navigate back to More Services, then Subscriptions.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

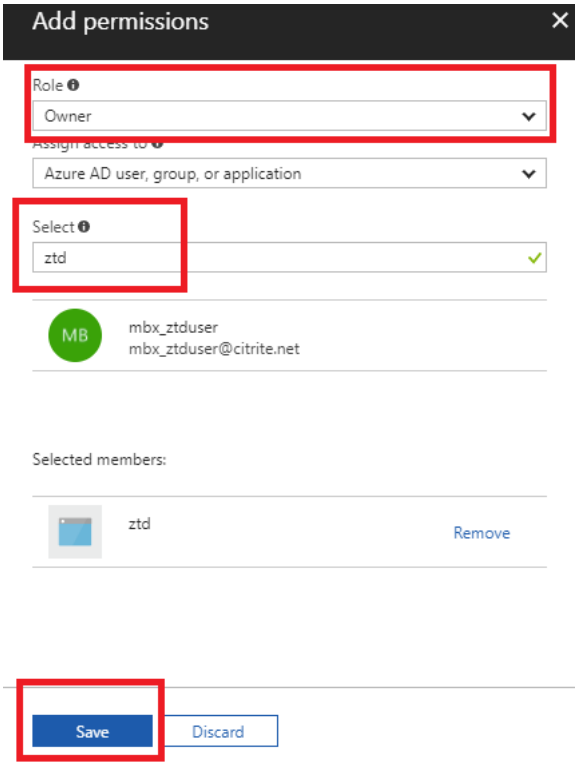


n) Select the active subscription, then **Access control (AIM)**, next click **Add.**

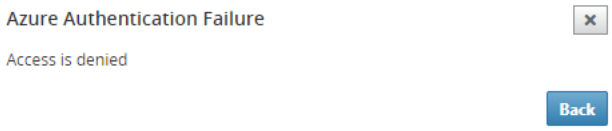


o) In the add permissions pane, select "**Owner**"role, assign access to **"Azure AD user, group, or application"** and search for the registered app in the **Select field** to allow the Zero Touch Deployment Cloud Service to create and configure the instance on the Azure subscription. Once the app is identified, select it and make sure it populates as a Selected member before clicking **Save**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



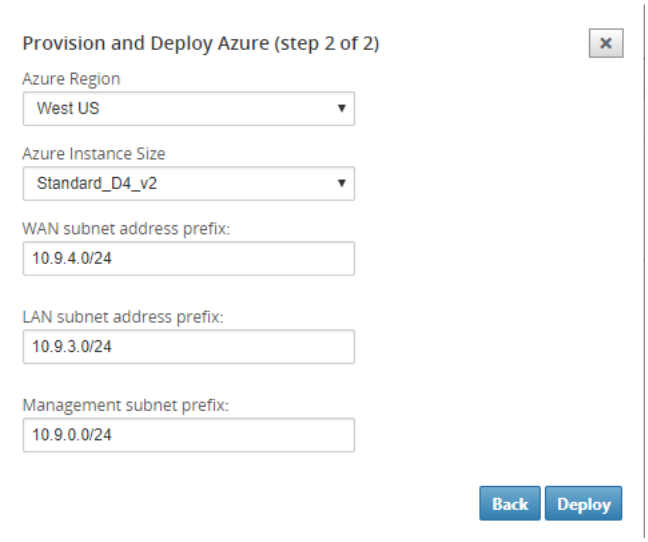
p) After collecting the required inputs and entering them into SD-WAN Center, click **Next**. If the inputs are not correct, you will encounter an authentication failure.



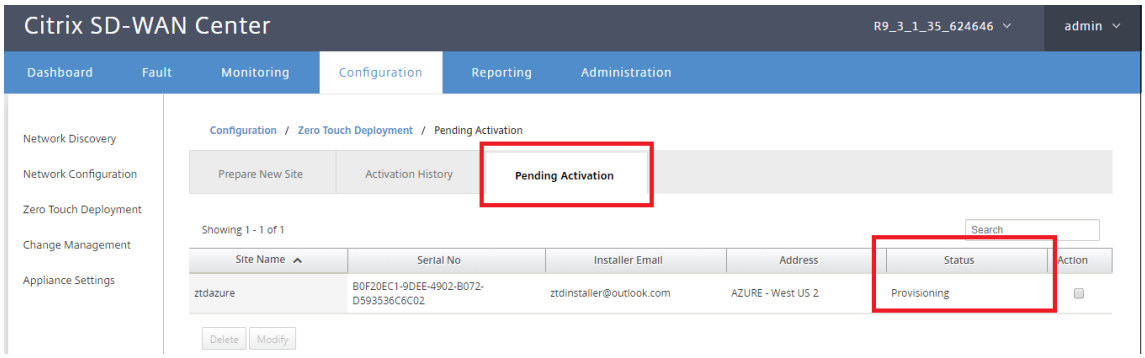
SD-WAN Center Provision and Deploy Azure (Step 2 of 2)

1. Once the Azure authentication is successful, populate the appropriate fields to select the desired Azure Region, and the appropriate Instance Size, then click **Deploy**.

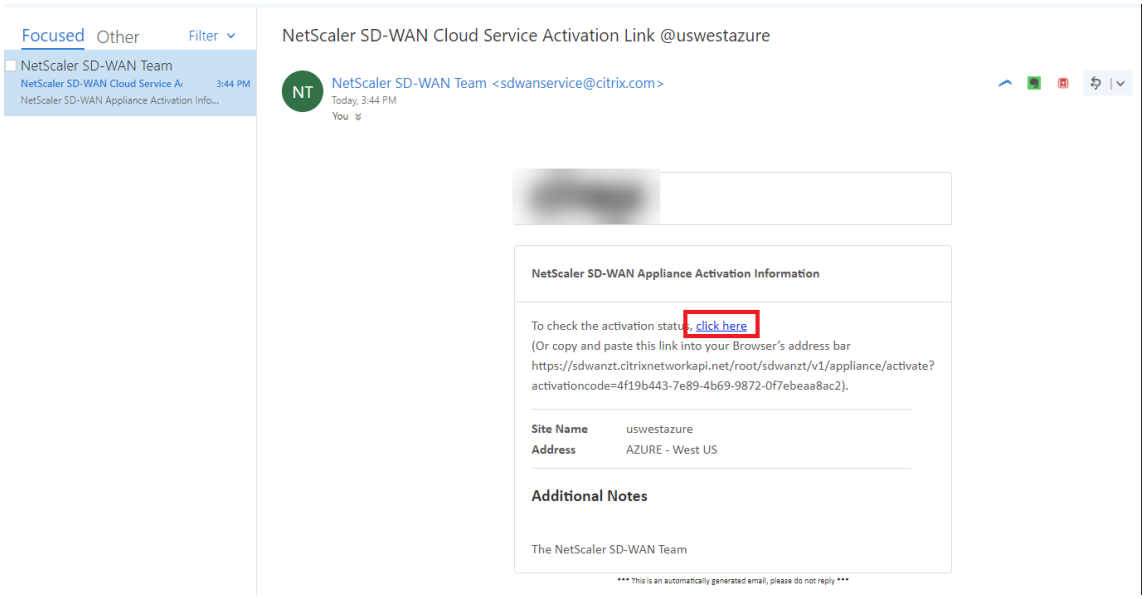
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



2. Navigating to the **Pending Activation** tab in SD-WAN Center, will help track the current status of the deployment.



3. An email with an activation code will be delivered to the email address inputted in step 1, obtain the email and open the **activation URL** to trigger the process and check the activation status.

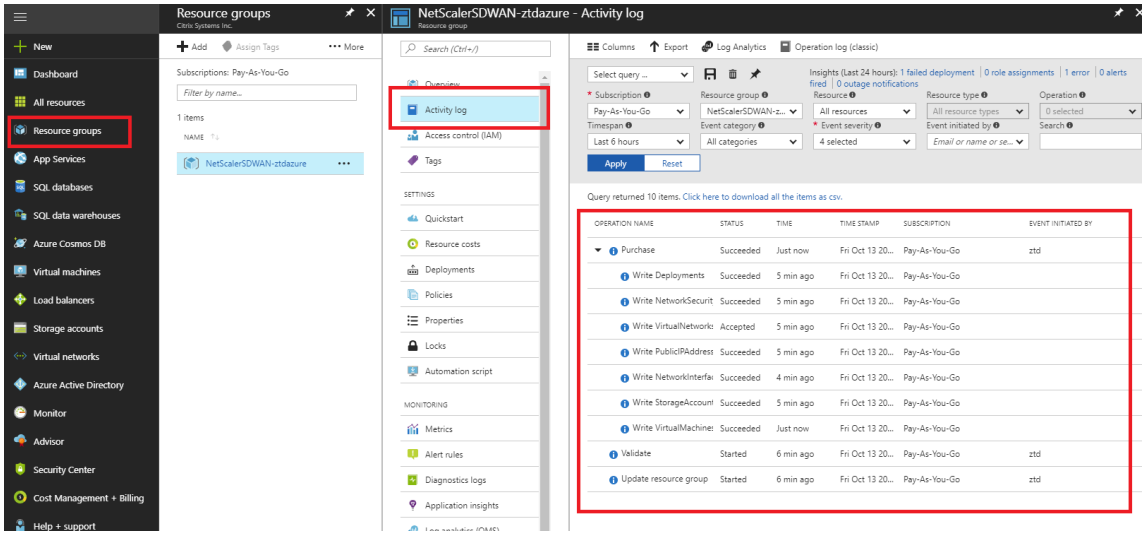


© 1999–2025 Cloud Software Group, Inc. All rights reserved.

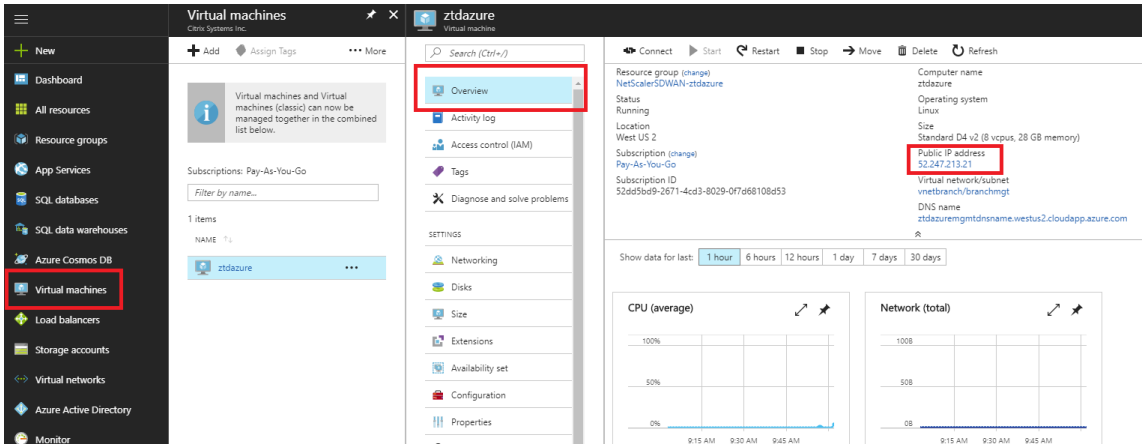
4. An email with an activation URL will be delivered to the email address inputted in step 1. Obtain the email and open the **activation URL** to trigger the process and check the activation status.

5. It will take a few minutes for the instance to be provisioned by the SD-WAN Cloud Service. You can monitor the activity on the Azure portal, under **Activity log** for the **Resource Group** which is automatically created. Any issues or errors with the provisioning will be populated here, as well as replicated to SD-WAN Center in the Activation Status.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

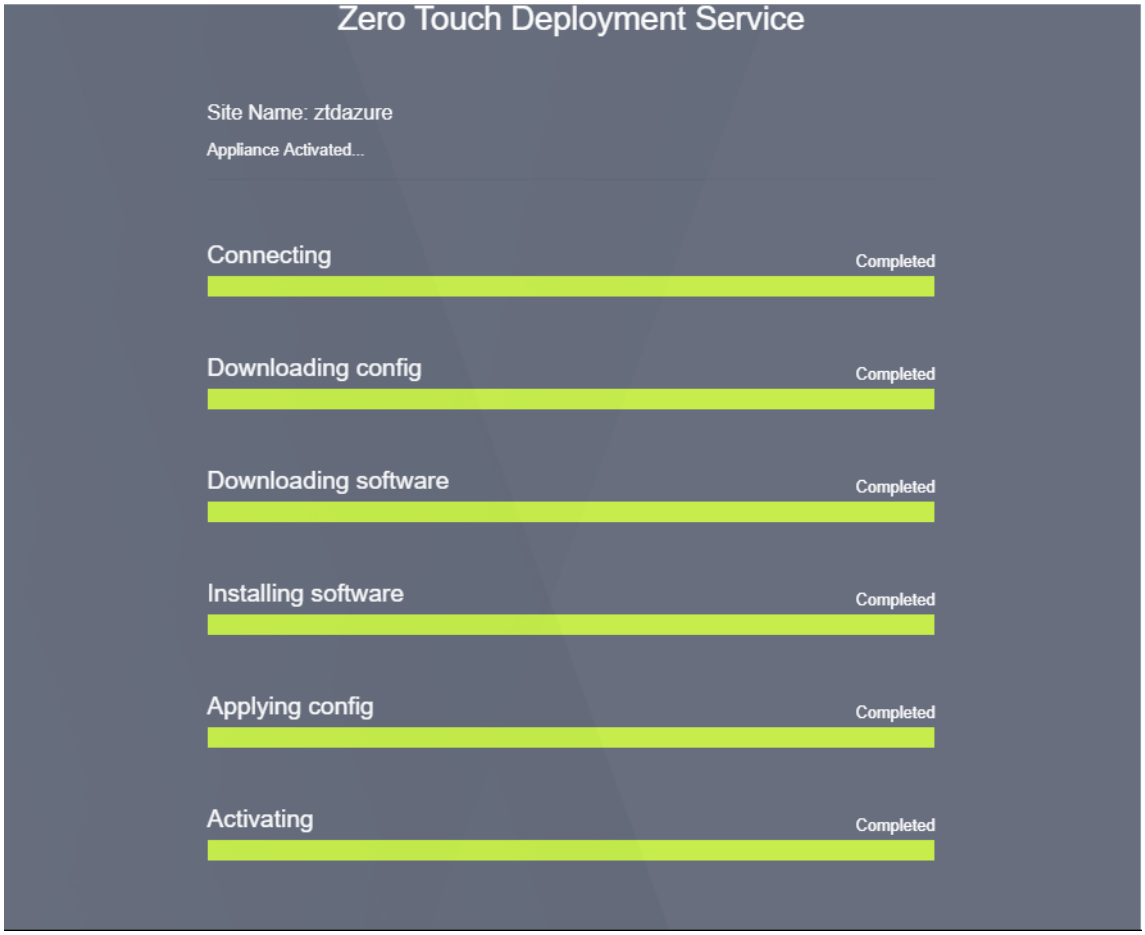


6. In the Azure portal, the successfully launched instance will be available under **Virtual Machines.** To obtain the assigned public IP, navigate to the Overview for the instance.

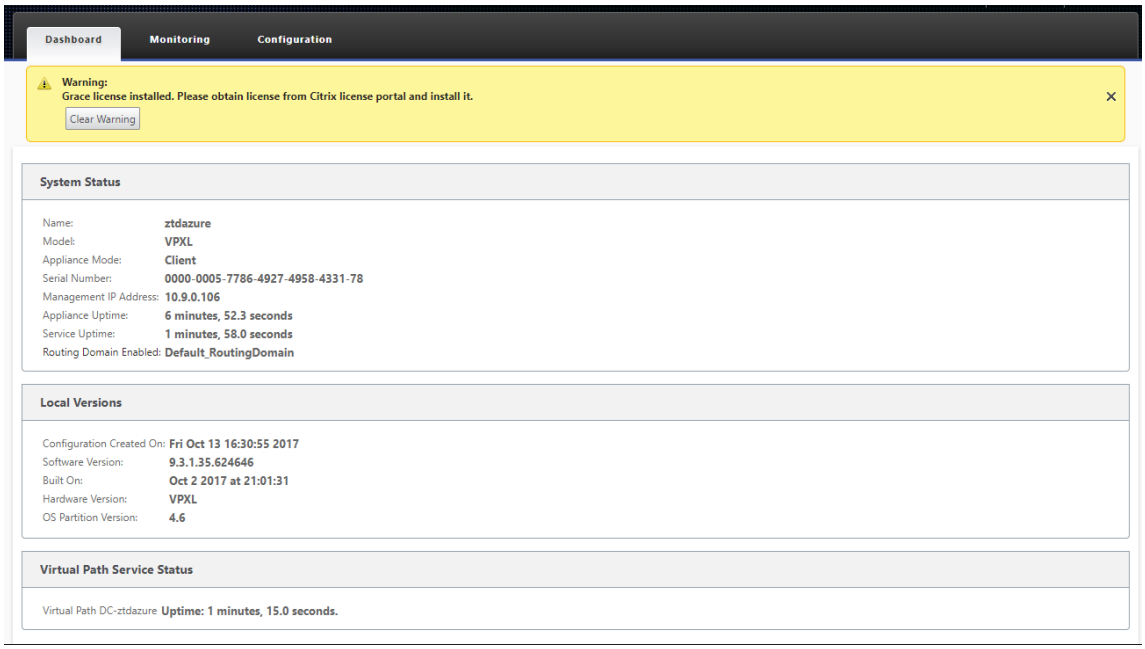


7. After the VM is in a running state, give it a minute before the service will reach out and start the process of downloading the configuration, software and license.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

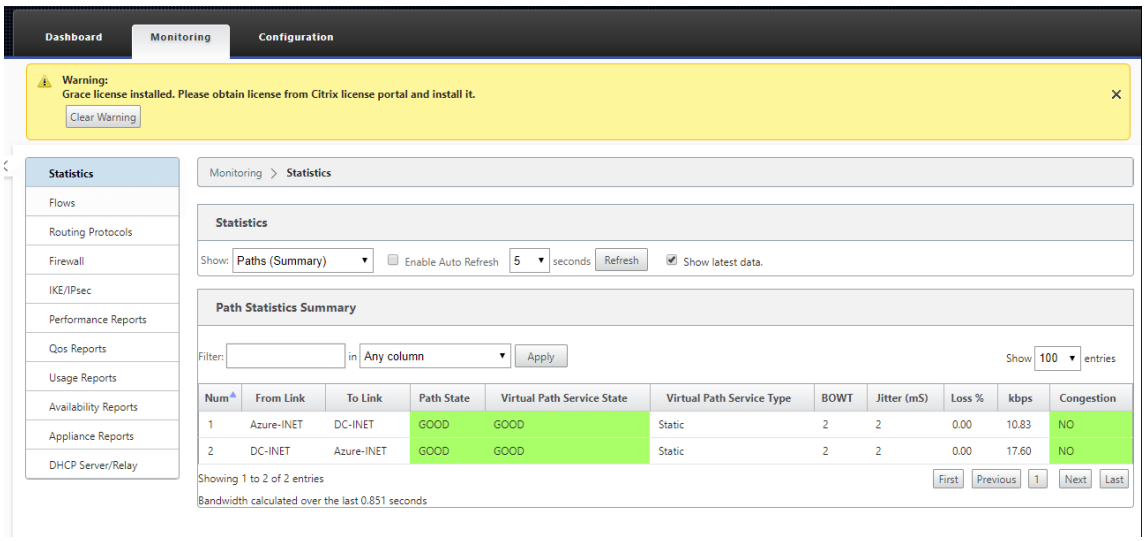


8. After each of the SD-WAN Cloud service steps are automatically complicated, log in to the SD-WAN instances web interface using the public IP obtained from the Azure portal.

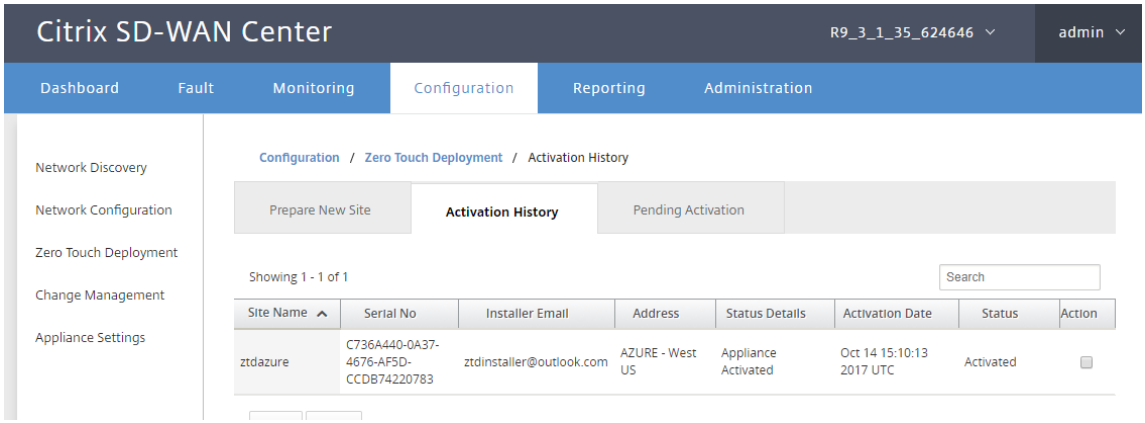


© 1999–2025 Cloud Software Group, Inc. All rights reserved.

9. The Citrix SD-WAN Monitoring Statistics page will identify successful connectivity from the MCN to the SD-WAN instance in Azure.



10. Furthermore, the successful (or unsuccessful) provisioning attempt will be logged in the SD-WAN Center's Activation History page.



Proxy Server Settings for zero touch deployment

March 12, 2021

As a prerequisite for Zero Touch Deployment, the Citrix SD-WAN Center should be connected to the internet. If your Citrix SD-WAN Center is connected to the internet through a proxy server, you have to configure the proxy server settings on the Citrix SD-WAN Center.

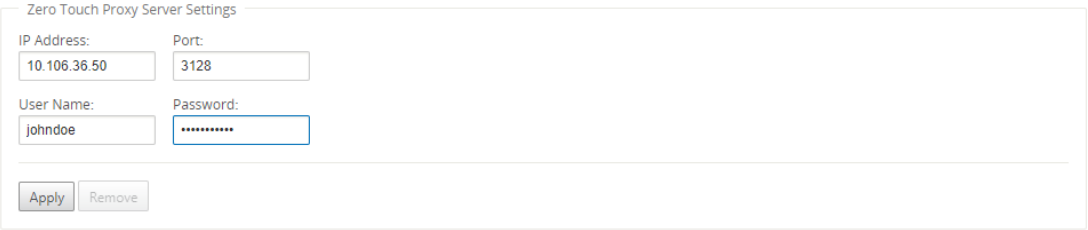
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> **Note**
>
> This proxy server setting is used for Zero Touch Deployment only.

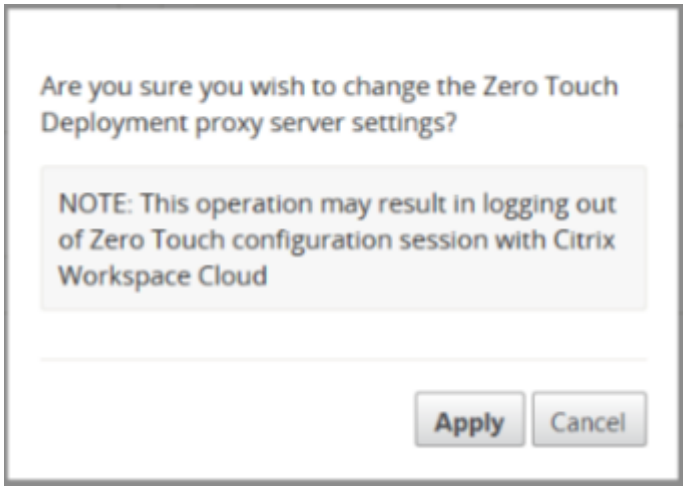
To configure zero touch proxy server settings:

1. In the SD-WAN Center web interface, navigate to **Administration** > **Global Settings** > **Management Interface**.
2. In the **Zero Touch Proxy Server Setting** section, enter values for the following fields:
   - **IP Address**: The IP address of the proxy server.
   - **Port**: The network port number on which the proxy server accepts connections.
   - **User Name**: The proxy server user name
   - **Password**: The password for the proxy server.

   > **Note**
   >
   > You can leave the **User Name** and **Password** field blank if there is no authentication configured on the proxy server.



3. Click **Apply**, a confirmation dialog box appears.



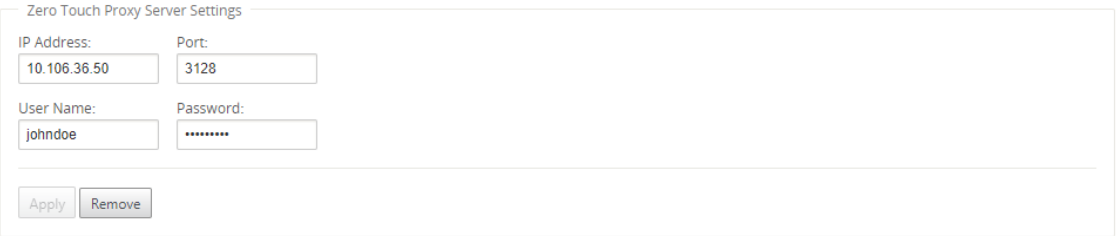
4. Click **Apply**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

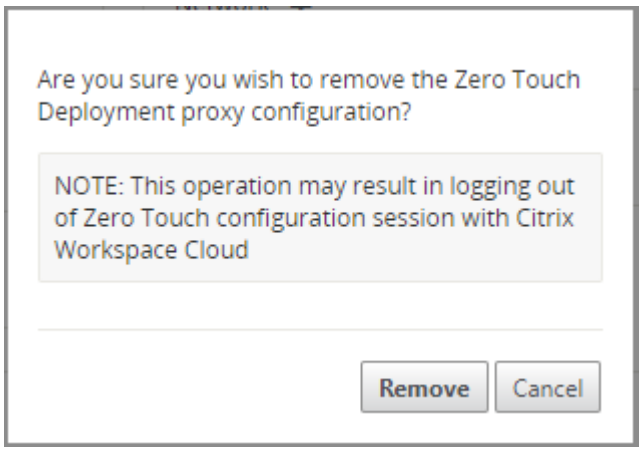
> **Note**
>
> You can remove the proxy server settings altogether, if the Citrix SD-WAN Center is connected to the internet directly. You can also remove the proxy server settings and configure another proxy server, if required.

To remove proxy server settings:

1. In the Citrix SD-WAN Center web interface, navigate to **Administration** > **Global Settings** > **Management Interface**.
2. In the **Zero Touch Proxy Server Setting** section, click **Remove**.



3. Click **Remove**, a confirmation dialog box appears.



4. Click **Remove**.

Palo Alto Network Integration

March 12, 2021

Palo Alto networks deliver cloud-based security infrastructure for protecting remote networks. It provides security by allowing organizations to set up regional, cloud-based firewalls that protect the SD-WAN fabric.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Prisma Access service for remote networks allows you to onboard remote network locations and deliver security for users. It removes the complexity in configuring and managing devices at every remote location. The service provides an efficient way to easily add new remote network locations and minimize the operational challenges with ensuring that users at these locations are always connected and secure, and it allows you to manage policy centrally from Panorama for consistent and streamlined security for your remote network locations.

To connect your remote network locations to the Prisma Access service, you can use the Palo Alto Networks next-generation firewall or a third-party, IPSec-compliant device including
SD-WAN, which can establish an IPsec tunnel to the service.

- Plan the Prisma Access Service for Remote Networks
- Configure the Prisma Access Service for Remote Networks
- Onboard Remote Networks with Configuration Import

The Citrix SD-WAN solution already provided the ability to break out Internet traffic from the branch. This is critical to delivering a more reliable, low-latency user experience, while avoiding the introduction of an expensive security stack at each branch. Citrix SD-WAN and Palo Alto Networks now offer distributed enterprises a more reliable and secure way to connect users in branches to applications in the cloud.

Citrix SD-WAN appliances can connect to the Palo Alto cloud service (Prisma Access Service) network through IPsec tunnels from SD-WAN appliances locations with minimal configuration. You can configure Palo Alto network in Citrix SD-WAN Center.

Before you begin to configure the Prisma Access Service for Remote Networks, make sure you have the following configuration ready to ensure that you are able to successfully enable the service and enforce policy for users in your remote network locations:

1. **Service Connection**—If your remote network locations require access to infrastructure in your corporate headquarters to authenticate users or to enable access to critical network assets, you must set up Access to Your Corporate Network so that headquarters and the remote network locations are connected.

If the remote network location is autonomous and does not need to access to infrastructure at other locations, you do not need to set up the service connection (unless your mobile users need access).

1. **Template**—The Prisma Access service automatically creates a template stack (Remote_Network_Template_
and a top-level template (Remote_Network_Template) for the Prisma Access service for remote networks. To Configure the Prisma Access Service for Remote Networks, you configure the top-level template from scratch or leverage your existing configuration, if you are already running a Palo Alto networks firewall on premise.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

The template requires the settings to establish the IPsec tunnel and Internet Key Exchange (IKE) configuration for protocol negotiation between your remote network location and the Prisma Access service for remote networks, zones that you can reference in security policy, and a log forwarding profile so that you can forward logs from the Prisma Access service for remote networks to the Logging Service.

2. **Parent Device Group**—The Prisma Access service for remote networks requires you to specify a parent device group that includes your security policy, security profiles, and other policy objects (such as application groups and objects, and address groups), as well as authentication policy so that the Prisma Access service for remote networks can consistently enforce policy for traffic that is routed through the IPsec tunnel to the Prisma Access service for remote networks. You need to either define policy rules and objects on Panorama or use an existing device group to secure users in the remote network location.

   > **Note:**
   >
   > If you use an existing device group that references zones, make sure to add the corresponding template that defines the zones to the Remote_Network_Template_Stack.

   This allows you to complete the zone mapping when you configure the Prisma Access Service for Remote Networks.

3. **IP Subnets**—In order for the Prisma Access service to route traffic to your remote networks, you must provide routing information for the subnetworks that you want to secure using the Prisma Access service. You can either define a static route to each subnetwork at the remote network location, or configure BGP between your service connection locations and the Prisma Access service, or use a combination of both methods.

   If you configure both static routes and enable BGP, the static routes take precedence. While it might be convenient to use static routes if you have just a few subnetworks at your remote network locations, in a large deployment with many remote networks with overlapping subnets, BGP will enable you to scale more easily.

Palo Alto network in SD-WAN Center

Ensure that the following prerequisites are met:

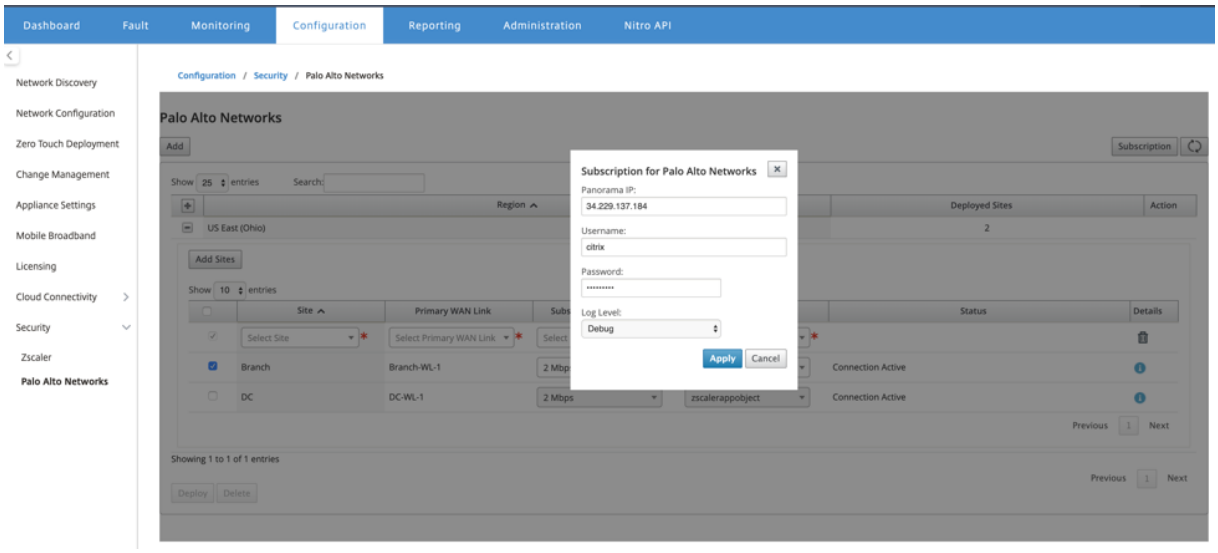
- Obtain panorama IP address from PRISMA ACCESS service.
- Obtain user name and password user in the PRISMA ACCESS service.
- Configure IPsec tunnels in the SD-WAN appliance GUI.
- Make sure the site is not onboarded to a Region, which already has a different site configured with ike/ipsec profiles other than Citrix-IKE-Crypto-Default/Citrix-IPSec-Crypto-Default.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- Make sure that Prisma Access configuration is not changed manually when config is updated by SD-WAN Center.

In the Citrix SD-WAN Center GUI, provide Palo Alto subscription information.

- Configure panorama IP address. You can obtain this IP address from Palo Alto (PRISMA ACCESS service).
- Configure user name and password used in the PRISMA ACCESS service.

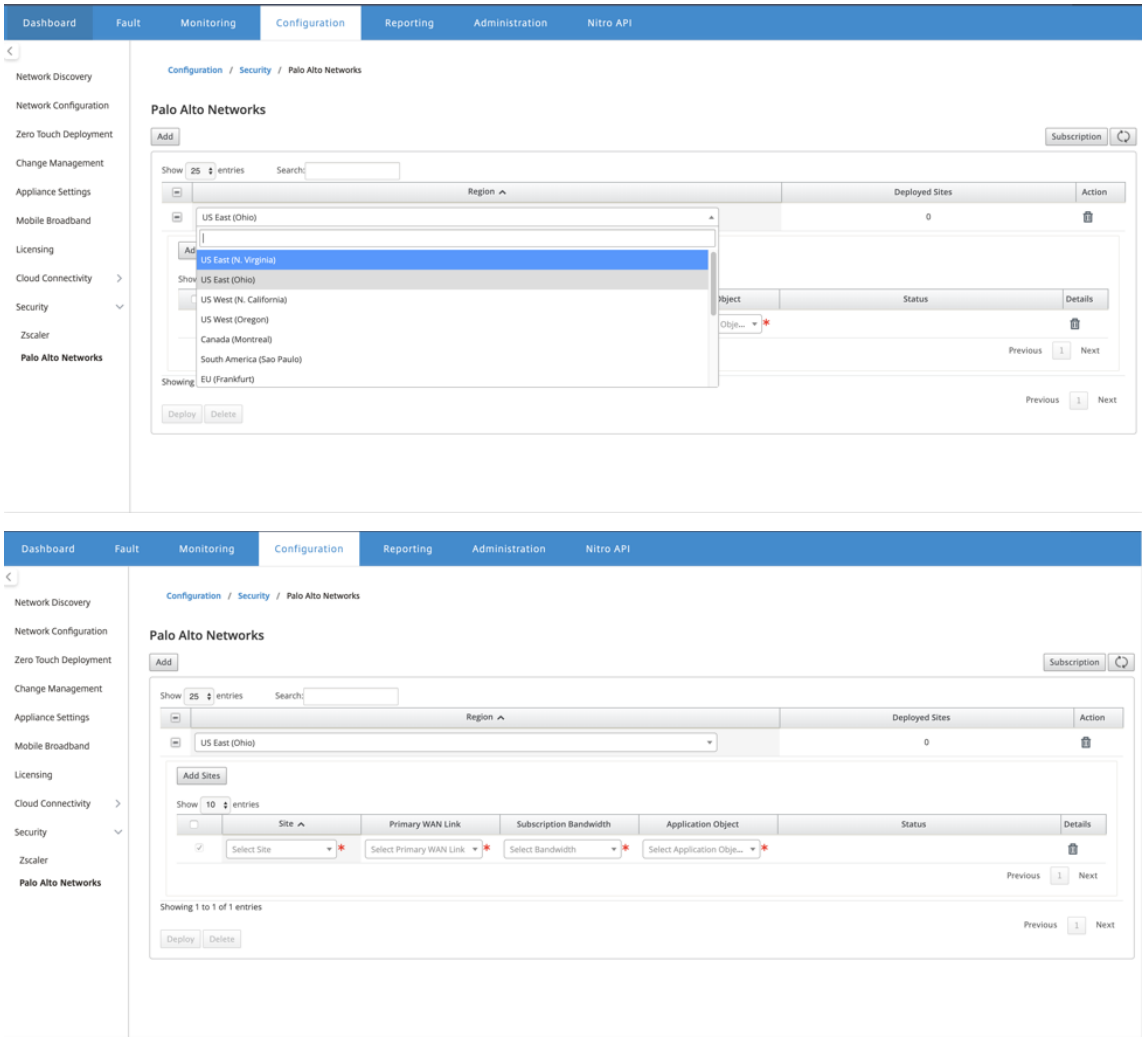


Add and deploy sites

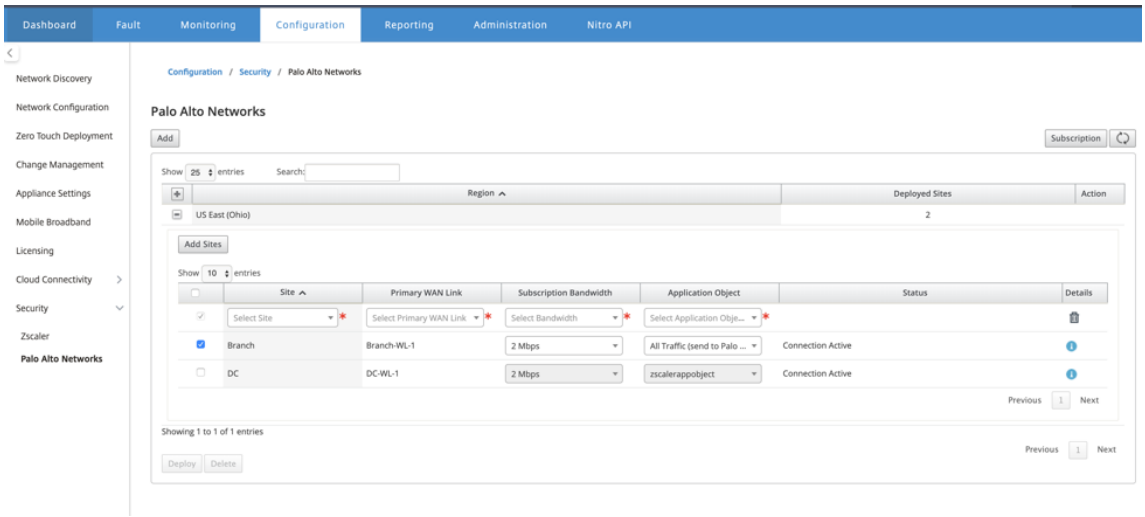
1. To deploy the sites, choose the PRISMA ACCESS network region and the SD-WAN site to be configured for the Prisma Access region, and then select the site WAN link, bandwidth, and application object for traffic selection.

   > **Note:**
   >
   > Traffic flow is impacted if the selected bandwidth exceeds available bandwidth range.
   >
   > You can choose to redirect all internet bound traffic to the PRISMA ACCESS service by selecting the **All traffic** option under the Application object selection.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

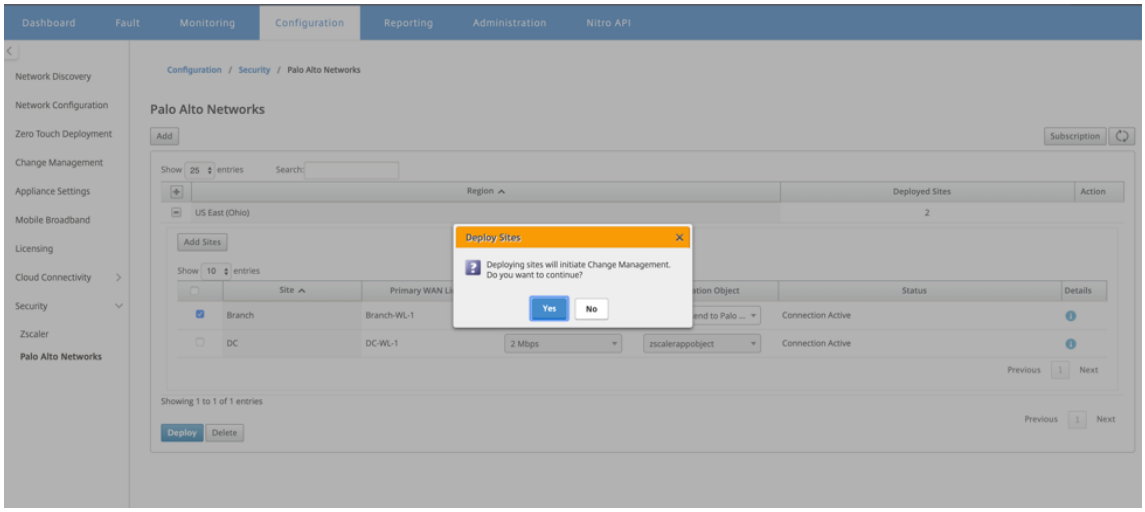


2. You can continue to add more SD-WAN branch sites as required.

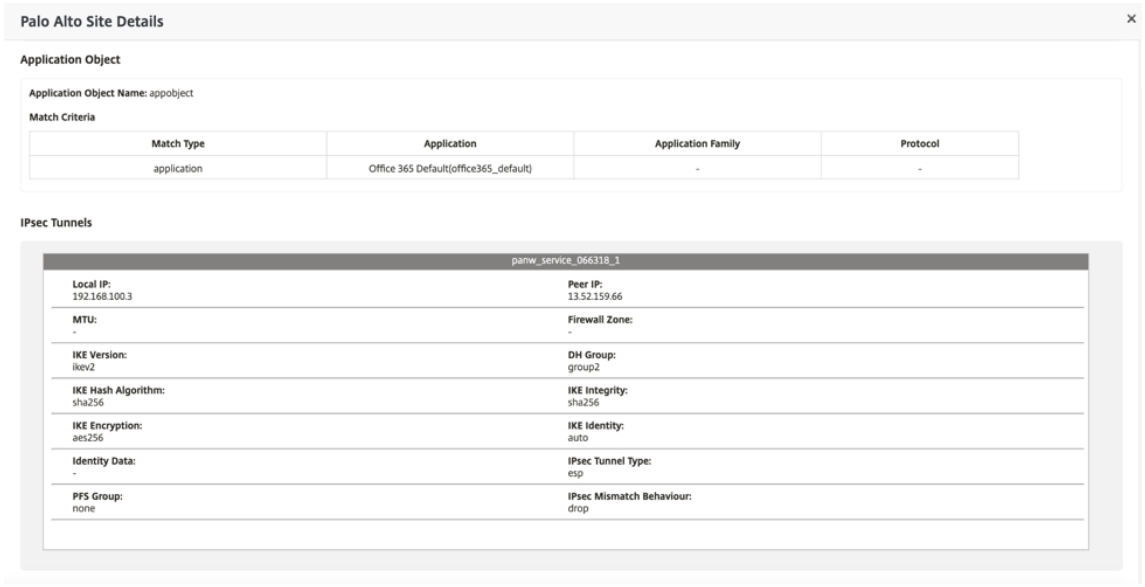


3. Click **Deploy**. The change management process is initiated. Click **Yes** to continue.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

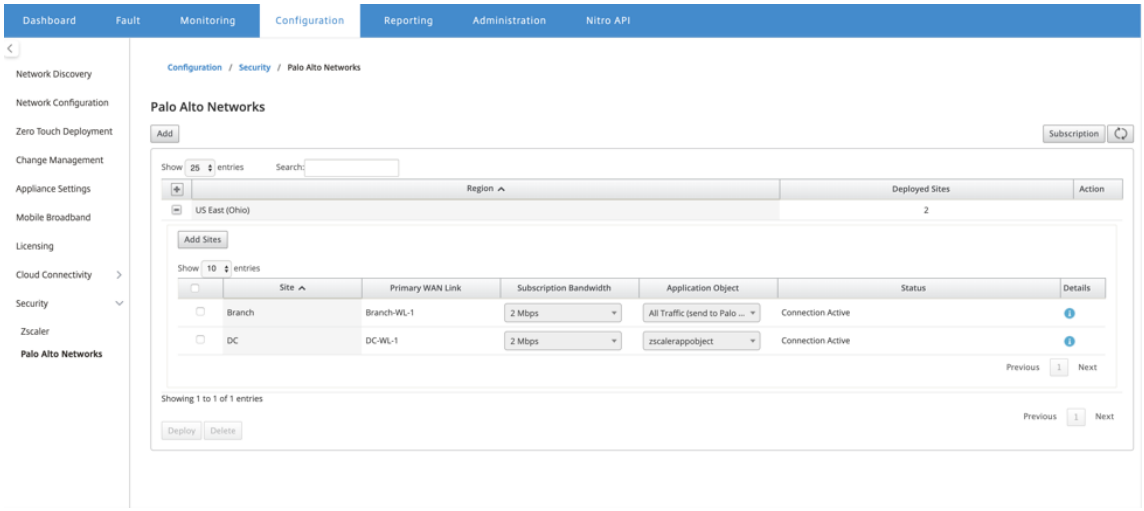


After deployment, the IPsec Tunnel configuration used to establish the tunnels is as follows.



The landing page shows the list of all sites configured and grouped under different SD-WAN regions.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Verify end-to-end traffic connection:

- From LAN subnet of branch, access internet resources.
- Verify that traffic goes through Citrix SD-WAN IPsec tunnel to the Palo Alto Prisma Access.
- Verify that Palo Alto security policy is applied on traffic under the Monitoring tab.
- Verify response from internet to host in a branch comes through.

Microsoft Azure Virtual WAN

March 12, 2021

Microsoft Azure Virtual WAN and Citrix SD-WAN provide simplified network connectivity and centralized management across hybrid cloud workloads. You can automate configuration of branch appliances to connect to the Azure WAN and configure branch traffic management policies according to your business requirements. The built-in dashboard interface provides instant troubleshooting insights that can save time and provides visibility for large-scale site-to-site connectivity.

Microsoft Azure Virtual WAN allows you to enable simplified connectivity to Azure Cloud workloads and to route traffic across the Azure backbone network and beyond. Azure provides 54+ regions and multiple points of presence across the globe Azure regions serve as hubs that you can choose to connect to the branches. After the branches are connected, use the Azure cloud service through hub-to-hub connectivity. You can simplify connectivity by applying multiple Azure services including hub peering with Azure VNETs. Hubs serve as traffic gateways for the branches.

Microsoft Azure Virtual WAN offers the following advantages:

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- Integrated connectivity solutions in hub and spoke - Automate site-to-site connectivity and configuration between on-premises and the Azure hub from various sources including connected partner solutions.
- Automated setup and configuration –Connect your virtual networks to the Azure hub seamlessly.
- Intuitive troubleshooting –You can see the end-to-end flow within Azure and use this information to take required actions.

Hub-to-Hub Communication

From 11.1.0 release onwards, Azure virtual WAN is supported hub-to-hub communication using **Standard** type method.

Azure Virtual WAN customers can now leverage Microsoft's global backbone network for inter-region hub-to-hub communication (Global transit network architecture). This enables branch to Azure, branch-to-branch over the Azure backbone, and branch to hub (in all Azure regions) communication.

You can leverage Azure's backbone for inter-region communication only when you purchase the Standard SKU for Azure virtual WAN. For pricing details, see Virtual WAN pricing. With the Basic SKU, you cannot use Azure's backbone for inter-region hub-to-hub communication. For more details, see Global transit network architecture and Virtual WAN.

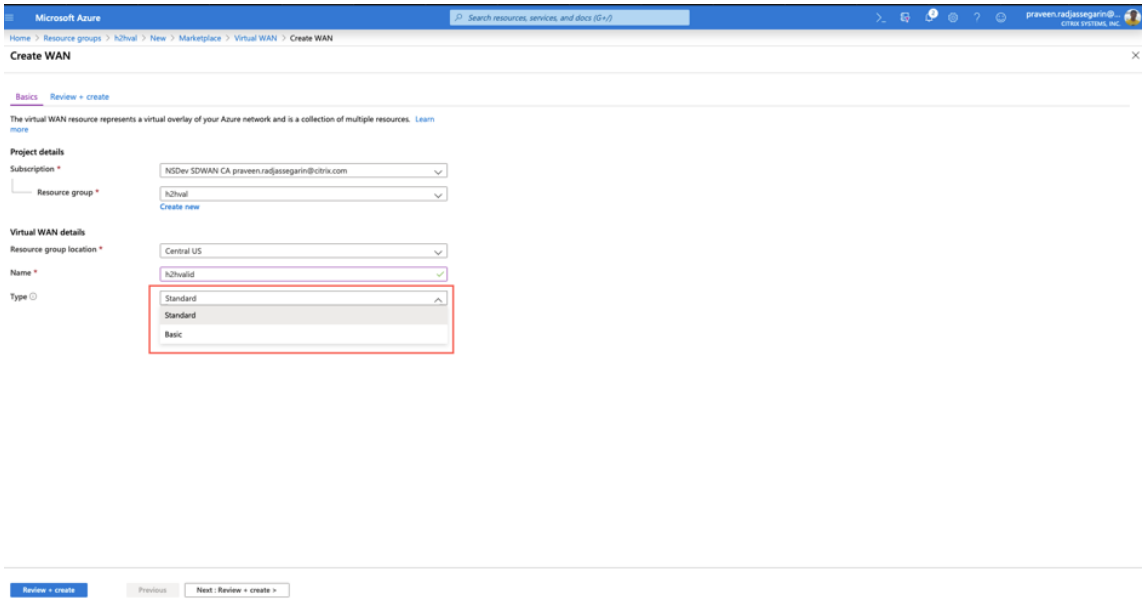
Hubs are all connected to each other in a virtual WAN. This implies that a branch, user, or VNet connected to a local hub can communicate with another branch or VNet using the full mesh architecture of the connected hubs.

You can also connect VNets within a hub transiting through the virtual hub, and VNets across hub, using the hub-to-hub connected framework.

There are two types of virtual WAN:

- **Basic**: Using the **Basic** method, the hub-to-hub communications happen within one region. The **Basic** WAN type helps to create a basic hub (SKU = Basic). Basic hubs are limited to site-to-site VPN functionality.
- **Standard**: Using **Standard** method, hub-to-hub communications happen among different regions. A **Standard** WAN helps to create standard hub (SKU = Standard). **Standard** hubs contain ExpressRoute, User VPN (P2S), full mesh hub, and VNet-to-VNet transit through the hubs.

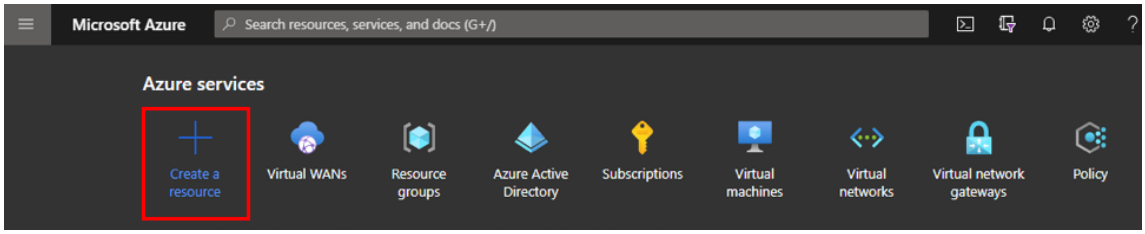
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Create Azure Virtual WAN service in Microsoft Azure

To create the Azure Virtual WAN resource, perform the following steps:

1. Log into the Azure portal and click **Create a resource**.



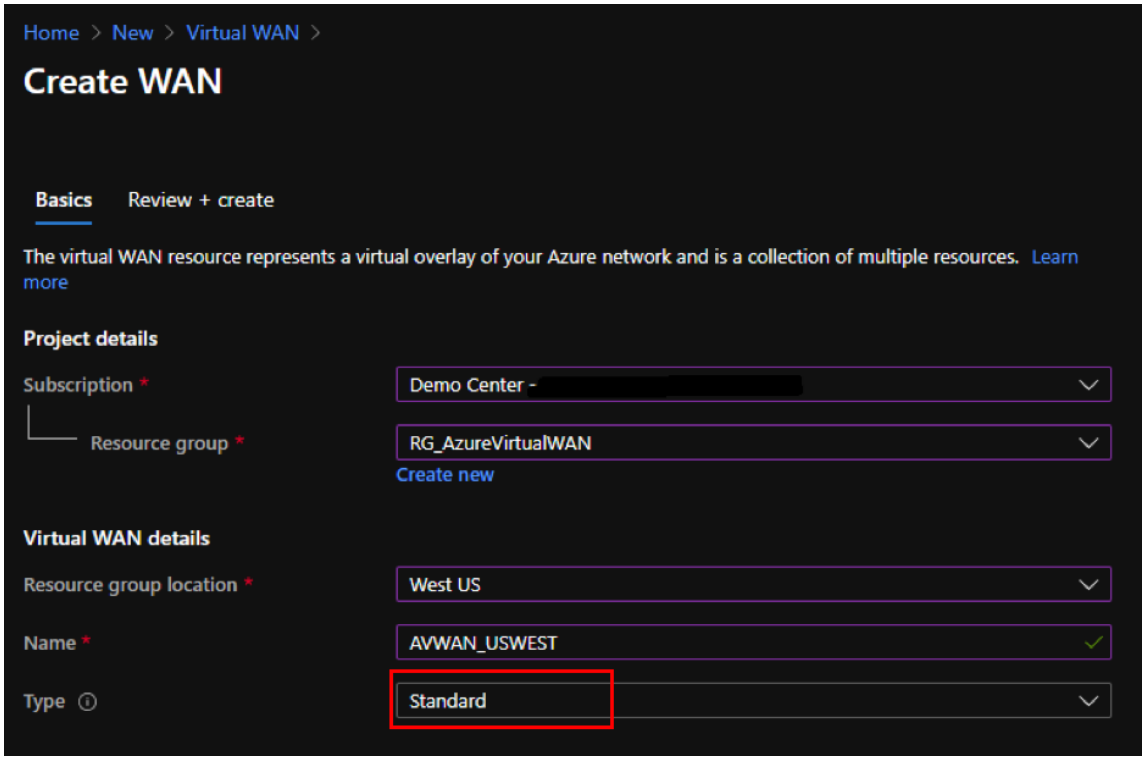
2. Search for **Virtual WAN** and click **Create**.
3. Under **Basic**, provide the values for the following fields:
   - **Subscription**: select and provide the subscription detail from the drop-down list.
   - **Resource group**: Select an existing resource group or create a new one.

     > **Note**
     >
     > When creating the service principal to allow Azure API communication, ensure to use the same resource group that contains the Virtual WAN. Otherwise, SD-WAN Orchestrator will not have sufficient permissions to authenticate to Azure Virtual WAN APIs that enable automated connectivity.

   - **Resource group location**: Select the Azure region from the drop-down list.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- **Name**: Provide the name for the new Virtual WAN.
- **Type**: select **Standard** type if you want to use hub-to-hub communication between different regions, otherwise select **Basic**.



4. Click **Review + create**.
5. Review the details that you entered to create the Virtual Wan and click **Create** to finish the Virtual WAN creation.

The deployment of the resource takes less than a minute.

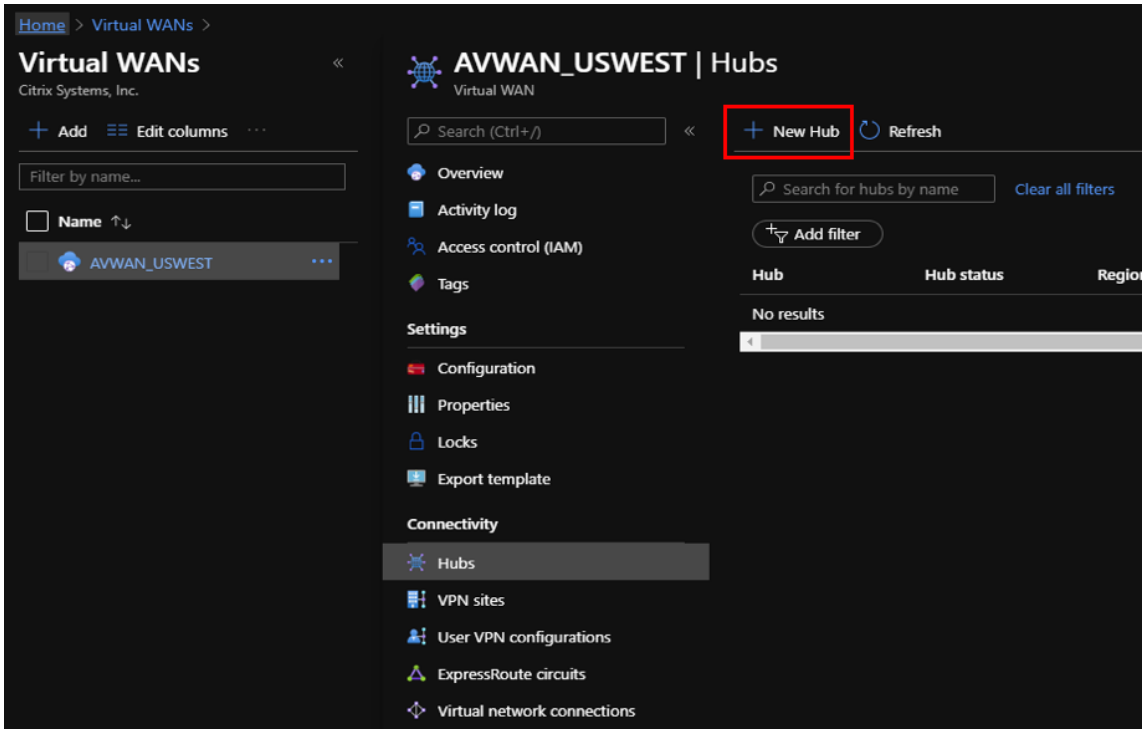
> **Note**
>
> You can upgrade from Basic to Standard, but cannot revert from Standard back to Basic. For steps to upgrade a virtual WAN, see Upgrade a virtual WAN from Basic to Standard.

Create a Hub in the Azure Virtual WAN

Perform the following steps to create a hub to enable connectivity from various different endpoints (for example, on-premises VPN devices, or SD-WAN devices):

1. Select the previously created Azure Virtual WAN.
2. Select **Hubs** under **Connectivity** section and click **+ New Hub**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

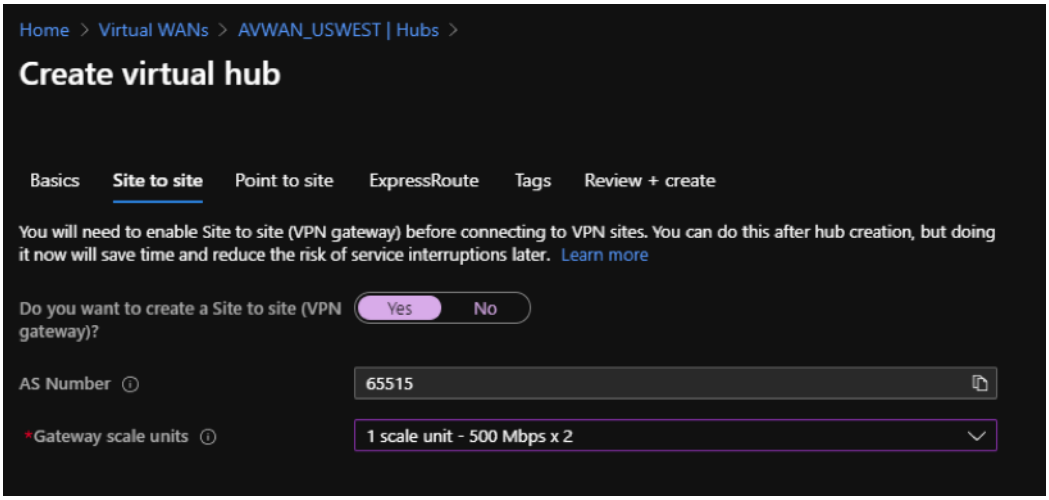


3. Under **Basic**, provide the values for the following fields:

   - **Region** –Select the Azure region from the drop-down list.
   - **Name** –Enter the name for the new Hub.
   - **Hub private address space** –Enter the address range in CIDR. Select a unique network that is dedicated for the hub only.

4. Click **Next: Site to Site >** and provide the values for the following fields:

   - **Do you want to create a Site to site (VPN gateway)?** –Select **Yes**.
   - **Gateway scale units** –Select the scale units from the drop-down list as needed.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

5. Click **Review + create**.
6. Review the settings and click **Create** to start the virtual hub creation.

The deployment of the resource can take up to 30 minutes.

Create a service principal for Azure Virtual WAN, and identify IDs

For SD-WAN Orchestrator to authenticate through Azure Virtual WAN APIs and enable automated connectivity, a registered application must be created and identified with the following authentication credentials:

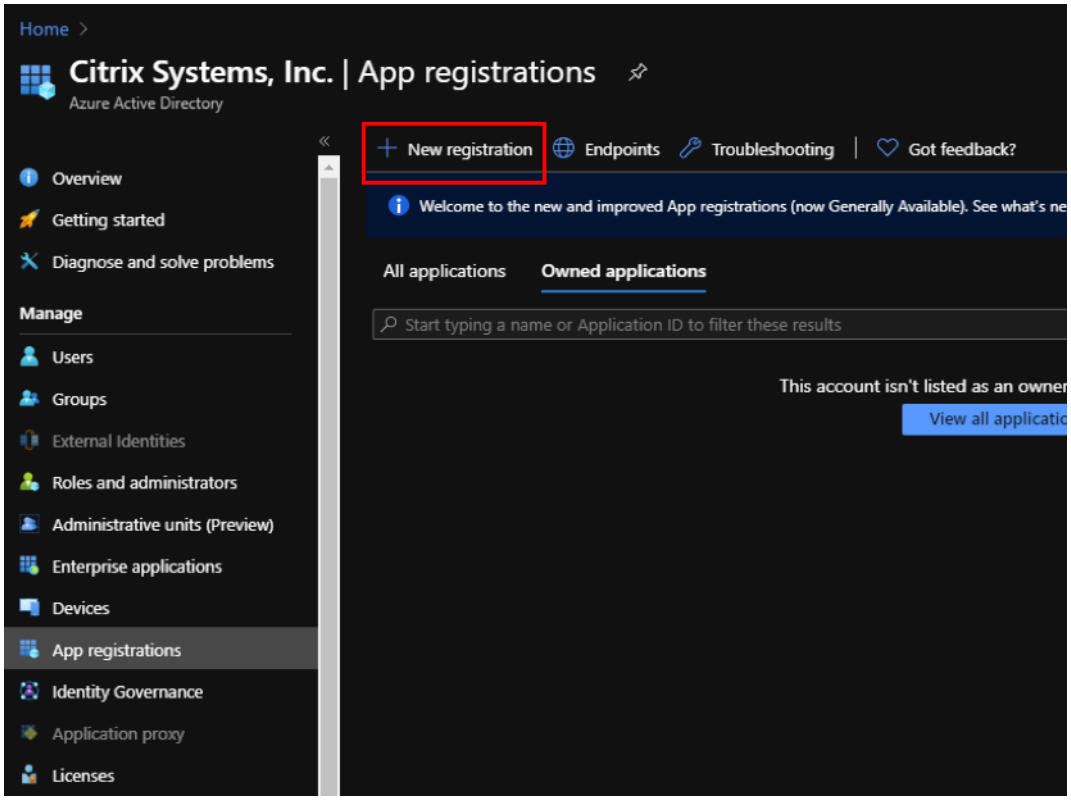
- Subscription ID
- Client ID
- Client Secret
- Tenant ID

> **Note**
>
> When creating the service principal to allow Azure API communication, ensure to use the same resource group that contains the Virtual WAN. Otherwise, SD-WAN Orchestrator will not have sufficient permissions to authenticate to Azure Virtual WAN APIs that enable automated connectivity.

Perform the following steps to create a new application registration:

1. In the Azure portal, navigate to **Azure Active Directory**.
2. Under Manage, select **App registration**.
3. Click **+ New registration**.

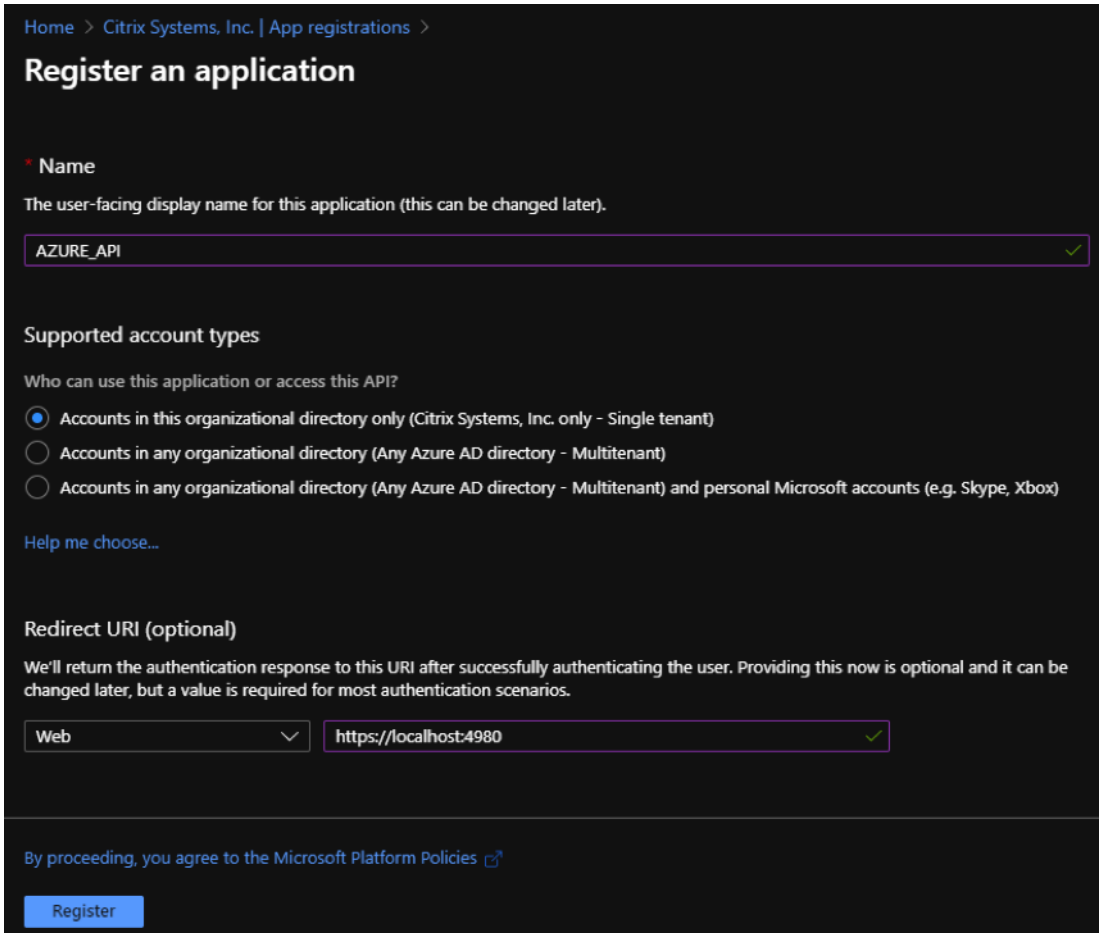
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



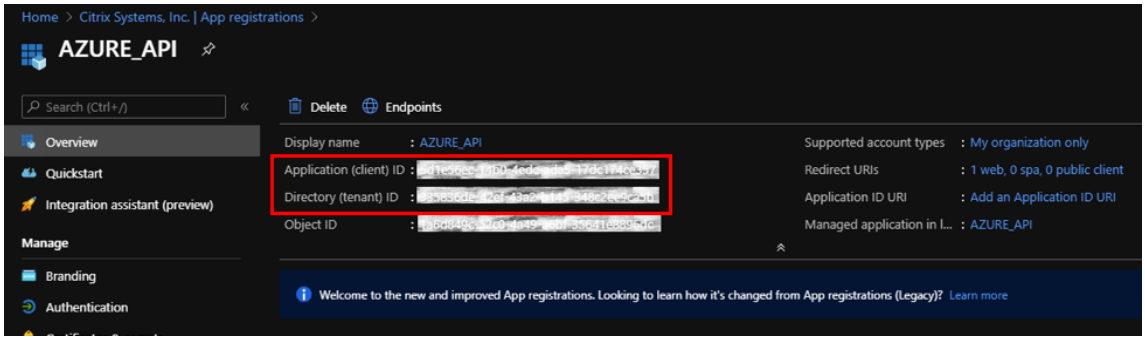
4. Provide values for the following fields to register an application:

   - **Name** –Provide the name for the application registration.
   - **Supported account types** –select Accounts in this organizational directory only (* - Single tenant) option.
   - **Redirect URI (optional)** –select Web from the drop-down list and enter a random, unique URL (for example, https:// localhost:4980)
   - Click **Register**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



You can copy and store the **Application (client) ID** and the **Directory (tenant) ID** that can be used in SD-WAN Orchestrator for authentication to the Azure subscription for usage of API.



The next step for the application registration, create a service principal key for authentication purposes.

To create the service principal key, perform the following steps:

a) In the Azure portal, navigate to **Azure Active Directory**.

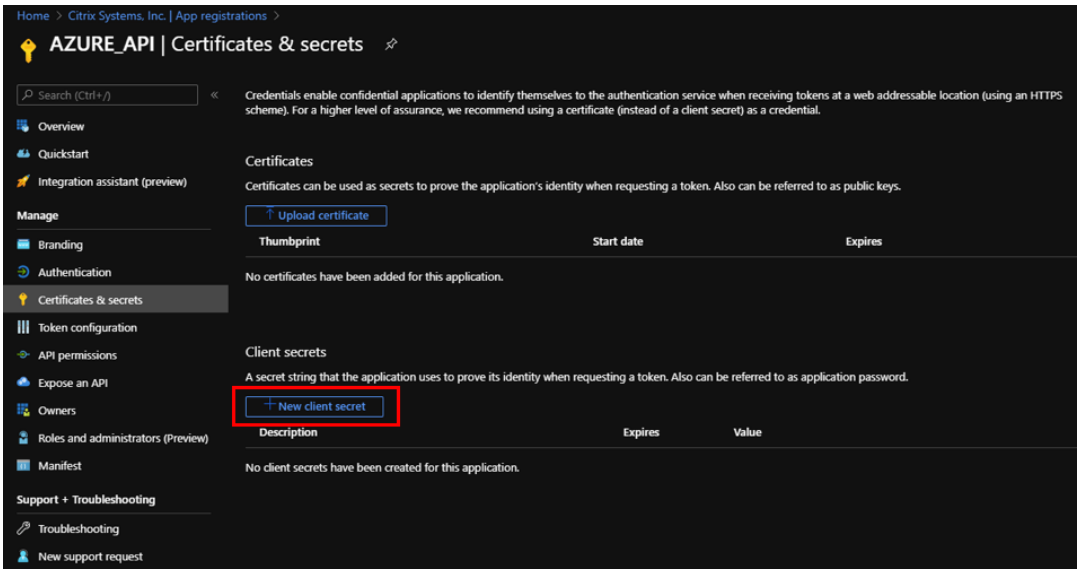
b) Under **Manage**, navigate to **App registration**.

c) Select the registered application (created previously).

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

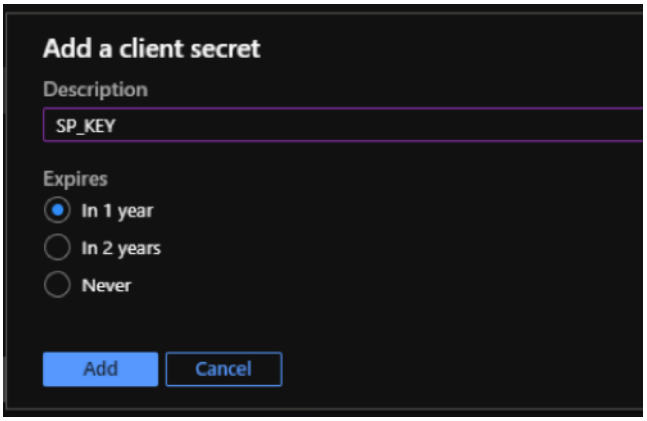
d) Under **Manage**, select **Certificates & secrets**.

e) Under **Client secrets**, click **+ New client secret**.



f) To add a client secret, provide values for the following fields:

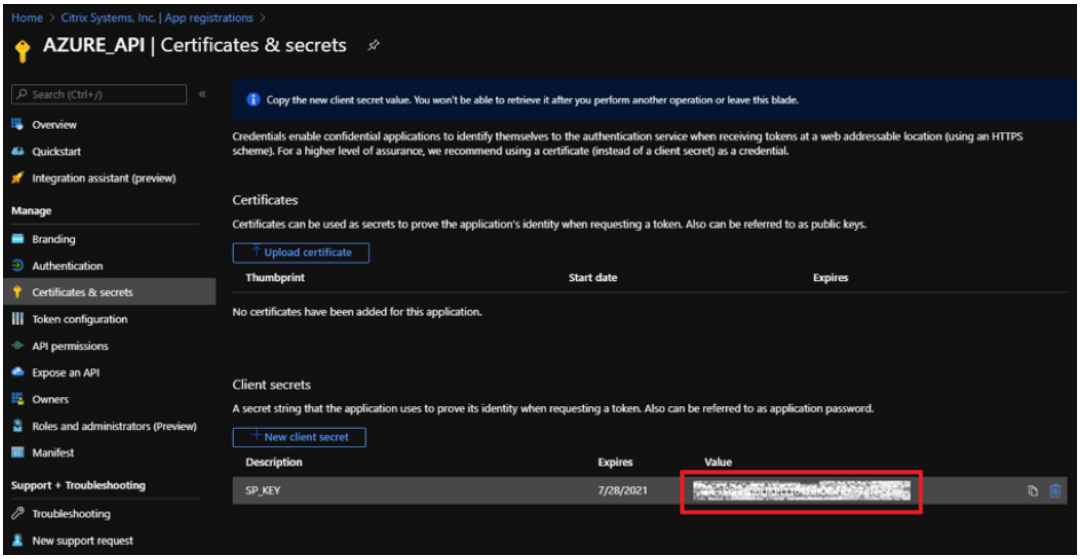
- **Description**: Provide a name for the service principal key.
- **Expires**: Select the duration for expiration as needed.



g) Click **Add**.

h) The client secrete is disabled in the **Value** column. Copy the key to your clipboard. This is the Client Secret that you must enter into SD-WAN Orchestrator.

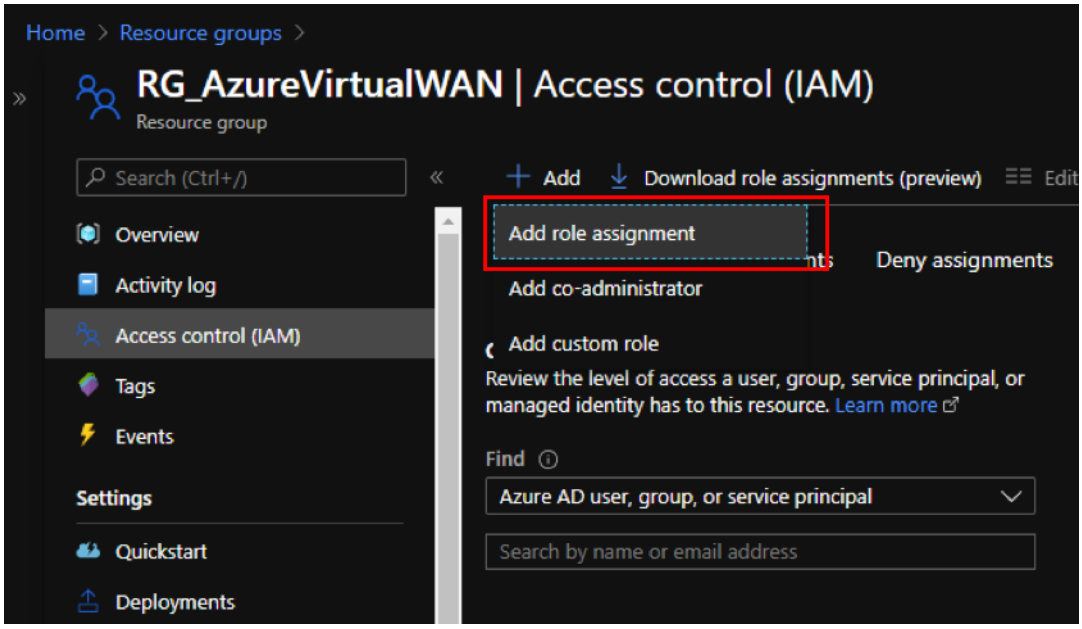
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



> **Note**
>
> You must copy and store the secret key value before reloading the page because, it will no longer be displayed afterwards.

Perform the following steps to assign the appropriate roles for authentication purpose:

1. In the Azure portal, navigate to the **Resource Group** where the Virtual WAN was created.
2. Navigate to **Access control (IAM)**.
3. Click **+ Add** and select **Add role assignment**.

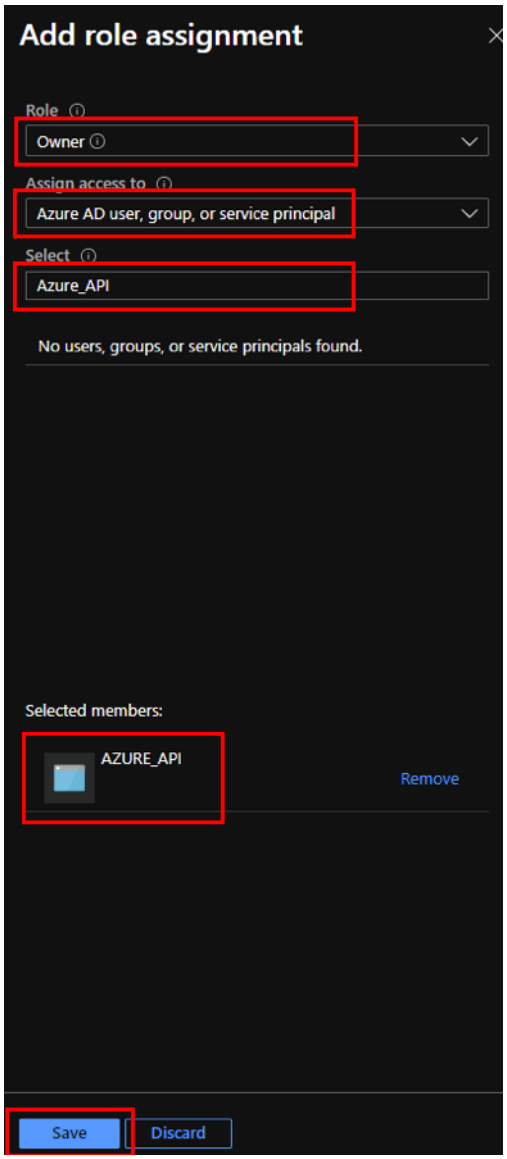


4. To add role assignment, provide values for the following fields:

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

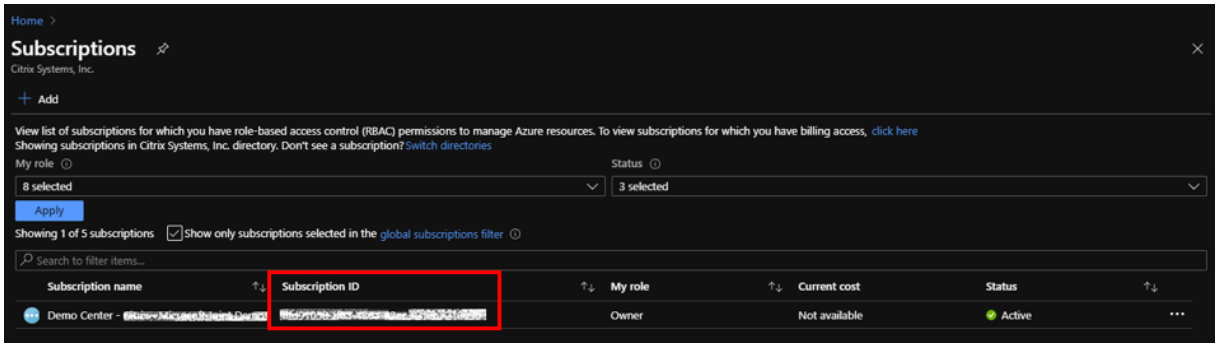
- **Role** –Select Owner from the drop-down list. This role allows management of everything including access to resources.
- **Assign access to** –select **Azure AD user, group,** or **service principal**.
- **Select** –Provide the name of the registered application created earlier and select the corresponding entry when it appears.

5. Click **Save**.

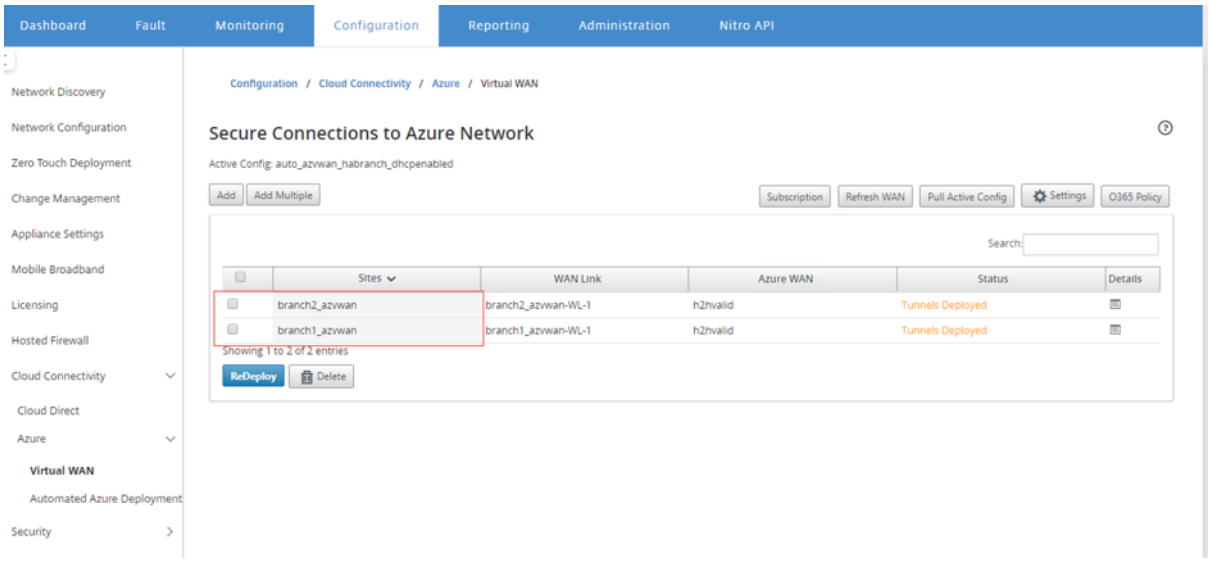


Lastly, you need to obtain the Subscription ID for the Azure account. You can identify your **Subscription ID** by searching for Subscriptions in the Azure portal.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Once you created the virtual WAN, log in to **SD-WAN Center UI > Configuration > Azure > Virtual WAN**.

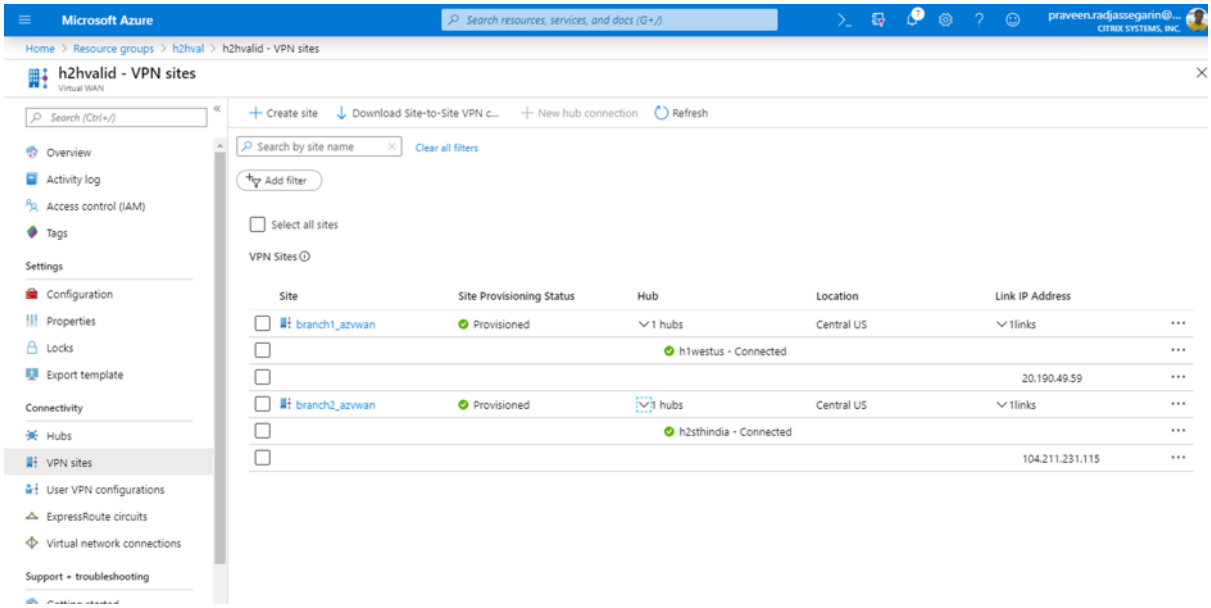


Select two different sites and start the deployment. Once the sites are deployed, you can associate both the sites to two different hubs.

> **NOTE**
>
> By default branch-to-branch and BGP is disabled. You can create a static route or enable BGP (under Settings) and branch-to-branch connectivity.

Enable BGP and branch-to-branch check box and deploy the tunnels. After the tunnels are deployed successfully, you can verify the status in **Microsoft Azure > Resource groups >** select the **resource group** that you created and click **VPN sites**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Using Citrix SD-WAN to connect to Microsoft Azure Virtual WAN

August 10, 2021

For on-premises devices to connect into Azure a controller is required. A controller ingests Azure APIs to establish site-to -site connectivity with the Azure WAN and a Hub.

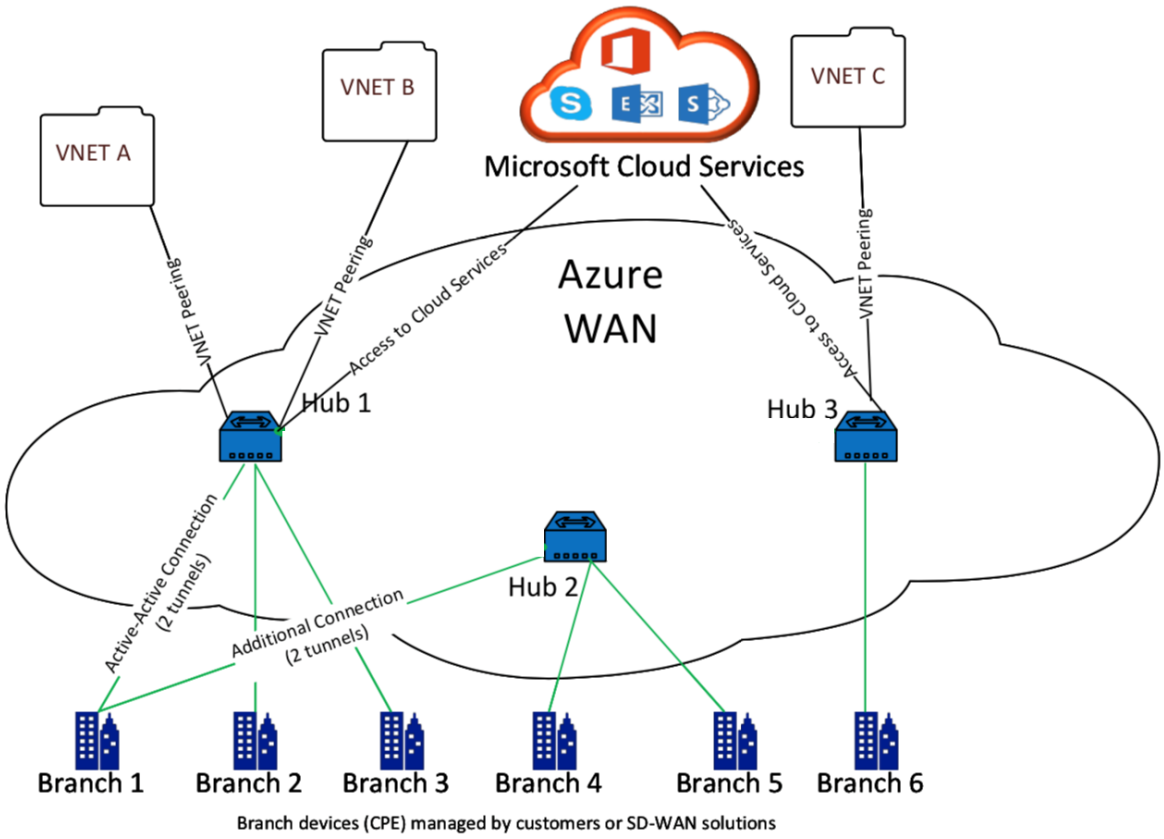
Microsoft Azure Virtual WAN includes the following components and resources:

- WAN: Represents entire network in Microsoft Azure. It contains links to all Hubs that you would like to have within this WAN. WANs are isolated from each other and cannot contain a common hub, or connections between two hubs in different WANs.
- Site: Represents your on-premises VPN device and its settings. A Site can connect to multiple hubs. By using Citrix SD-WAN, you can have a built-in solution to automatically export this information to Azure.
- Hub: Represents the core of your network in a specific region. The Hub contains various service endpoints to enable connectivity and other solutions to your on-premises network. Site-to-site connections are established between the Sites to a Hubs VPN endpoint.
- Hub virtual network connection: Hub network connects the Azure Virtual WAN Hub seamlessly to your virtual network. Currently, connectivity to virtual networks that are within the same Virtual Hub Region is available.
- Branch: The branches are the on-premises Citrix SD-WAN appliances, which exist in customer office locations. An SD-WAN controller manages the branches centrally. The connection origi-

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

nates from behind these branches and terminates into Azure. The SD-WAN controller is responsible for applying the required configuration to these branches and to Azure Hubs.

The following illustration describes the Virtual WAN components:



How does Microsoft Azure Virtual WAN work

1. The SD-WAN Center is authenticated by using service principal, principal, or role-based access functionality, which is enabled in the Azure GUI.
2. The SD-WAN Center obtains Azure connectivity configuration and updates the local device. This automates the configuration download, editing, and updating of the on premise device.
3. After the device has the correct Azure configuration, a site-to-site connection (two active IPsec tunnels) is established to the Azure WAN. Azure requires the branch device connector to support IKEv2 settings. The BGP configuration is optional.

   Note: IPsec parameters for establishing IPsec tunnels are standardized.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

IPsec Property	Parameter
Ike Encryption Algorithm	AES 256
Ike Integrity Algorithm	SHA 256
Dh Group	DH2
IPsec Encryption Algorithm	GCM AES 256
IPsec Integrity Algorithm	GCM AES 256
PFS Group	None

Azure Virtual WAN automates connectivity between the workload virtual network and the hub. When you create a Hub Virtual Network Connection, it sets the appropriate configuration between the provisioned hub and the workloads virtual network (VNET).

Prerequisites and requirements

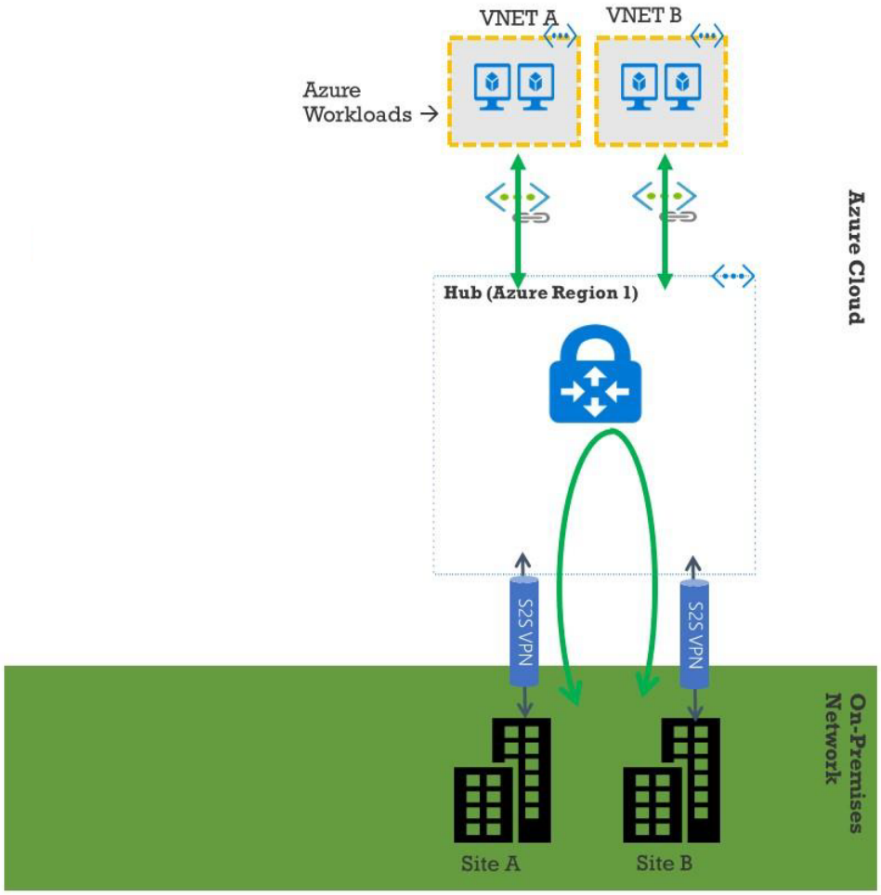
Read the following requirements before proceeding with configuring Azure and SD-WAN to manage branch sites connecting to Azure hubs.

1. Have whitelisted Azure subscription for Virtual WAN.
2. Have an on premise appliance such as, an SD-WAN appliance to establish IPsec into Azure resources.
3. Have Internet links with public IP addresses. Though a single Internet link is sufficient to establish connectivity into Azure, you need two IPsec tunnels to use the same WAN link.
4. SD-WAN controller –a controller is the interface responsible for configuring SD-WAN appliances for connecting into Azure.
5. A VNET in Azure that has at least one workload. For instance, a VM, which is hosting a service. Consider the following points:

    a) The virtual network must not have an Azure VPN or Express Route gateway, or a network virtual appliance.
    b) The virtual network must not have a user-defined route, which routes traffic to a non-Virtual WAN virtual network for the workload accessed from on-premises branch.
    c) Appropriate permissions to access the workload must be configured. For example, port 22 SSH access for a ubuntu VM.

The following diagram illustrates a network with two sites and two virtual networks in Microsoft Azure.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Set up Microsoft Azure Virtual WAN

For on premise SD-WAN branches to connect into Azure and access the resources over IPsec tunnels, the following steps need to be completed.

1. Configuring WAN resources.
2. Enabling SD-WAN branches to connect into Azure using IPsec tunnels.

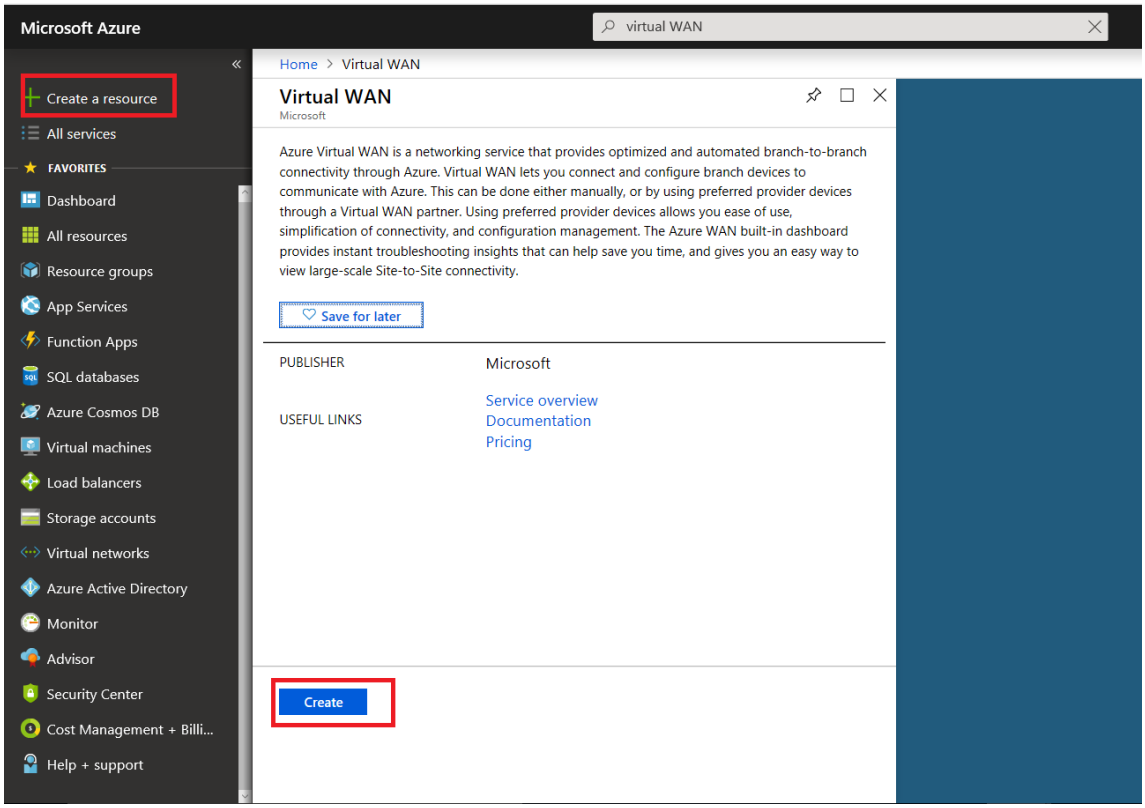
Configure Azure network before configuring SD-WAN network, since the Azure resources required to connect to SD-WAN appliances must be available beforehand. However, you can configure SD-WAN configuration before configuring Azure resources, if you prefer. This topic discusses setting up the Azure Virtual WAN network first before configuring SD-WAN appliances. https://microsoft.com Azure virtual-wan.

Create a WAN resource

To use Virtual WAN features and connect the on premises branch appliance into Azure:

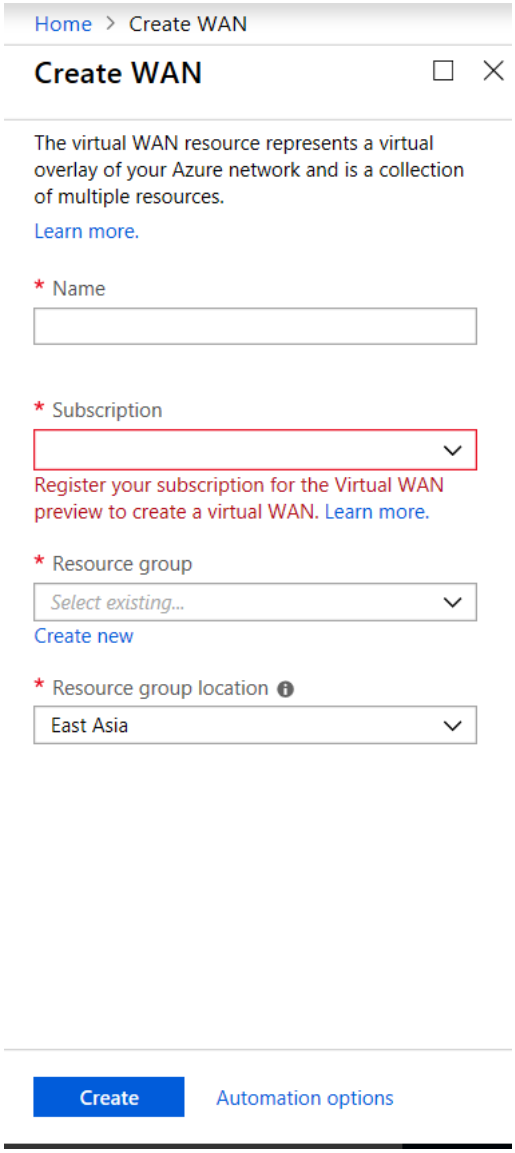
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

1. Sign in to Azure Marketplace, go to the Virtual WAN app, and select **Create WAN**.



2. Enter a name for the WAN and select the subscription you want to use for WAN.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



3. Select an existing resource group or create a fresh resource group. Resource groups are logical constructs and data exchange across resource groups is always possible.
4. Select the location where you want your resource group to reside. WAN is a global resource that does not have a location. However, you must enter a location for the resource group that contains metadata for WAN resource.
5. Click **Create**. This starts the process to validate and deploy your settings.

Create site

You can create a site by using a preferred vendor. The preferred vendor sends the information about your device and site to Azure or you can decide to manage the device yourself. If you want to manage the device, you need to create the site in Azure Portal.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

SD-WAN network and Microsoft Azure Virtual WAN workflow

Configure SD-WAN appliance:

1. Provision a Citrix SD-WAN appliance
    - Connect SD-WAN branch appliance to the MCN appliance.
2. Configure SD-WAN appliance
    - Configure Intranet Services for Active-Active connection.

Configure SD-WAN Center:

- Configure SD-WAN Center to connect to Microsoft Azure.

Configure Azure settings:

- Provide Tenant ID, Client ID, Secure Key, Subscriber ID, and Resource Group.

Configure branch site to WAN association:

1. Associate one WAN resource to a branch. Same site cannot be connected to multiple WANs.
2. Click **New** to configure Site-WAN association.
3. Select **Azure Wan-resources**.
4. Select **Services** (Intranet) for the site. Select two services for Active-Standby support.
5. Select **Site Names** to be associated with the Wan-resources.
6. Click **Deploy** to confirm the association.
7. Wait for the status to change to **Tunnels Deployed** to view the **IPsec tunnel** settings.
8. Use the SD-WAN Center Reporting view to check status of the respective IPsec tunnels.

Configure Citrix SD-WAN network

MCN:

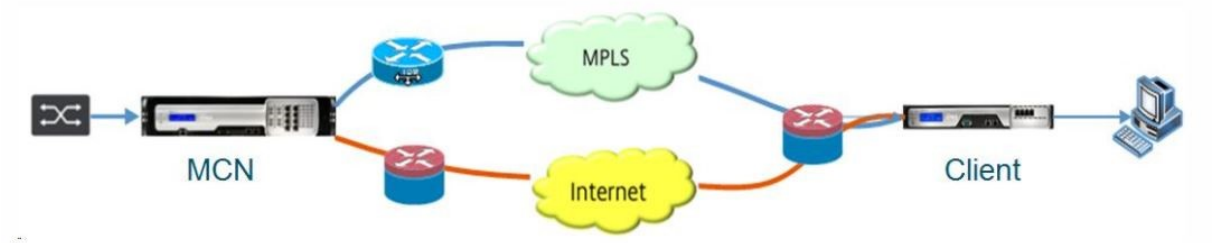
The MCN serves as the distribution point for the initial system configuration and subsequent configuration changes. There can be only one active MCN in a Virtual WAN.
By default, appliances have the pre-assigned role of client. To establish an appliance as the MCN, you must first add and configure the site as an MCN. The network configuration GUI becomes available after a site is configured as an MCN. Upgrades and configuration changes must be performed from the MCN or SD-WAN center only.

Role of MCN:

The MCN is the central node that acts as the controller of an SD-WAN network and the central administration point for the client nodes. All configuration activities, in addition to preparation of firmware

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

packages and their distribution to the clients, are configured on the MCN. In addition, monitoring information is available only on the MCN. The MCN can monitor the entire SD-WAN network, whereas client nodes can monitor only the local Intranets and some information for those clients, which they are connected. The primary purpose of the MCN is to establish overlay connections (virtual paths) with one or more client nodes located across the SD-WAN network for Enterprise Site-to-Site communication. An MCN can administer and have Virtual Paths to multiple client nodes. There can be more than one MCN, but only one can be active at any given time. The below figure illustrates the basic diagram of the MCN and client (branch node) appliances for a small two site network.



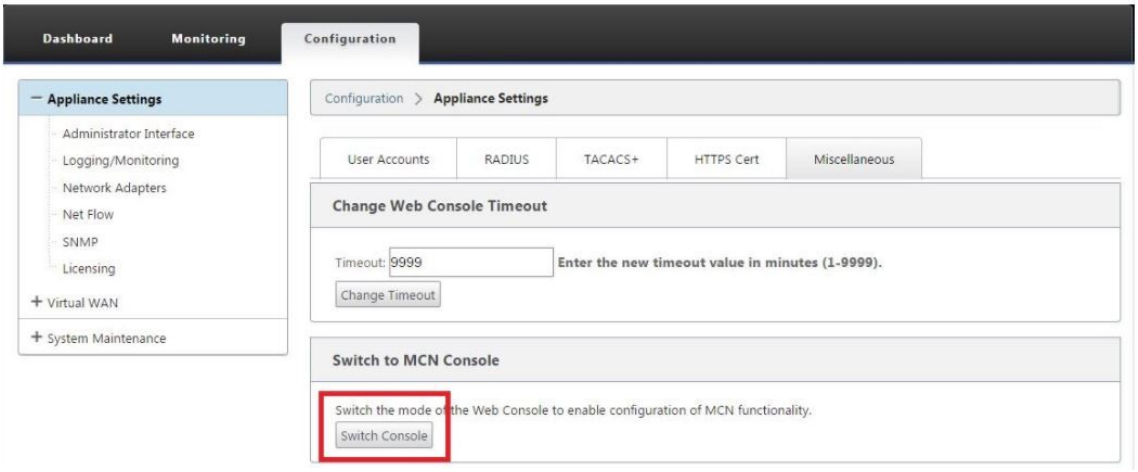
Configure SD-WAN appliance as MCN

To add and configure the MCN, you must first log into the Management Web Interface on the appliance you are designating as the MCN, and switch the Management Web Interface to MCN Console mode. MCN Console mode enables access to the Configuration Editor in the Management Web Interface to which you are currently connected. You can then use the Configuration Editor to add and configure the MCN site.

To switch the Management Web Interface to MCN Console mode, do the following:

1. Log into the SD-WAN management web interface on the appliance you want to configure as the MCN.
2. Click **Configuration** in the main menu bar of the Management Web Interface main screen (blue bar at the top of the page).
3. In the navigation tree (left pane), open the **Appliance Settings branch** and click **Administrator Interface**.
4. Select the **Miscellaneous** tab. The miscellaneous administrative settings page opens.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



At the bottom of the **Miscellaneous** tab page is the **Switch to [Client, MCN] Console** section. This section contains the **Switch Console** button for toggling between appliance console modes.

The section heading indicates the current console mode, as follows:

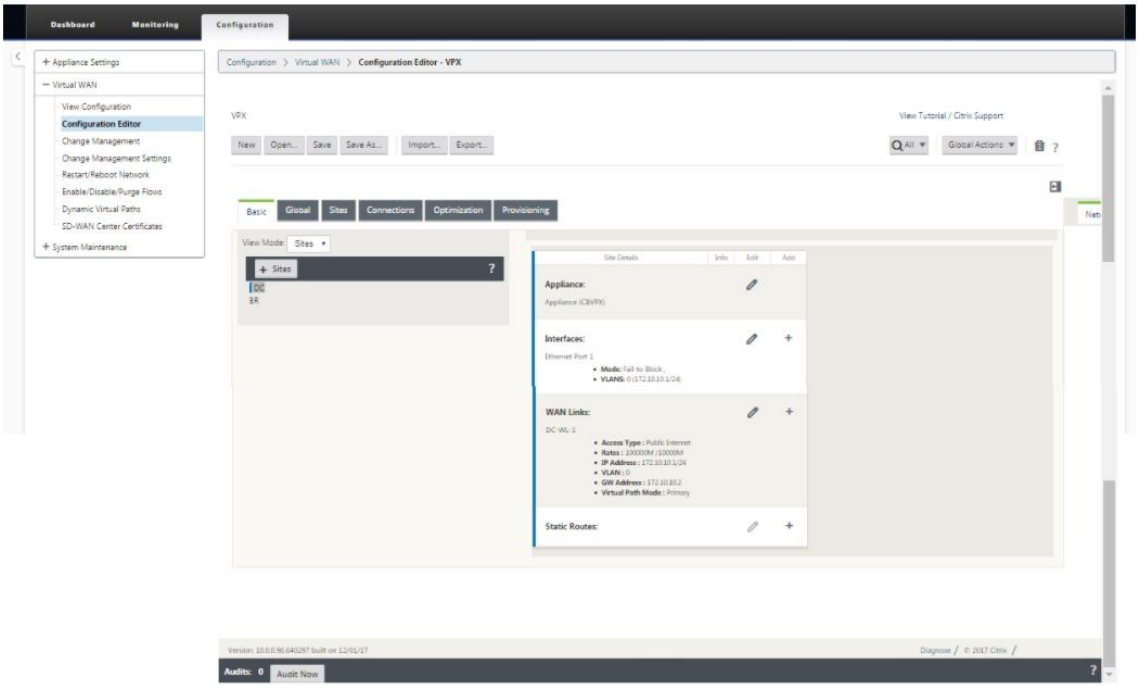
- When in Client Console mode (default), the section heading is Switch to MCN Console.
- When in MCN Console mode, the section heading is Switch to Client Console.

By default, a new appliance is in the Client Console mode. MCN Console mode enables the Configuration Editor view in the navigation tree. The Configuration Editor is available on the MCN appliance, only.

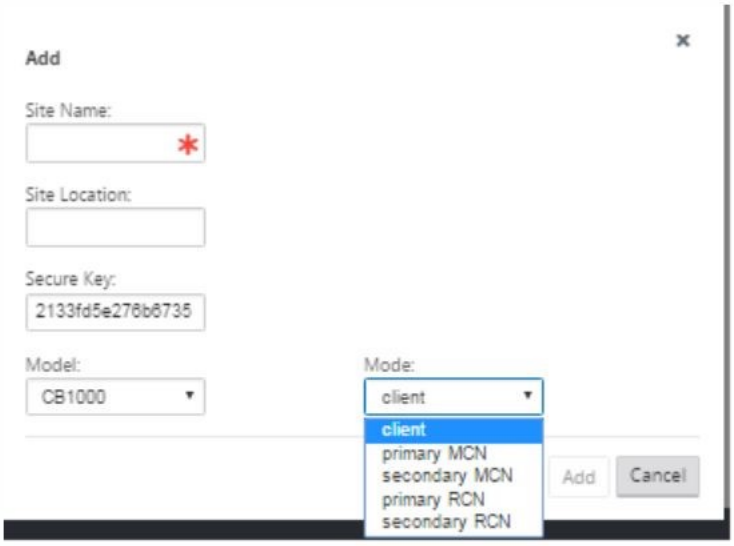
Configure MCN To add and begin configuring the MCN appliance site, do the following:

1. In the SD-WAN appliance GUI, navigate to **Virtual WAN** > **Configuration Editor**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

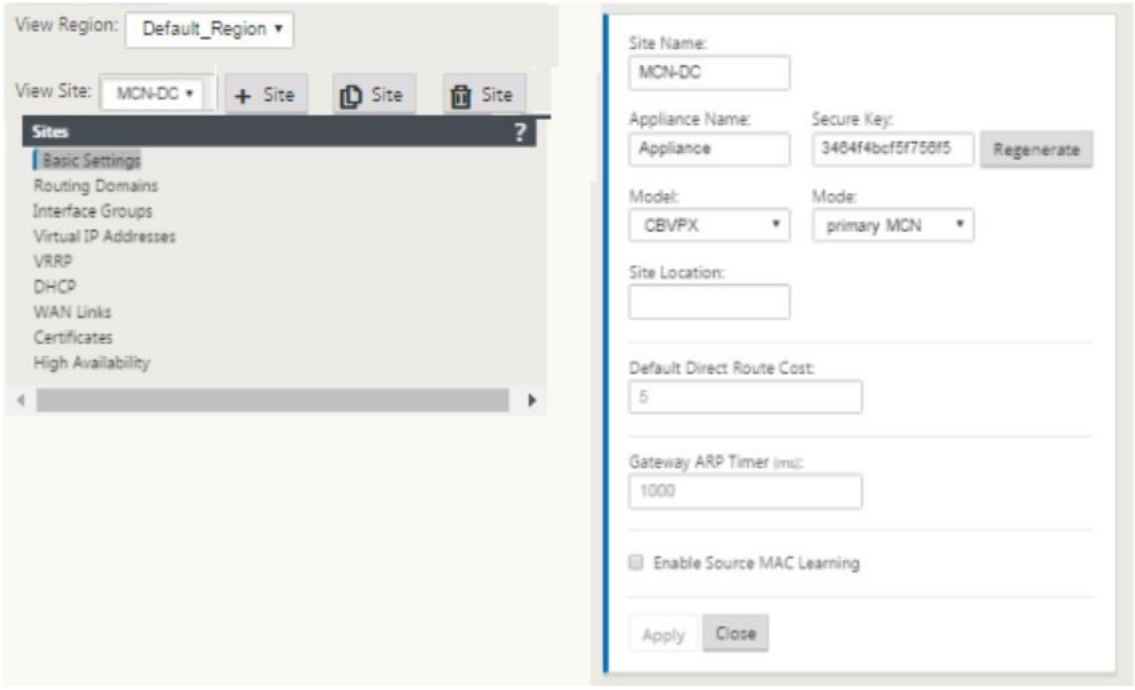


2. Click **+ Sites** in the Sites bar to begin adding and configuring the MCN site. The **Add Site** dialog box is displayed.

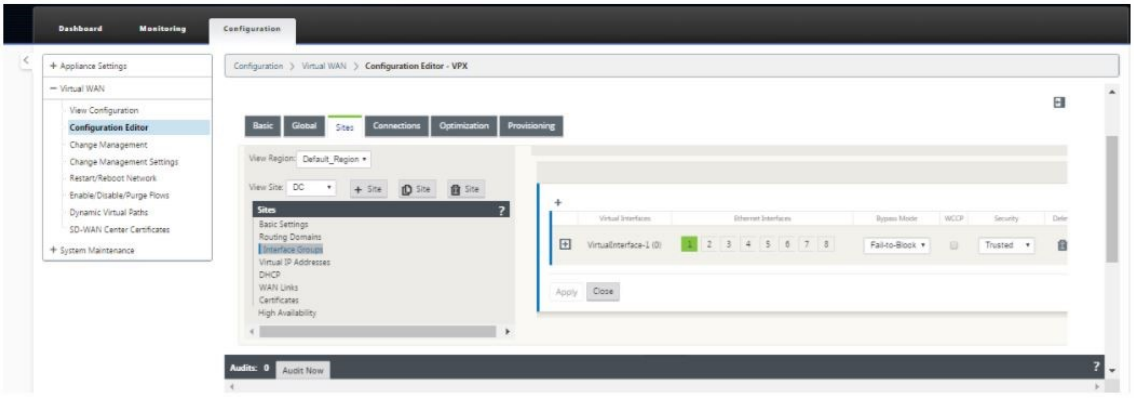


3. Enter a site name that lets you determine the geographic location and role of the appliance (DC/secondary DC). Select the correct appliance model. Selecting the correct appliance is crucial since the hardware platforms differ from each other in terms of processing power and licensing. Since we are configuring this appliance as the primary head end appliance, choose the mode as primary MCN and click **Add**.
4. This adds the new site to the sites tree and the default view shows the basic settings configuration page as shown below:

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

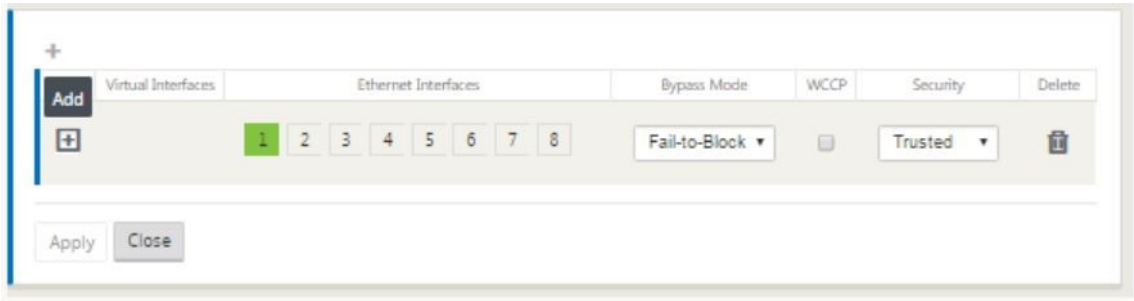


5. Enter the basic settings such as location, site name.
6. Configure the appliance so that it can accept traffic from Internet/MPLS/Broadband. Define the interfaces where the links are terminated. This depends on whether the appliance is either in overlay or underlay mode.
7. Click **Interface groups** to start defining the interfaces.

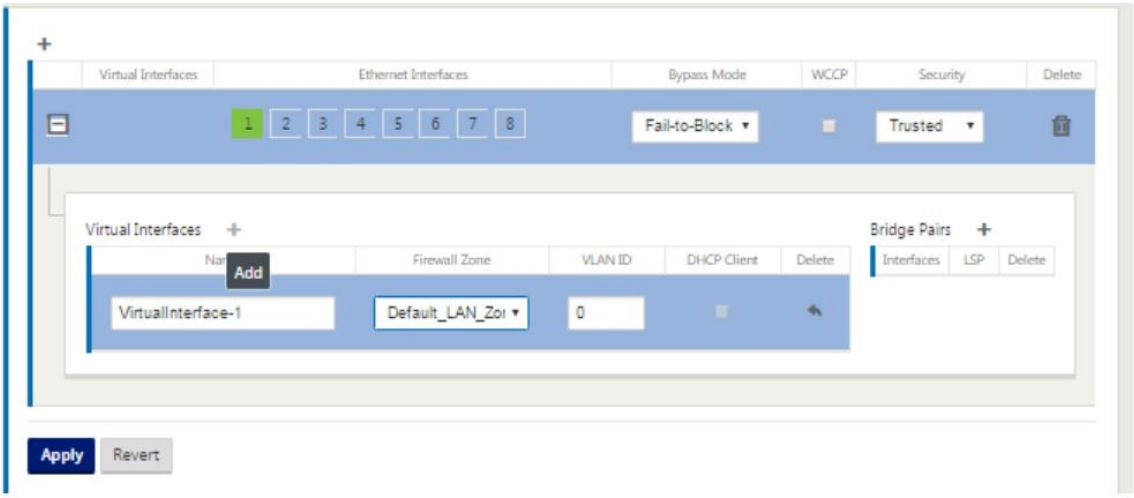


8. Click + to add virtual interface groups. This adds a new virtual interface group, the number of virtual interfaces depends on the links that you want the appliance to handle. The number of links that an appliance can handle varies from appliance model to model and the maximum number of links can be up to eight.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

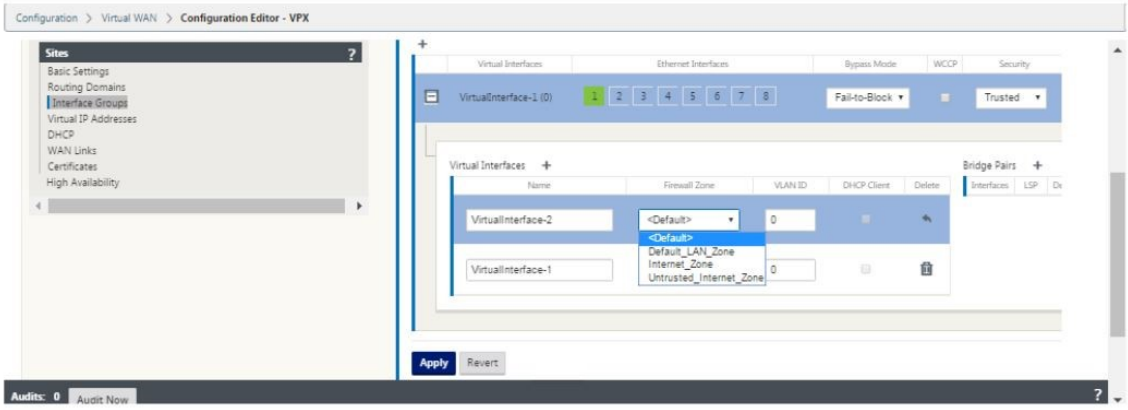


9. Click + to the right of virtual interfaces to view the screen as shown below.

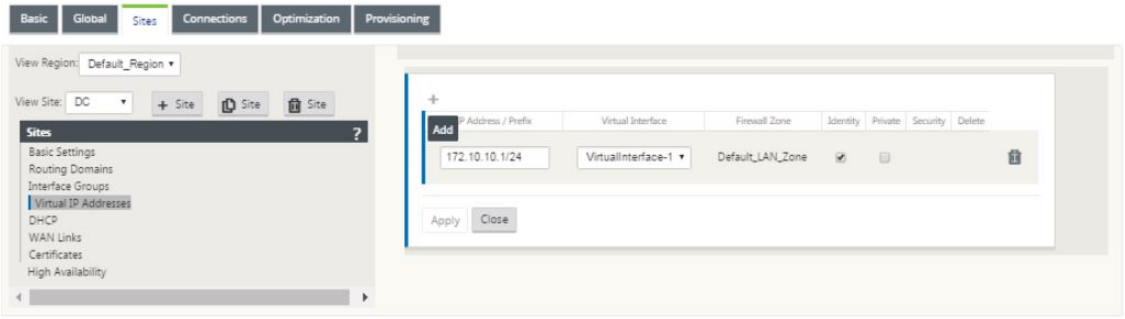


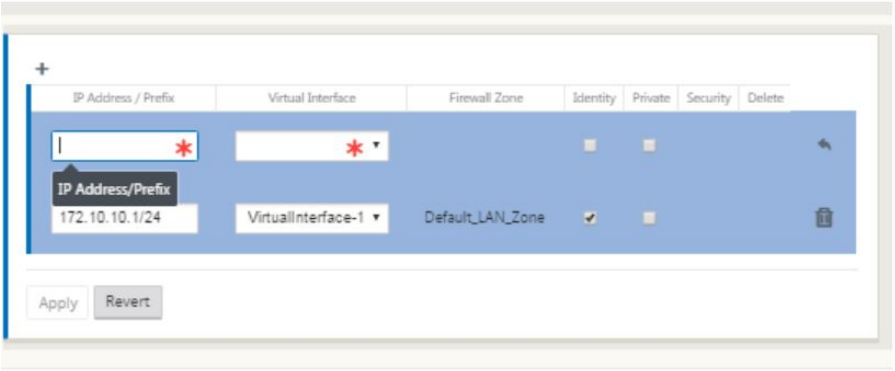
10. Select the **Ethernet interfaces**, which form the part of this virtual interface. Depending on the platform model, appliances have a pre-configured pair of fail-to-wire interfaces. If you want to enable fail-to-wire on appliances, then ensure that you are choosing the correct pair of interfaces and ensure that you choose fail-to-wire under the **Bypass Mode** column.
11. Select the security level from the drop-down list. Trusted mode is chosen, if the interface is serving MPLS links and Untrusted is chosen when Internet links are used on the respective interfaces.
12. Click + to the right of the label named virtual interfaces. This shows the Name, firewall zone and VLAN IDs. Enter the **Name and VLAN ID** for this virtual interface group. VLAN ID is used to identifying and marking traffic to and from the virtual interface, use 0 (zero) for native/untagged traffic.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



13. To configure the interfaces in fail to wire, click Bridge pairs. This adds a new bridge pair and allows for editing. Click **Apply** to confirm these settings.
14. To add more virtual interface groups click + to the right of the interface groups branch and proceed as above.
15. After the interfaces are chosen, the next step is to configure IP addresses on these interfaces. In Citrix SD-WAN terminology this is known as a VIP (Virtual IP).
16. Continue in the sites view and click the Virtual IP address to view the interfaces for configuring VIP.



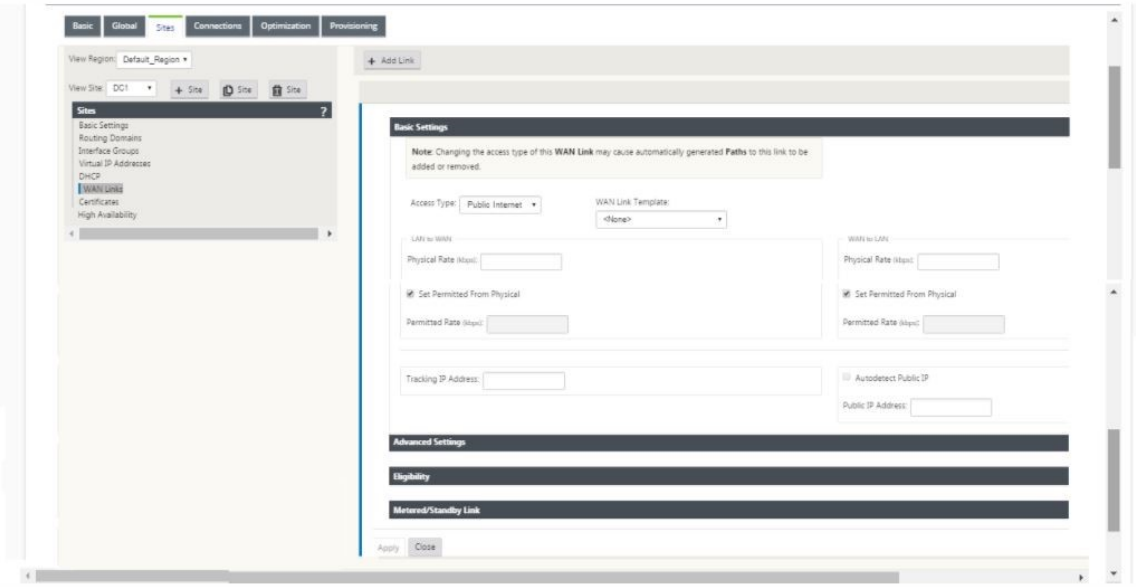


17. Enter the IP Address / Prefix information, and select the **Virtual Interface** with which the ad-

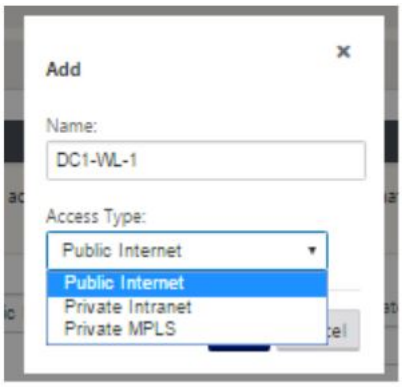
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

dress is associated. The Virtual IP Address must include the full host address and netmask. Select the desired settings for the Virtual IP address, such as the Firewall Zone, Identity, Private, and Security. Click **Apply**. This adds the address information to the site and includes it in the site Virtual IP Addresses table. To add more Virtual IP Addresses, click + to the right of the Virtual IP Addresses, and proceed as above.

18. Continue in the sites section to configure WAN Links for the site.



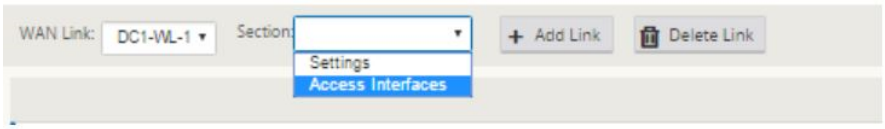
19. Click **Add link**, at the top of the panel on the right hand side. This opens a dialog box, which allows you to choose the type of link to be configured.

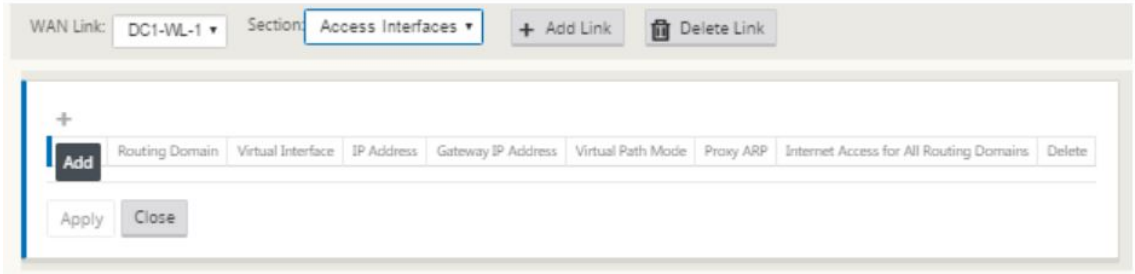


20. Public Internet is for Internet/broadband/DSL/ADSL links, whereas private MPLS is for MPLS links. Private Intranet is also for MPLS links. The difference between private MPLS and private Intranet links is that private MPLS allows for preserving the QoS policies of MPLS links.
21. If you are choosing public Internet and the IPs are assigned through DHCP, choose the auto detect IP option.
22. Select **Access Interfaces** in the WAN link configuration page. This opens the Access Interfaces

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

view for the site. Add and configure the VIP and gateway IP for each of the links as shown below.

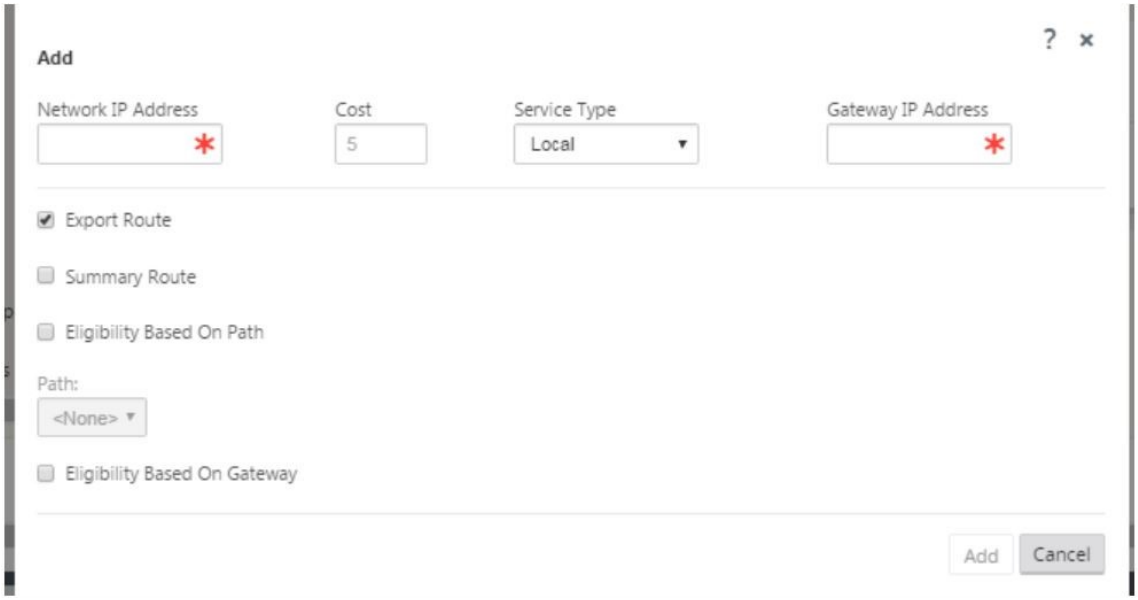




23. Click **+** to add an interface. This adds a blank entry to the table and opens it for editing.
24. Enter the name you want to assign to this Interface. You may choose to name it based on the link type and location. Keep the routing domain as default if you do not want to segregate networks and assign an IP to the Interface.
25. Ensure that you provide a publicly reachable gateway IP address if the link is an internet link or a private IP if the link is an MPLS link. Keep the virtual path mode as primary since you need this link to form virtual path.

    Note: Enable proxy ARP as the appliance replies to ARP requests for the gateway IP address when the gateway is unreachable.
26. Click **Apply** to finish configuring WAN link. If you want to configure more WAN links, then repeat the steps for another link.
27. Configure routes for the site. Click Connections view and select routes.
28. Click + to add routes, this opens a dialog box as shown below.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



29. Enter the following information is available for the new route:

    - Network IP Address
    - Cost –Cost determines which route takes precedence over the other. Paths with lower costs take precedence over higher cost routes. The default value is five.
    - Service type –Select the service, a service can be any of the following:
        - Virtual Path
        - Intranet
        - Internet
        - Passthrough
        - Local
        - GRE Tunnel
        - LAN IPsec tunnel

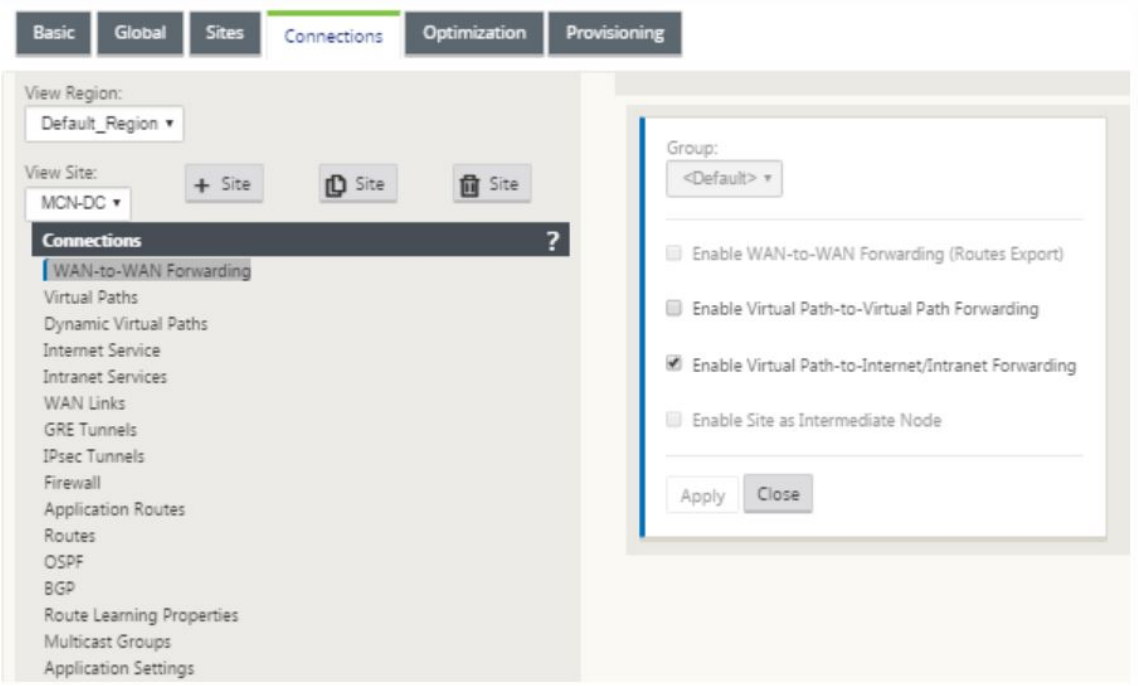
30. Click **Apply**.

To add more routes for the site click + to the right of the routes branch and proceed as above. For more information, refer to Configure MCN.

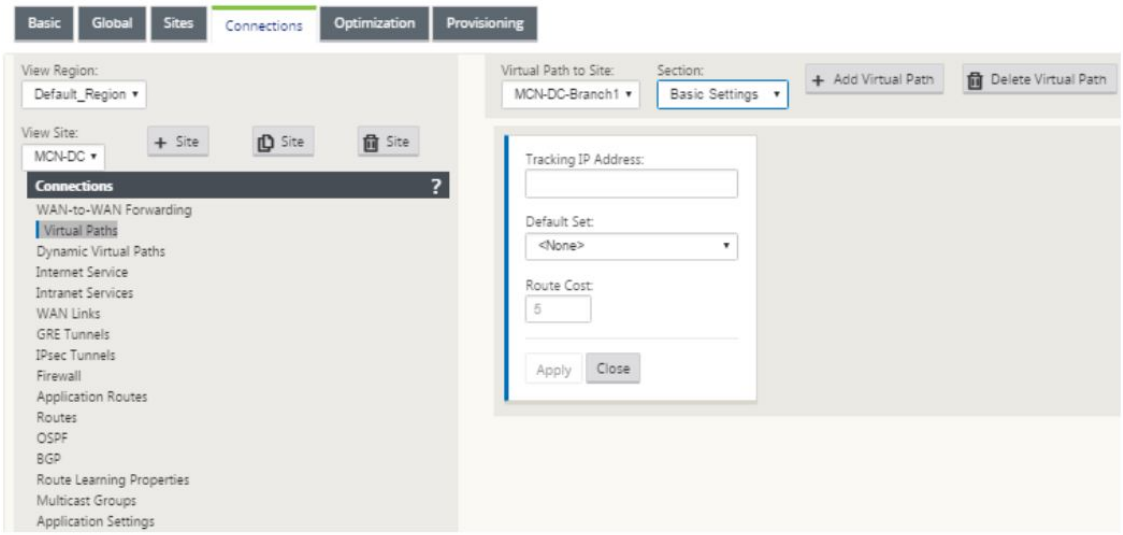
Configure virtual path between MCN and branch sites Establish connectivity between the MCN and branch node. You can do this by configuring a virtual path between these two sites. Navigate to the **Connections** tab in the configuration tree of the configuration editor.

1. Click the **Connections** tab in the configuration section. This displays the connections section of configuration tree.
2. Select the **MCN** from view site drop-down menu in the **connections** section page.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

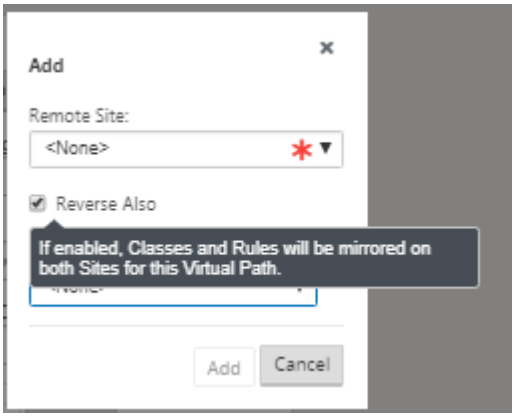


3. Select virtual path from under the connections tab to create virtual path between the MCN and branch sites.

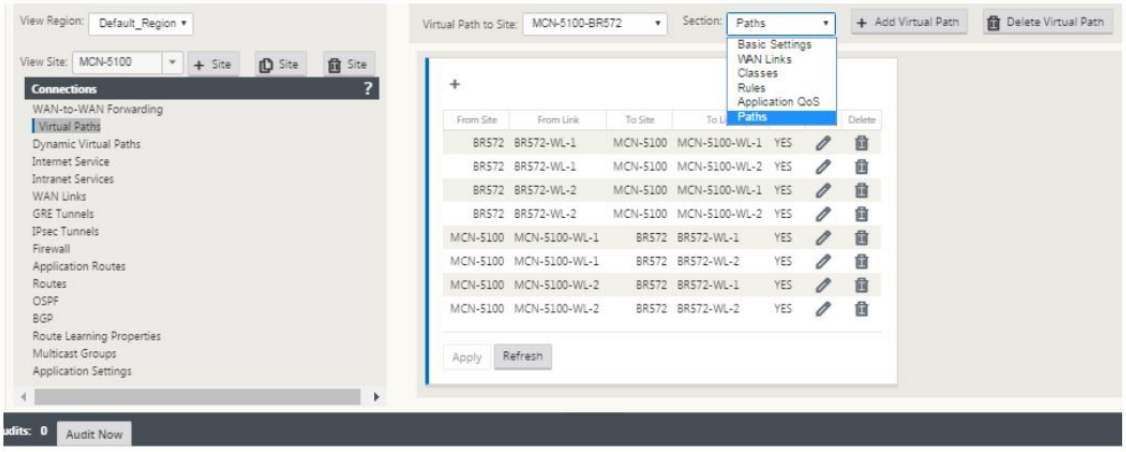


4. Click **Add Virtual Path** next to the name of the static virtual path in the virtual paths section. This opens up a dialog box as shown below. Choose the branch for which you want the Virtual path to be configured. You must configure this under the label named remote site. Select the branch node from this drop-down list, and click the check box **Reverse Also**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Traffic classification and steering are mirrored on both sites of the virtual path. After this is complete, select paths from the drop-down menu under the label named section as shown below.



5. Click **+ Add** above the paths table, which displays the add path dialog box. Specify the endpoints within which the virtual path must be configured. Now, click **Add** to create the path and click the **Reverse Also checkbox**.

   Note: Citrix SD-WAN measures link quality in both directions. This means point A to point B is one path and point B to point A is another path. With the help of unidirectional measurement of link conditions, the SD-WAN is able to choose the best route to send traffic over. This is different from measures such as RTT, which is a bi-directional metric to measure latency. For example, one connection between point A and point B is displayed as two paths and for each of them the link performance metrics are calculated independently.

This setting is enough to bring the virtual paths up between the MCN and the branch, other configuration options are also available. For more information, refer to
Configure virtual path service between MCN and Client sites.

Deploy MCN configuration The next step is to deploy the configuration. This involves the following two steps:

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

1. Export the SD-WAN configuration package to Change Management.

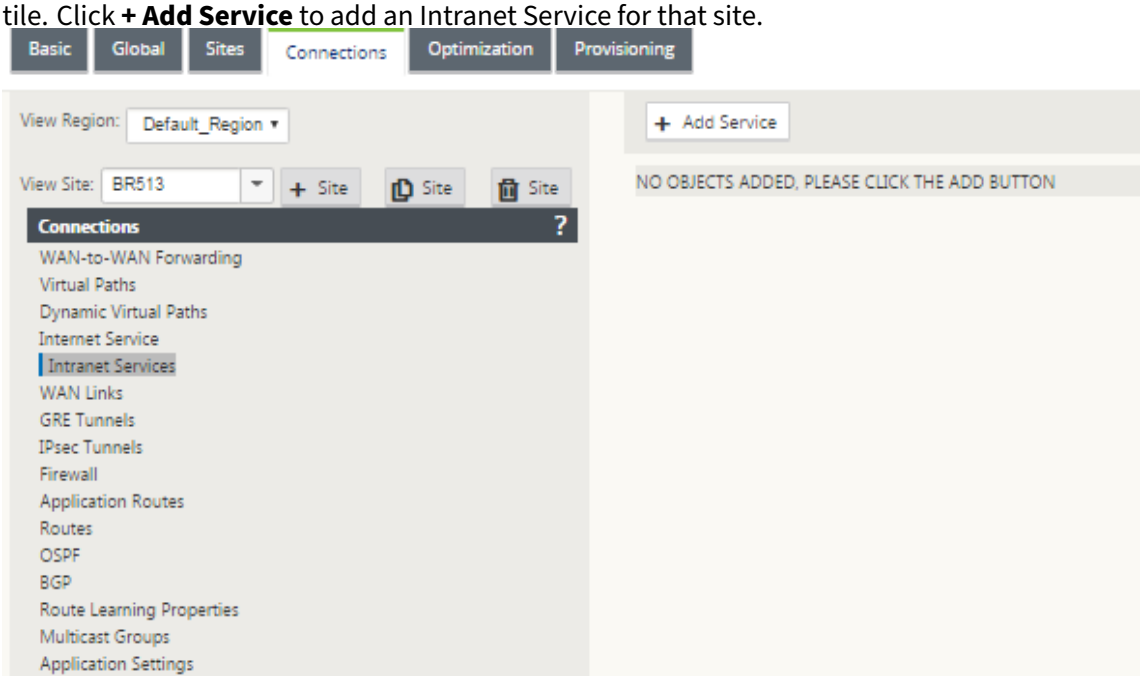
    - Before you can generate the Appliance Packages, you must first export the completed configuration package from the **Configuration Editor** to the global **Change Management** staging inbox on the MCN. Refer to the steps provided in the section, Perform change management.

2. Generate and stage the appliance packages.

    - After you have added the new configuration package to the Change Management inbox, you can generate and stage the Appliance Packages on the branch sites. To do this, you use the Change Management wizard in the management web interface on the MCN. Refer to the steps provided in the section, Stage Appliance Packages.

Configure intranet services to connect with Azure WAN resources

1. In the SD-WAN appliance GUI, go to the **Configuration Editor**, navigate to the **Connections** tile. Click **+ Add Service** to add an Intranet Service for that site.

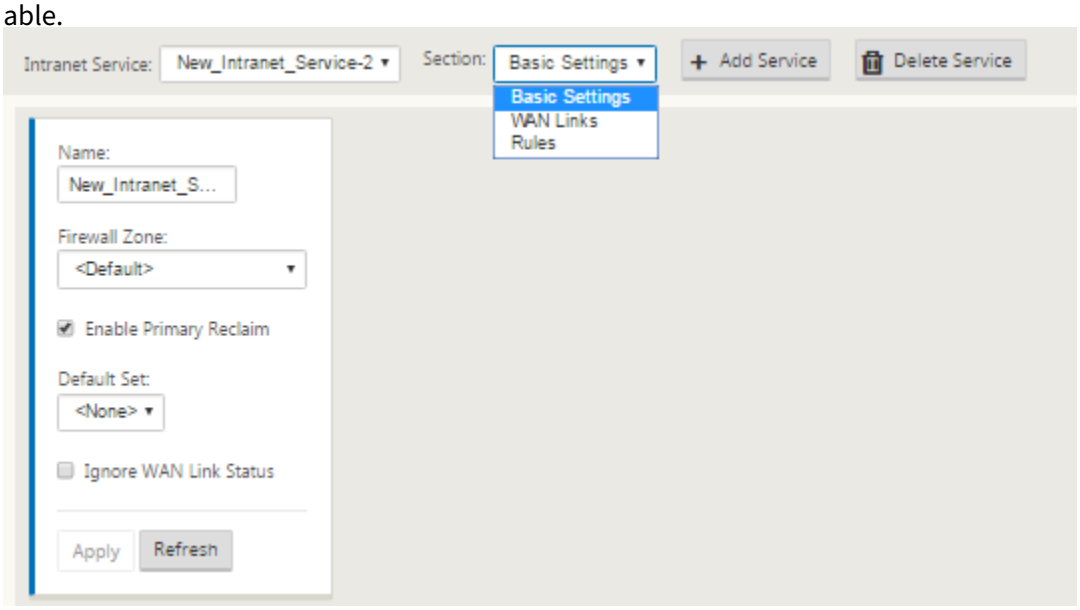


2. In the **Basic Settings** for the Intranet Service, there are several options on how you want the Intranet Service to behave during unavailability of WAN links.

    - **Enable primary reclaim** –check this box if you want the chosen primary link to take over when it comes up after failing over. If you however, choose not to check this option then the secondary link would continue to send traffic over.
    - **Ignore WAN Link status** –If this option is enabled, then packets destined for this intranet service would continue to use this service even if the constituent WAN links are unavail-

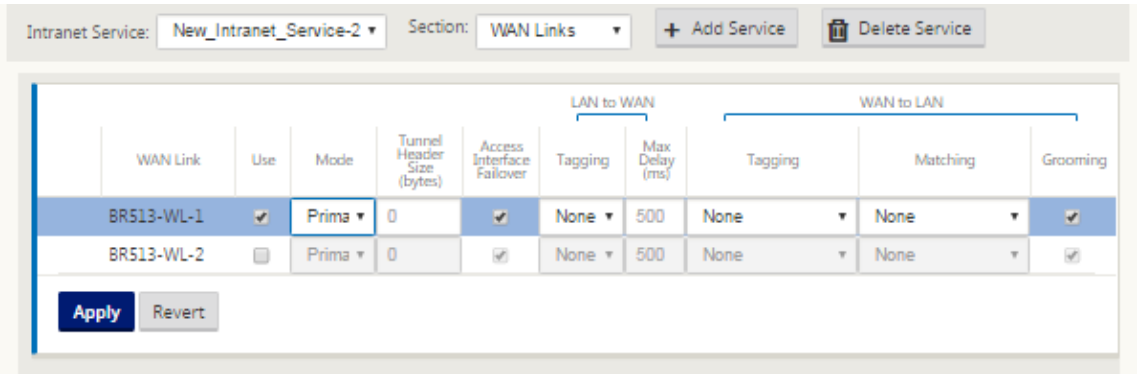
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

able.



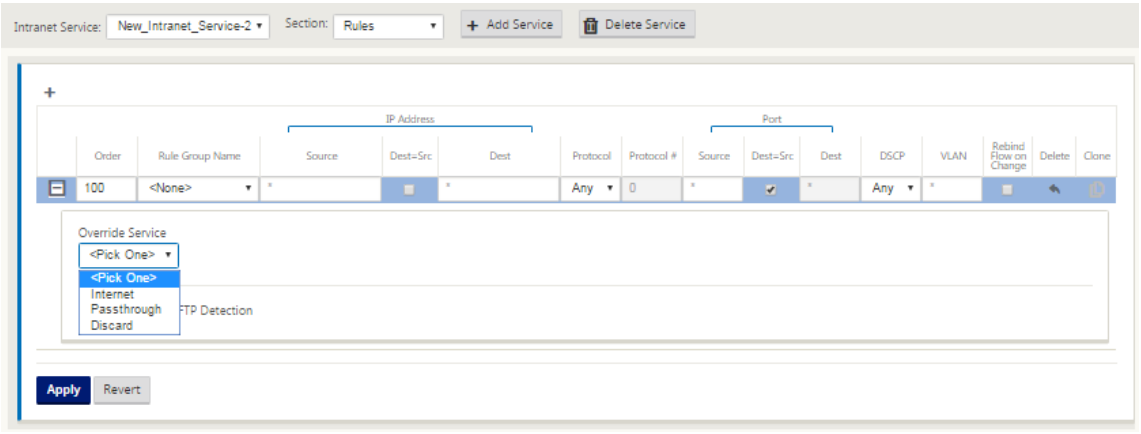
3. After configuring the basic settings, the next step is to choose the constituent WAN Links for this service. At the maximum of two links are chosen for one Intranet service. To choose the WAN links please select the WAN links option from the drop-down list labeled Section. The WAN links function in primary and secondary mode and only one link are chosen as a primary WAN link.

   Note: When a second intranet service is created, it must have the primary and secondary wan-link mapping.

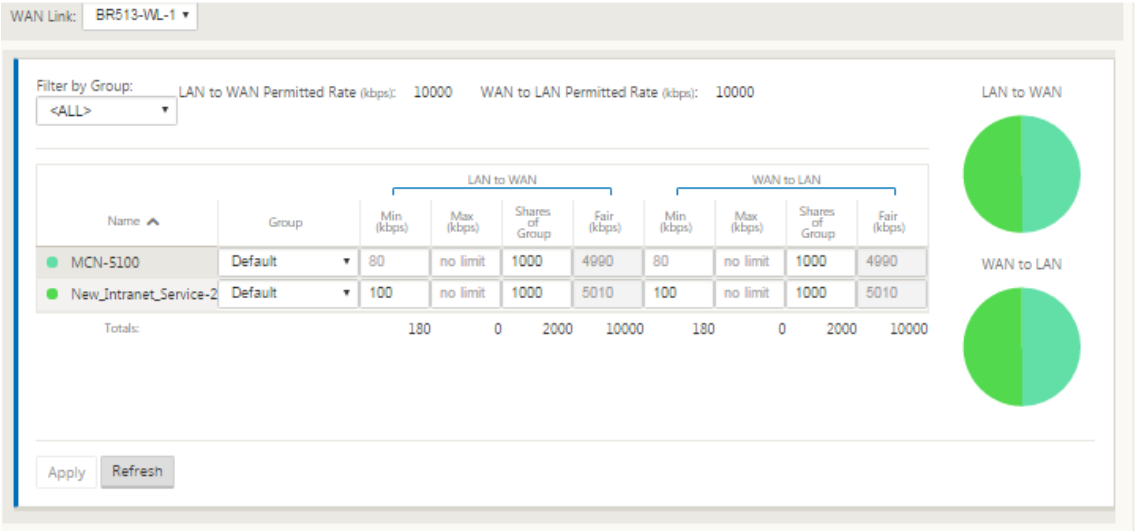


4. Branch site specific Rules are available, enabling the capability of customization of each branch site uniquely overriding any general settings configured in the global default set. Modes include desired delivery over a specific WAN link, or as an Override Service allowing for pass through or discard of the filtered traffic. For instance, if there is some traffic, which you do not wants to be going over the intranet service, you can write a rule to discard that traffic or send it over a different service (internet or pass through).

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



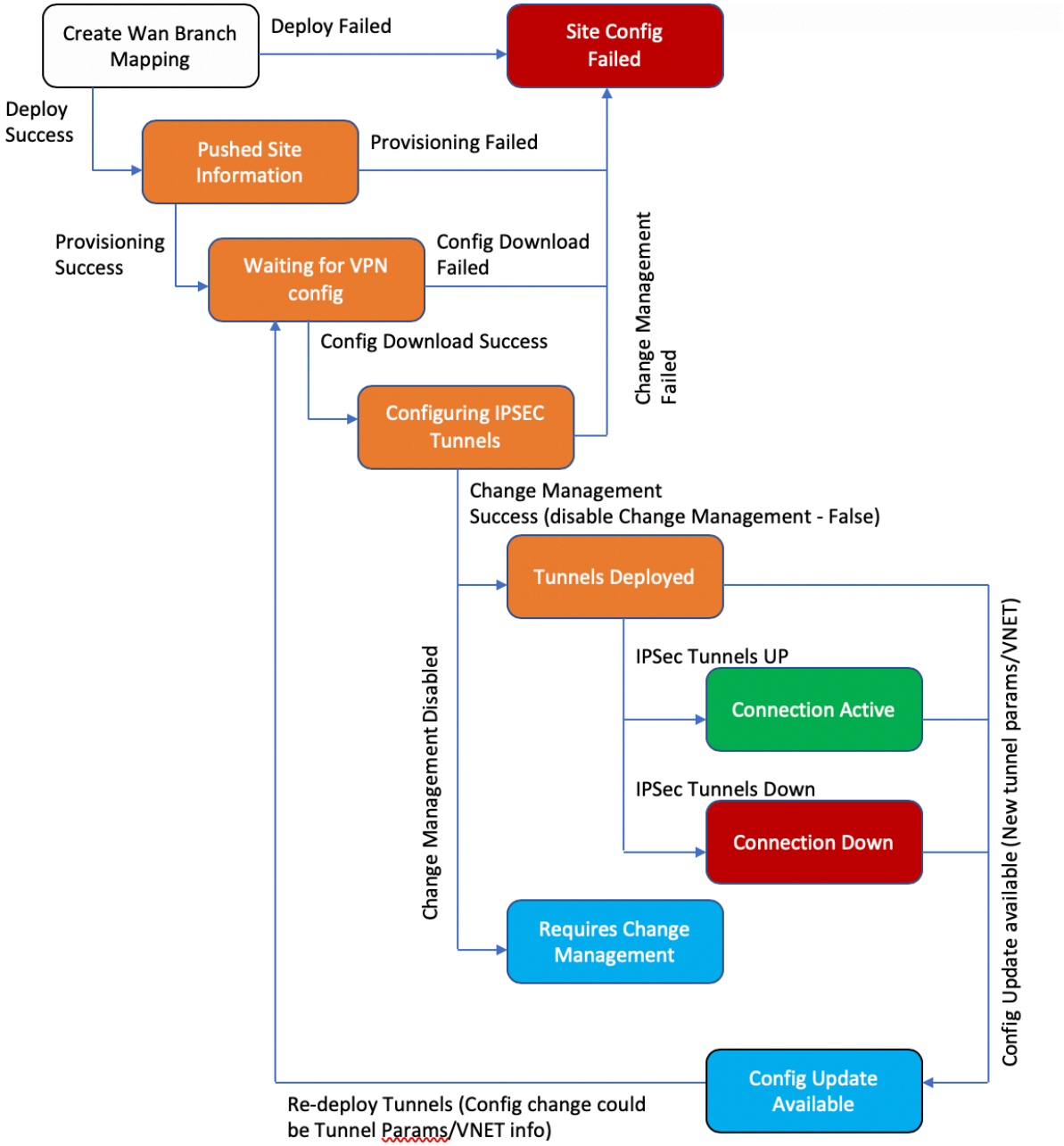
5. With Intranet Service enabled for a site, the **Provisioning** tile is made available to allow for the bidirectional (LAN to WAN / WAN to LAN) distribution of bandwidth for a WAN link among the various services utilizing the WAN link. The **Services** section allows you to further fine-tune bandwidth allocation. In addition, fair share can be enabled, allowing services to receive their minimum reserved bandwidth before fair distribution is enacted.



Configure SD-WAN Center

The following diagram describes the high-level workflow of SD-WAN Center and Azure Virtual WAN connection and corresponding state transitions of the deployment.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Configure Azure settings:

- Provide Azure Tenant ID, Application ID, Secret Key and Subscription ID (also known as service

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

principal).

Configure branch site to WAN association:

- Associate a branch site to a WAN resource. Same site cannot be connected to multiple WANs.
- Click **New** to configure Site-WAN association.
- Select **Azure WAN-resources**.
- Select **Site Names** to be associated with the WAN resources.
- Click **Deploy** to confirm the association. The WAN links to be used for Tunnel Deployment is auto-populated with the one with best link capacity.
- Wait for the status to change to 'Tunnels Deployed'to view the **IPsec tunnel** settings.
- Use the SD-WAN Center Reporting view to check status of the respective IPsec tunnels. The IPsec tunnel status must be GREEN for the data traffic to flow, which says the connection is active.

Provision SD-WAN Center:

SD-WAN center is the management and reporting tool for Citrix SD-WAN. The required configuration for Virtual WAN is performed in SD-WAN Center. SD-WAN center is available only as a virtual form factor (VPX) and needs to be installed on a VMware ESXi or a XenServer hypervisor. The minimum resources needed to configure an SD-WAN center appliance are 8 GB RAM and 4 CPU cores. Here are the steps to Install and configure an SD-WAN center VM.

Configure SD-WAN Center for Azure connectivity

Read create a service principal for more information.

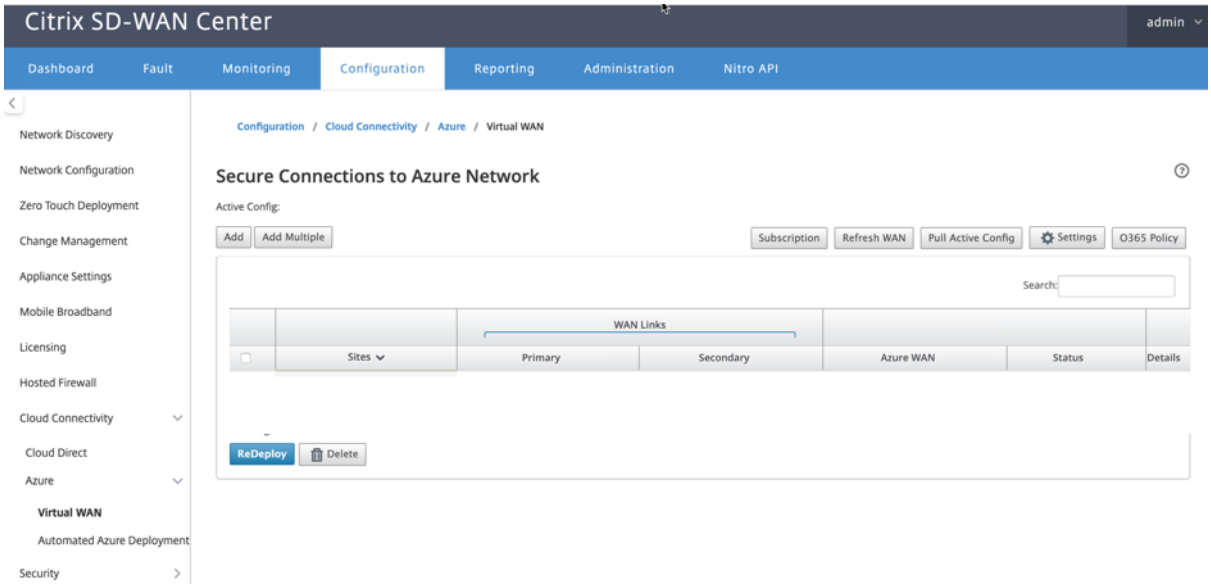
To successfully authenticate SD-WAN center with Azure, the following parameters must be available:

- Directory(Tenant ID)
- Application(Client ID)
- Secure Key(Client Secret)
- Subscriber ID

Authenticate SD-WAN Center:

In the SD-WAN Center UI, navigate to **Configuration** > **Cloud Connectivity** > **Azure** > **Virtual WAN**. Configure Azure connection settings. Refer to the following link for more information about configuring Azure VPN connection,
Azure Resource Manager.

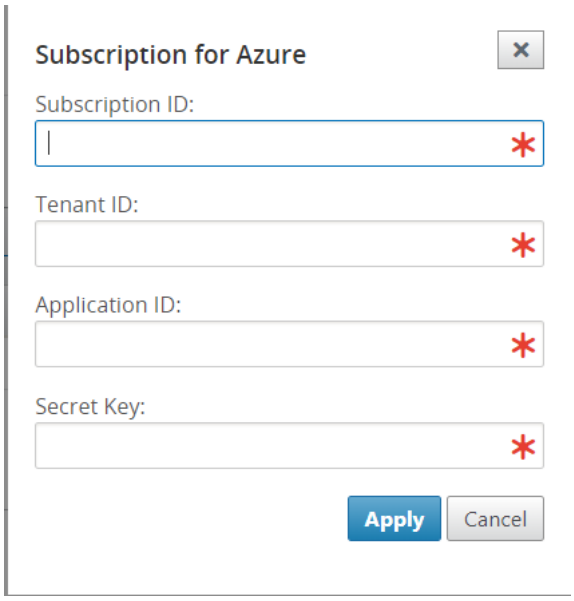
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



With 11.1.0 release and above, the Primary and Secondary WAN link configuration for Azure Virtual WAN integration is supported. The primary reason of adding secondary WAN link is to have redundancy from the Citrix SD-WAN site.

With the previous implementation, failure of the WAN link could result in traffic disruption and connectivity loss to Azure Virtual WAN. With the current implementation, the Site to Azure Virtual WAN connectivity is kept alive even if the primary WAN link is down.

Enter the **Subscription ID**, **Tenant ID**, **Application ID** and **Secure Key**. This step is required to authenticate SD-WAN center with Azure. If the credentials entered above are not correct, then the authentication fails and further action is not allowed. Click **Apply**.



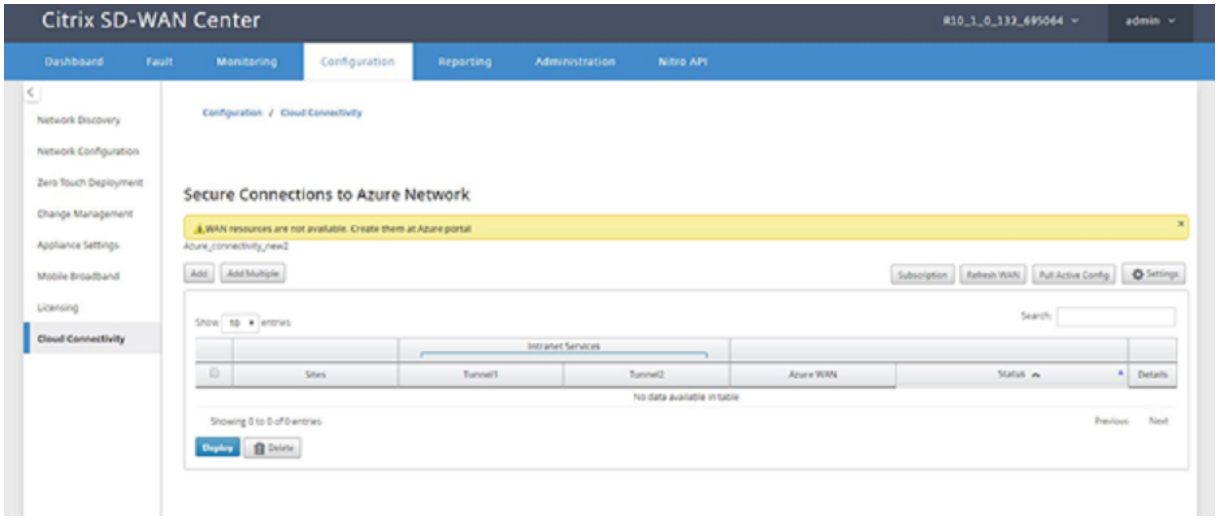
The **Storage account** field refers to the storage account that you have created in Azure. If you did

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

not create a storage account then a new storage account is automatically created in your subscription when you click **Apply**.

Obtain Azure Virtual WAN resources:

After authentication is successful, Citrix SD-WAN polls Azure for obtaining a list of Azure virtual WAN resources, which you created in the first step after logging into Azure portal. The WAN resources represent your entire network in Azure. It contains links to all Hubs that you would like to have within this WAN. WANs are isolated from each other and cannot contain a common hub or connections between two different hubs in different WAN resources.



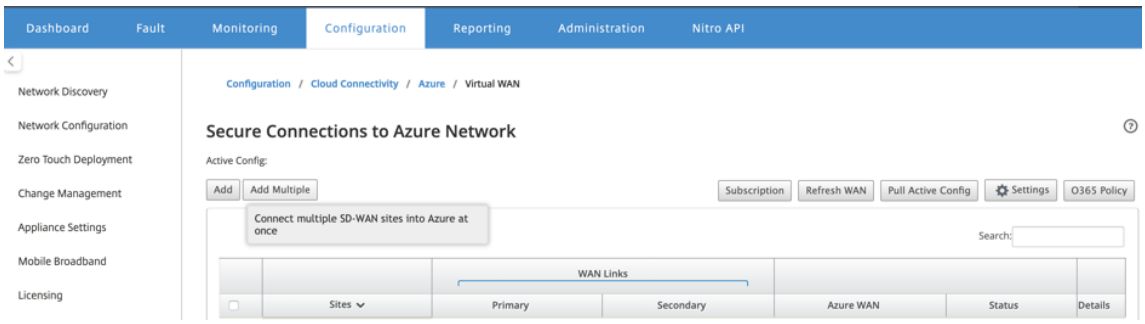
To associate branch sites and Azure WAN resources:

A Branch site needs to be associated with Azure WAN resources to establish IPsec tunnels. One Branch can be connected to multiple Hubs within an Azure virtual WAN resource and one Azure virtual WAN resource can be connected with multiple on premise branch sites. Create single rows for each Branch to Azure Virtual WAN resource deployments.

To add multiple sites:

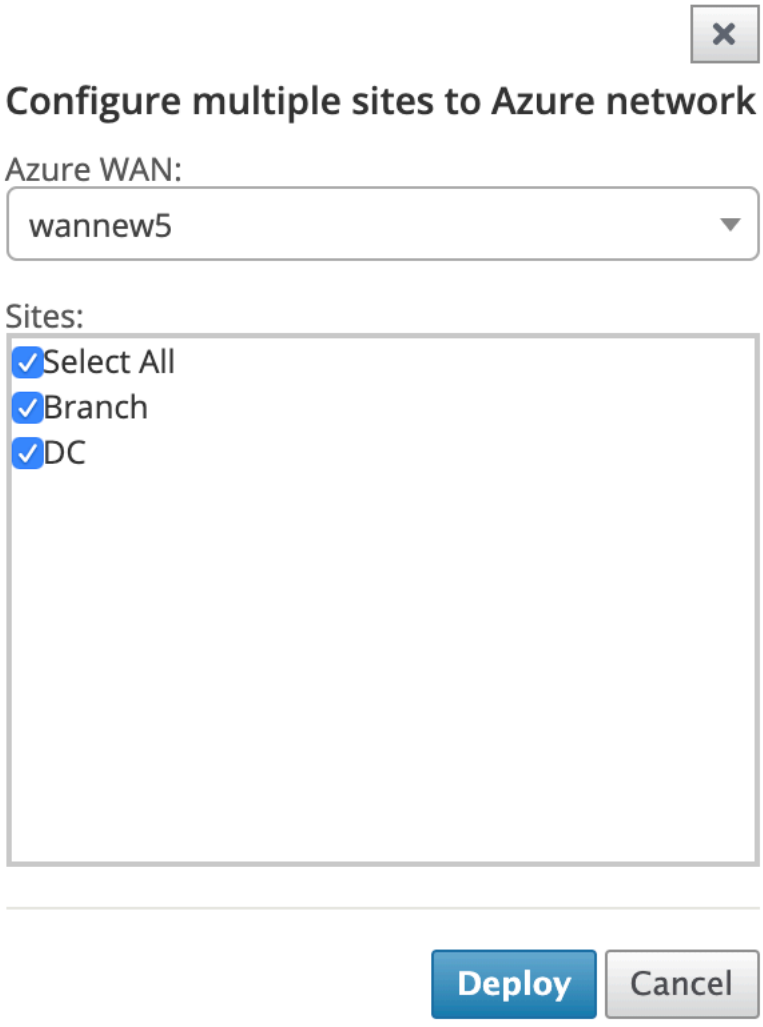
You can choose to add all the respective sites and associate them with the chosen single WAN resources.

1. Click **Add Multiple** to add all the sites that must be associated with the chosen WAN resources.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

2. The Azure WAN resources drop-down list (shown below) is pre-populated with the resources belonging to your Azure account. If no WAN resources have been created then this list is empty, and you must navigate to the Azure portal to create the resources. If the list is populated with WAN resources, choose the **Azure WAN resource** to which you need the branch sites to be connected to.
3. Choose one or all of the branch sites to initiate the process of IPsec tunnel establishment. The Sites best capacity Public Internet WAN links are chosen automatically to establish the IPsec tunnels to the Azure VPN Gateways.

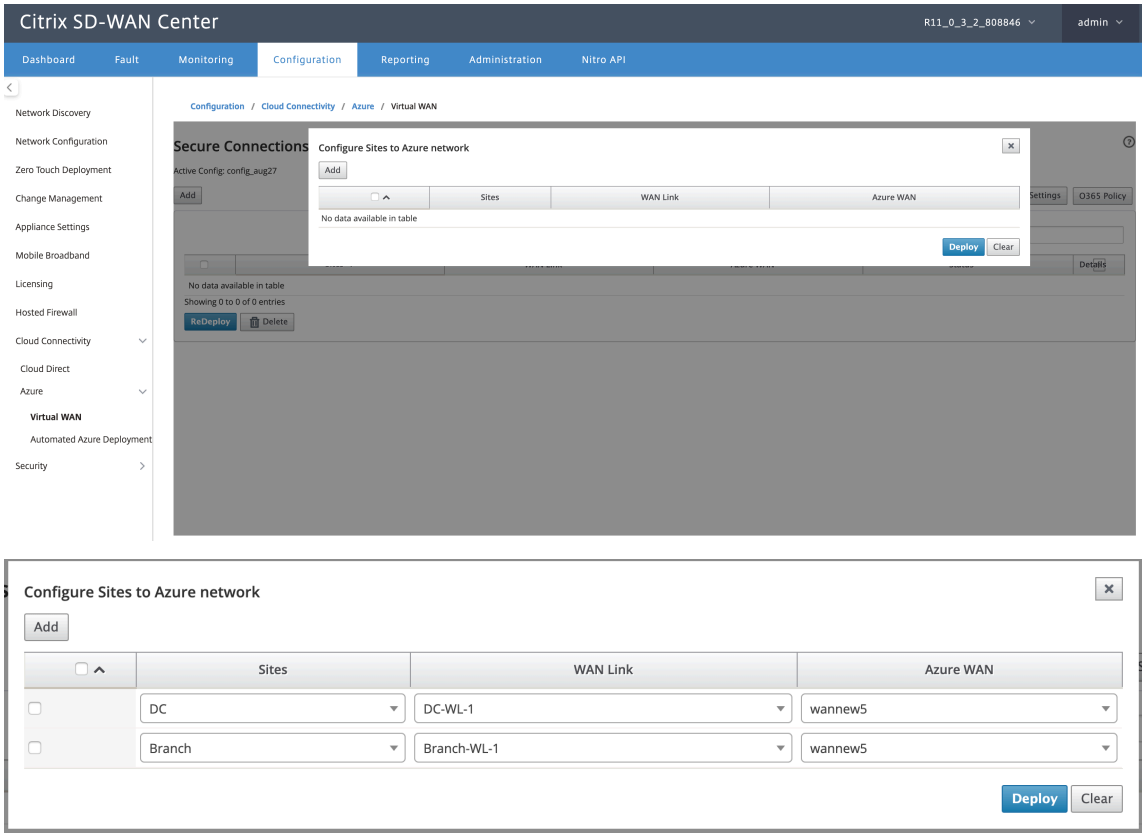


To add single site:

You can also choose to add sites one-by-one (single) and as your network grows, or if you are performing a site-by-site deployment, you can choose to add multiple sites as described above.

1. Click **Add New Entry** to select one Site Name for the Site-Wan association. Add sites in the Configure Sites to **Azure Network** dialog box.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

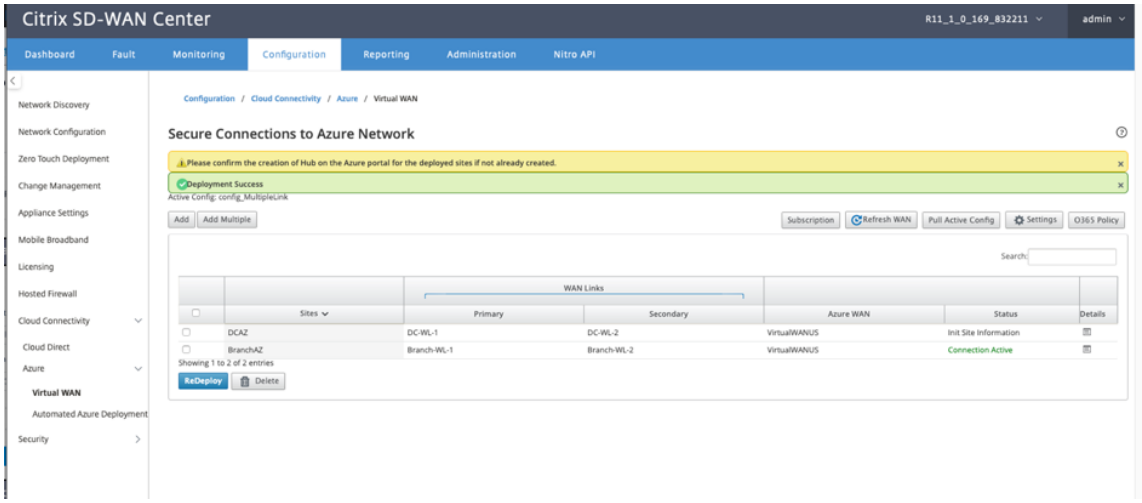


2. Select the Branch site to configure to the Azure Virtual WAN network.
3. Select the WAN link associated with the site(the Public Internet type links are listed in the order best physical link capacity)
4. Select the WAN resource to which the site must be associated to from the **Azure Virtual WANs** drop-down menu.
5. Click **Deploy** to confirm the association. The status (“Init Site Information “Pushed Site Information”& “Waiting for VPN configuration”) is updated to notify you about the process.

The deploy process includes the following status:

- Push Site Information
- Waiting for VPN configuration
- Tunnels Deployed
- Connection Active (IPsec Tunnel is up) or Connection Down (IPsec Tunnel is down)

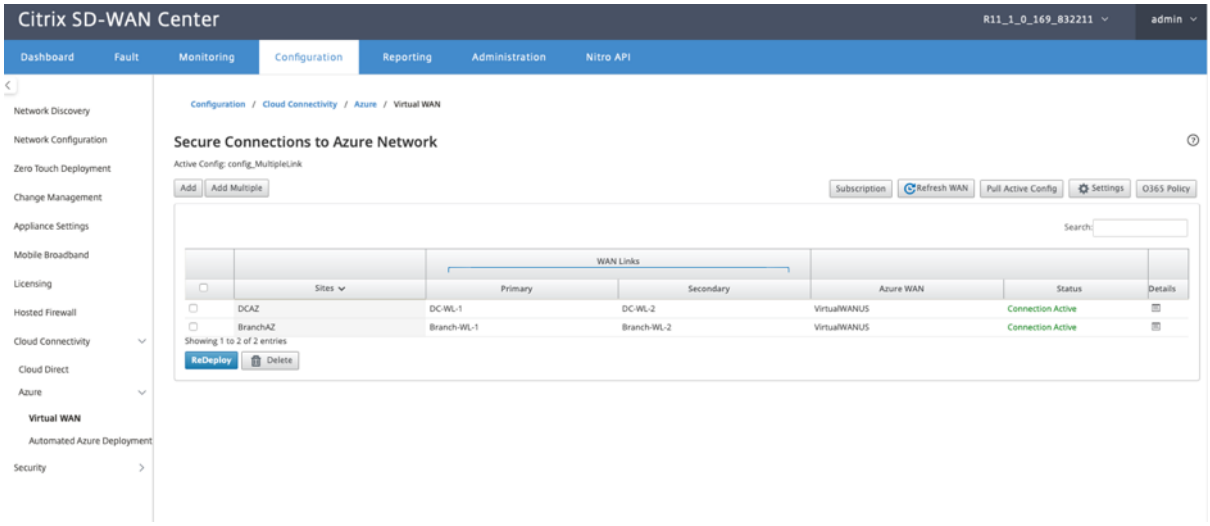
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



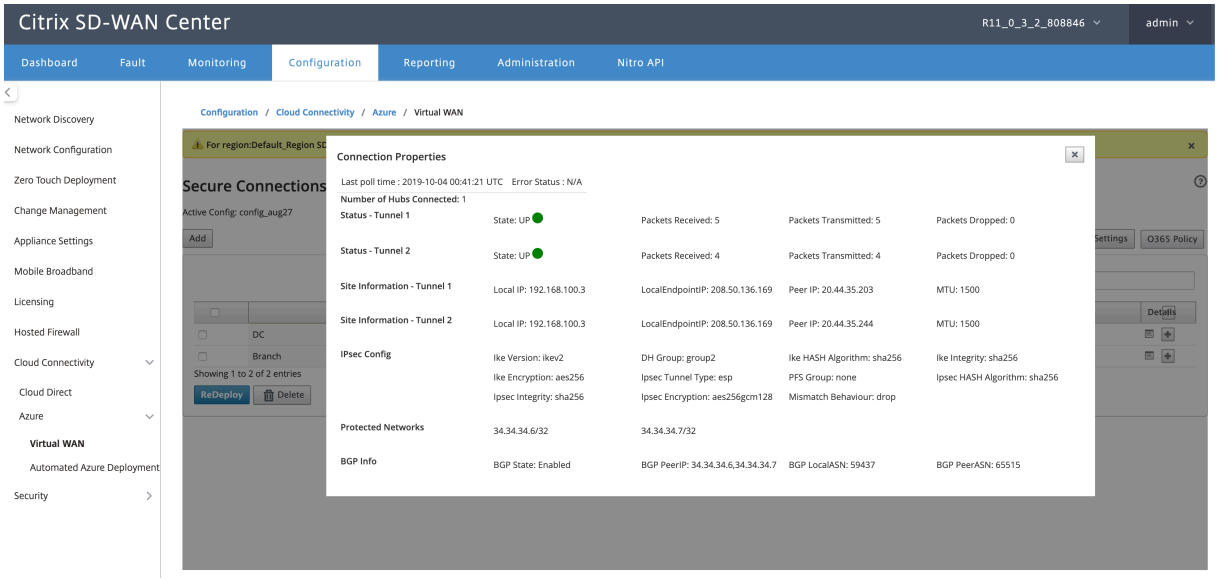
Associate Site Wan Resource Mappings (Azure portal):

Associate the deployed sites on the Azure portal to the Virtual Hubs created under the Azure Virtual WAN resource. One or more Virtual Hubs can associated with the Branch site. Each Virtual Hub is created in a specific region and specific workloads can be associated with the Virtual Hubs by creating Virtual Network Connections. Only after the Branch Site to Virtual Hub association is successful, the VPN configurations gets downloaded and respective IPsec tunnels are established from the Site to VPN Gateways.

Wait for the Status to change to Tunnels Deployed or Connection Active to view the **IPsec tunnel** settings. View IPsec settings associated with the selected services.



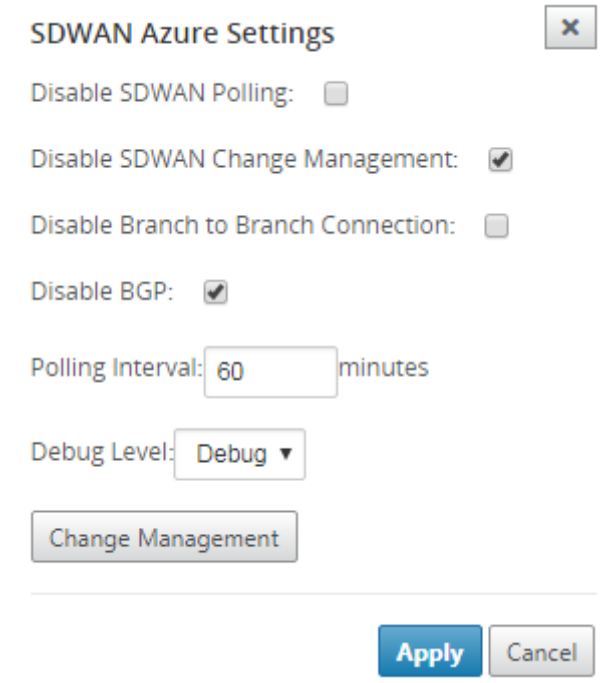
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



SD-WAN Azure settings:

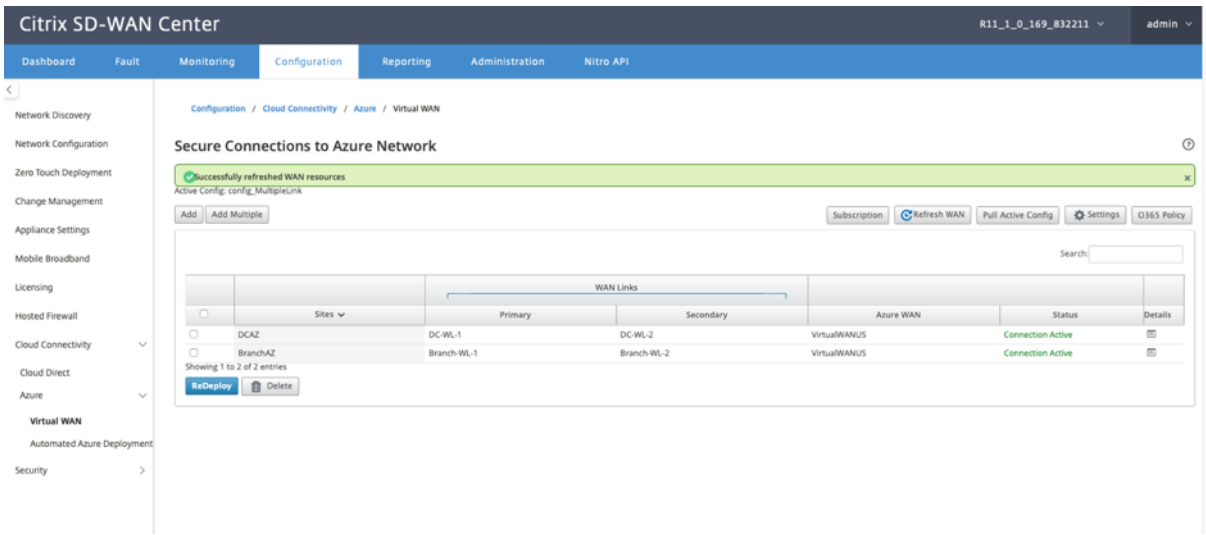
- **Disable SD-WAN change management** –By default, the Change Management process is automated. This means that anytime a new configuration is available at Azure Virtual WAN infrastructure, SD-WAN Center obtains it and starts applying it to branches automatically. However, this behavior is controlled, if you want to control when a configuration must be applied to branches. One benefit of disabling automatic change management is that the configuration for this feature and other SD-WAN features is managed independently.
- **Disable SDWAN Polling**–Disables all SD-WAN Azure new deployments and polling on existing deployments.
- **Polling Interval** - Polling interval option controls the interval of looking for configuration updates in Azure Virtual WAN infrastructure, the recommended time for polling interval is 1 hour.
- **Disable Branch-to-Branch Connection** –Disables branch-to-branch communication over Azure Virtual WAN infrastructure. By default, this option is disabled. Once you enable this, it means on-prem branches are able to communicate with each other and the resources behind the branches over IPsec through Azure's Virtual WAN Infra. This does not have any effect on branch-to-branch communication over SD-WAN virtual path, branches are able to communicate with each other and their respective resources/end points over virtual path even if this option is disabled.
- **Disable BGP** –This disables BGP over IP, by default it is disabled. Once enabled the site routes are advertised over BGP.
- **Debug Level** –Enables capturing logs to debug if there is any connectivity issues.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Refresh WAN resources:

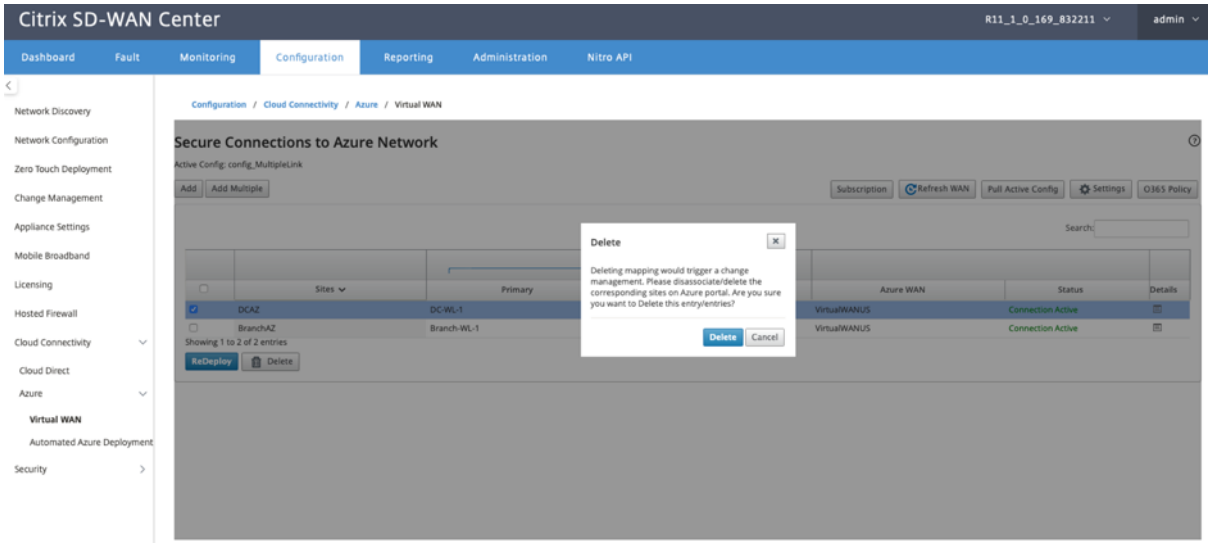
Click the **Refresh** icon to retrieve latest set of WAN Resources that you updated on the Azure Portal. A message stating, "successfully refreshed WAN resources"is displayed after the refresh process is complete.



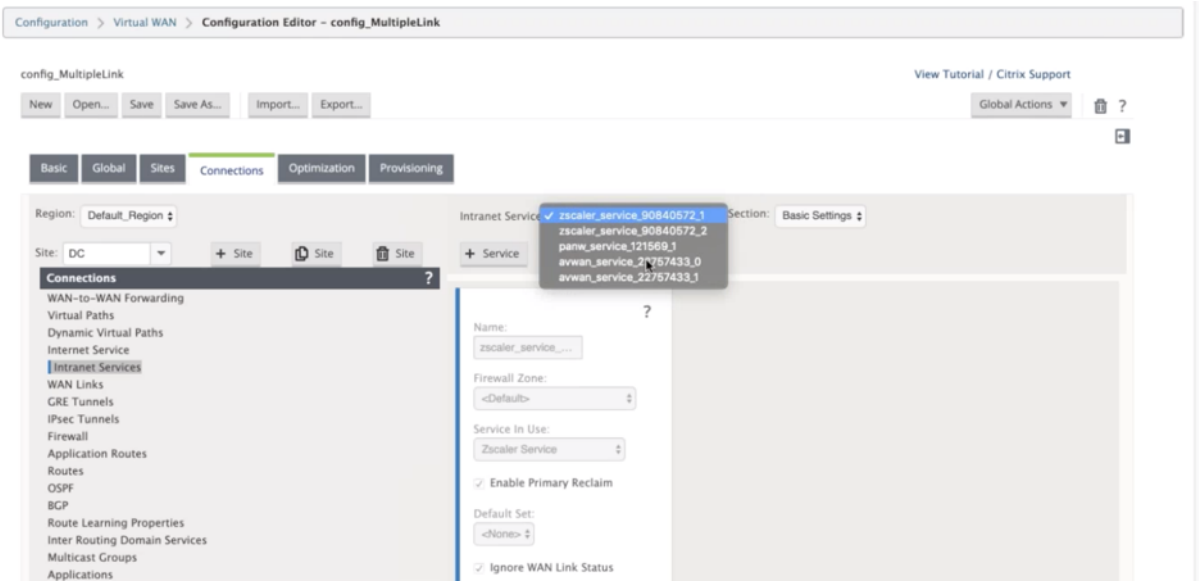
Remove site WAN resource association Select one or multiple mappings to perform deletion. Internally, the SD-WAN appliance Change Management process is triggered and until it is successful, the Delete option is disabled to prevent from performing further deletions. Deleting mapping requires you to disassociate or delete the corresponding sites in the Azure portal. The user has to perform this

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

operation manually.

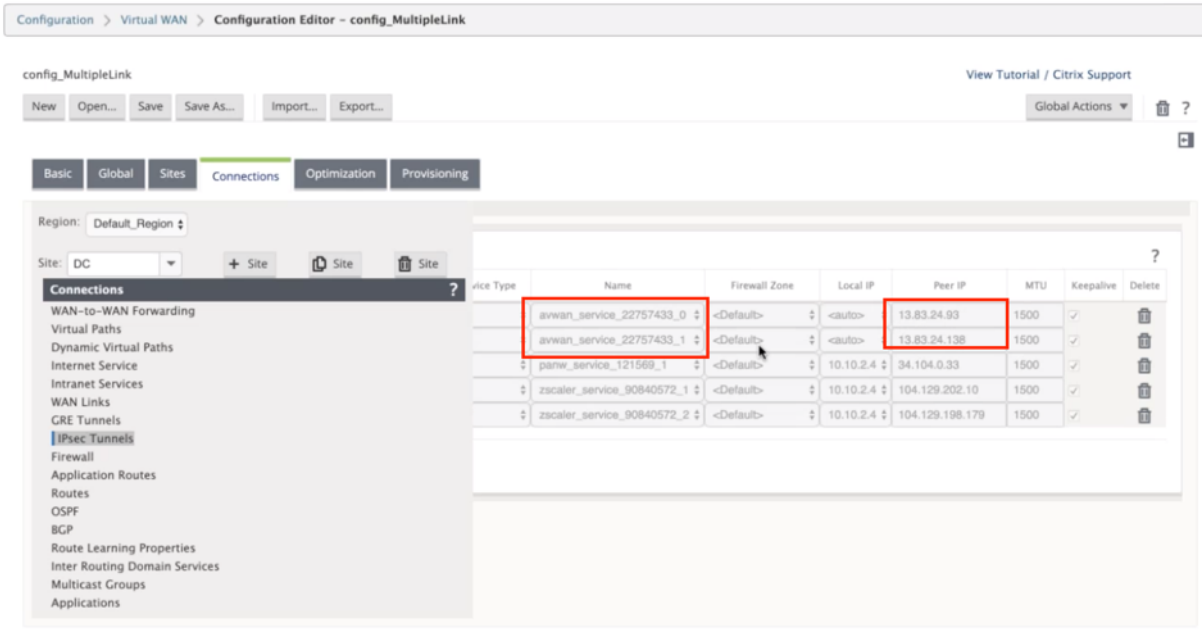


Once the tunnels are created, you can see two intranet services created in your MCN.

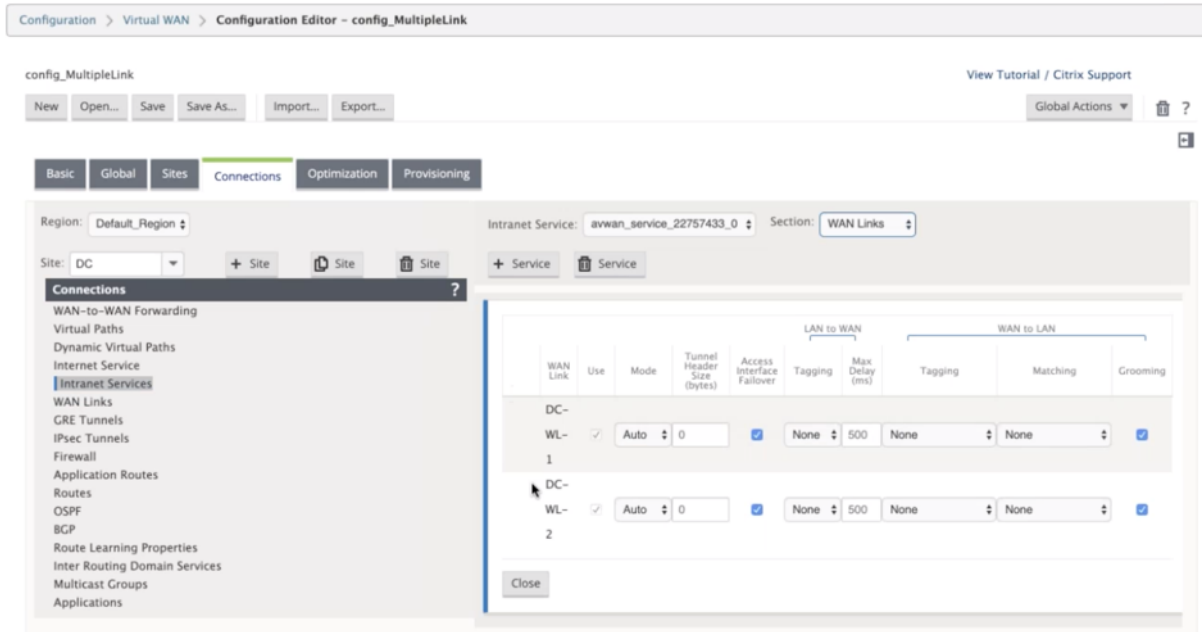


Each Intranet service corresponds to IPsec tunnels that are created with Peer IPs (Azure Virtual WAN end point IPs).

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

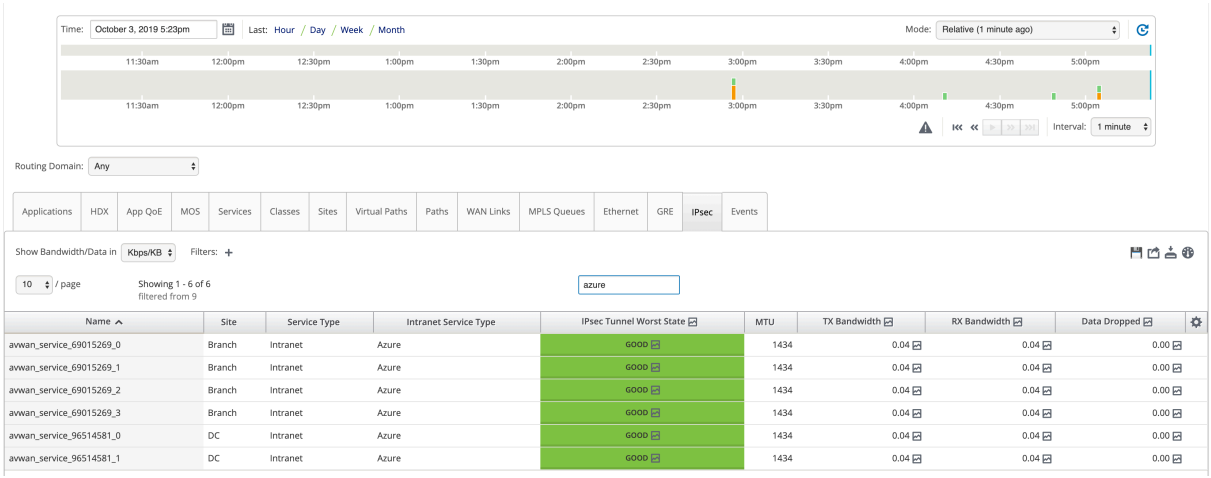


From the **Intranet Services**, if you select **WAN Links** from the **Section** drop-down list, you can see both primary and secondary WAN link that specified by you. By default the mode is set to **Auto**.



Monitor IPsec Tunnels In the SD-WAN Center UI, navigate to **Reporting** > **IPsec** to check the status of IPsec tunnels. The tunnel status must be GREEN for the data traffic to flow.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Cloud Direct Service

March 12, 2021

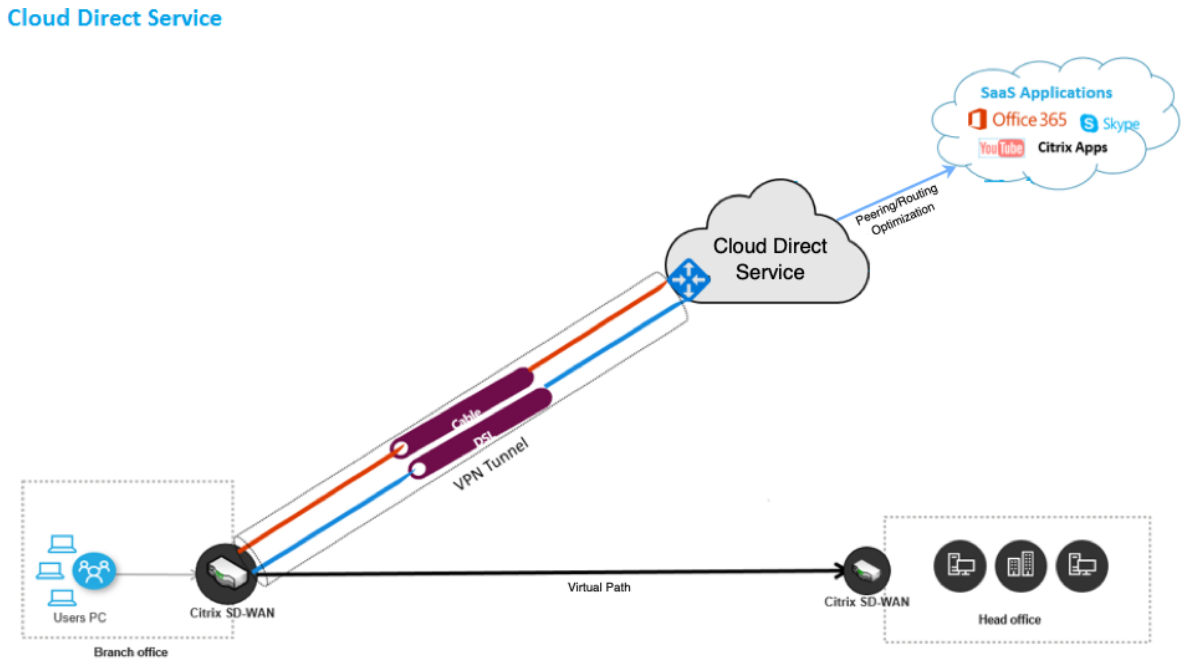
The Cloud Direct service delivers SD-WAN functionalities as a cloud service through reliable and secure delivery for all internet-bound traffic regardless of the host environment (data center, cloud, and internet). It improves network visibility and management. It enables partners to offer managed SD-WAN services for business critical SaaS applications to their end customers.

Cloud direct service offers the following advantages:

- **Redundancy** - Uses multiple internet WAN links and provides seamless failover.
- **Link aggregation** - Uses all internet WAN links at the same time.
- Intelligent load-balancing across WAN connections from different providers:
  - Measuring packet loss, jitter and throughput.
  - Custom application identification.
  - Application requirement and circuit performance matching (adapt to real-time network conditions).
- SLA-grade Dynamic QoS Capability to internet circuit:
  - Dynamically adapts to varying circuit throughput.
  - Adaption through the tunnel at ingress and egress endpoints.
- Rerouting VOIP calls between circuits without dropping the call.
- End-to-end monitoring and visibility.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Cloud direct service workflow



Before you begin deploying the Cloud Direct Service, ensure that the following steps are completed:

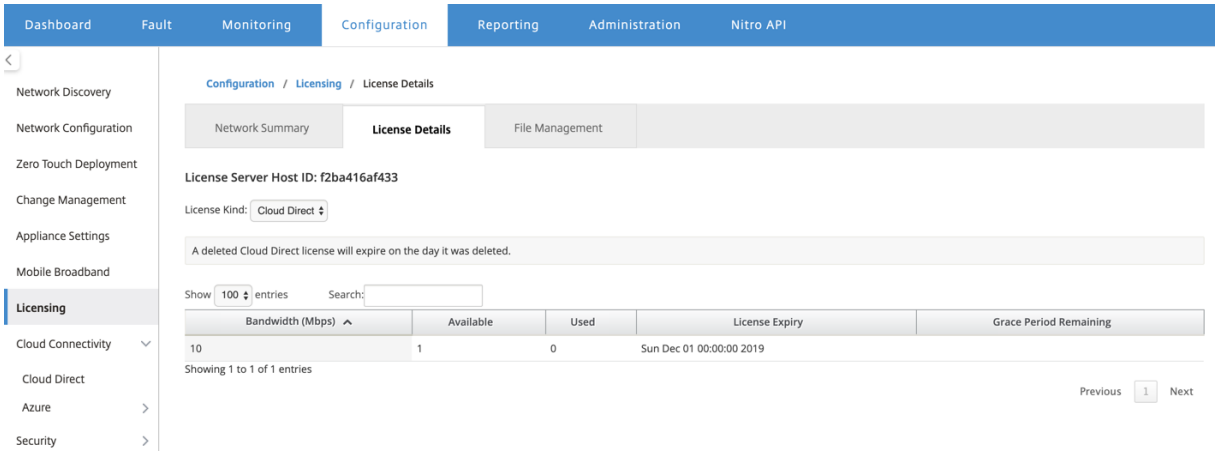
1. Have a 410-SE, 210-SE, or 1100-SE/PE edition appliance. If the factory shipped SD-WAN version of the appliance is earlier than 9.3.5, then you must follow the USB reimaging procedure to upgrade the appliance to the latest shipping base image.
2. Perform single step upgrade procedure to install the software version that supports Cloud Direct Service.
3. Configure the MCN appliance and establish the virtual paths with its branches:
    - Configure branch site. See Configure Branch for more information.
    - Create application objects for application-based routes.
        - If you intend to selectively steer the applications through the Cloud direct service, create the application objects by including the corresponding applications, see how to create Application Objects, which are routed through the Cloud direct service. To manage Internet bound traffic, the Internet service must be created from the appliance configuration editor. For more information, see Internet Service.
        - If you intend to steer all internet bound traffic through the Citrix Cloud direct service, then you can skip creating the specific application objects.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Licensing

The Cloud Direct service feature is licensed independently from the base licenses of SD-WAN. Ensure that you have installed the required licenses for the Cloud Direct service on SD-WAN Center. For more information, see Citrix SD-WAN Center as a license server.sd-wan-center-as-license-server.

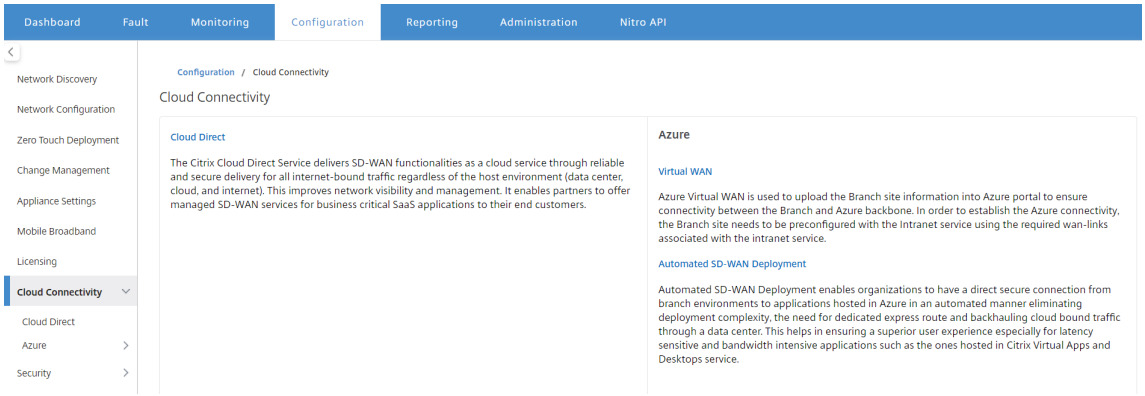
The Licensing page provides details about the installed Cloud Direct service license information.



> **Note**
>
> There is a grace period of 30 days for the expired or deleted Cloud Direct licenses, before which you need to install the valid licenses for the deployed Cloud Direct sites to be functional. If no valid licenses are installed before the expiry of the Grace period, SD-WAN Center disables the Cloud Direct service on site using the expired license.

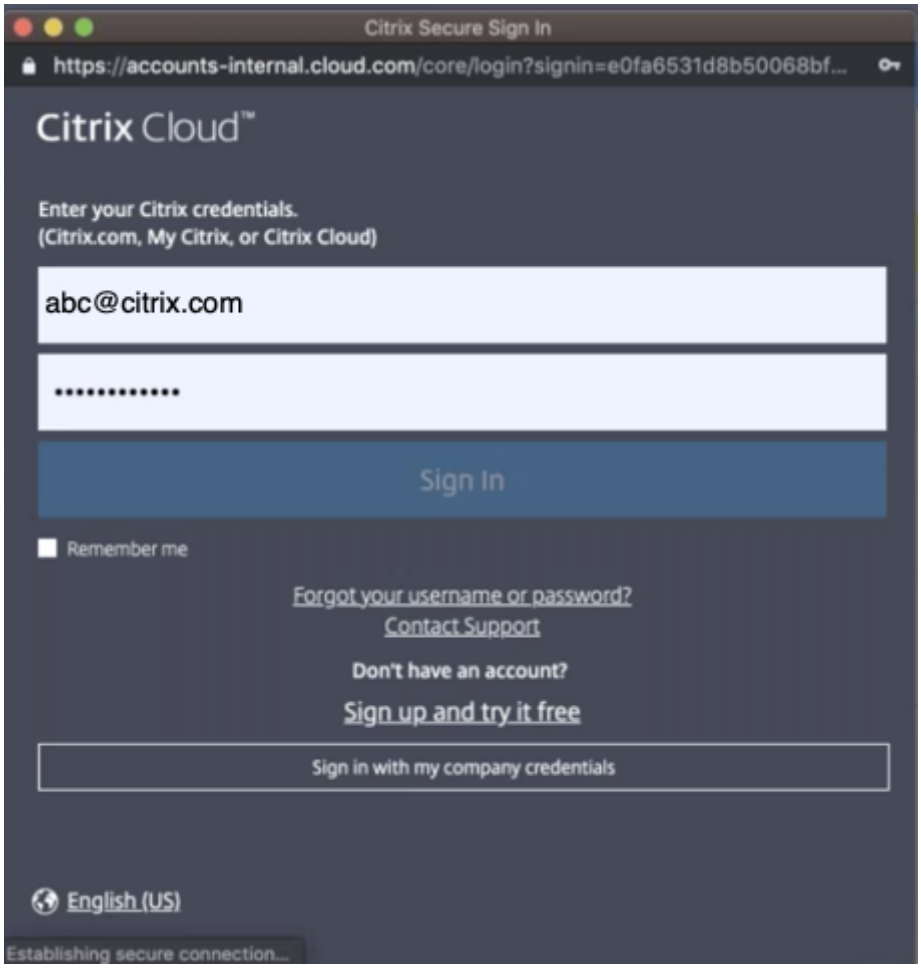
Configure cloud direct service in SD-WAN Center

1. In the SD-WAN Center GUI, navigate to **Configuration** > **Cloud Connectivity** > **Cloud Direct**.

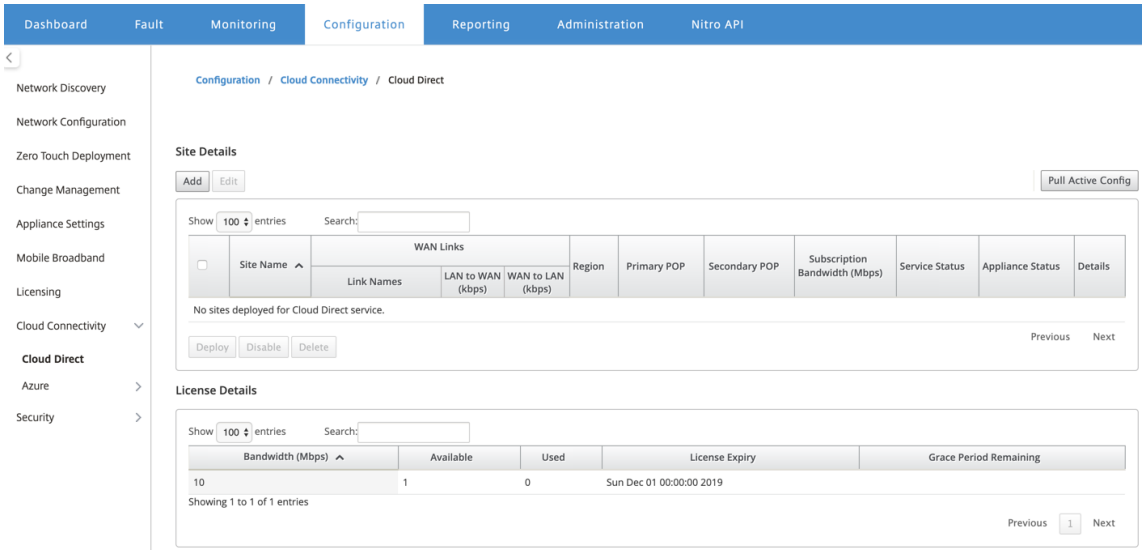


2. Log in with Citrix Cloud credentials.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

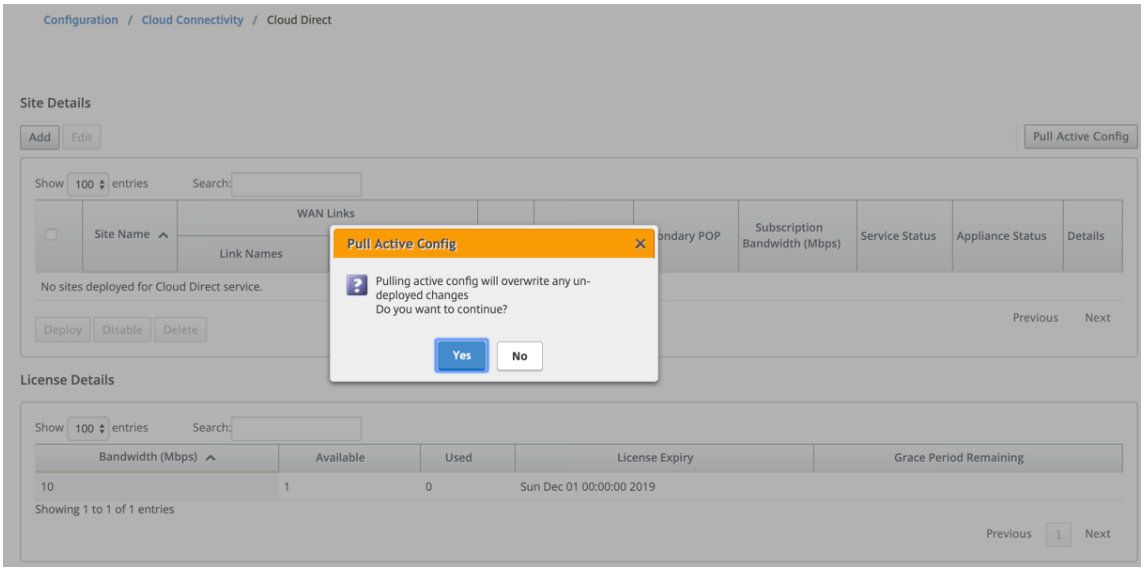


The Cloud Direct home page appears after you successfully logged into the Citrix Cloud Service.



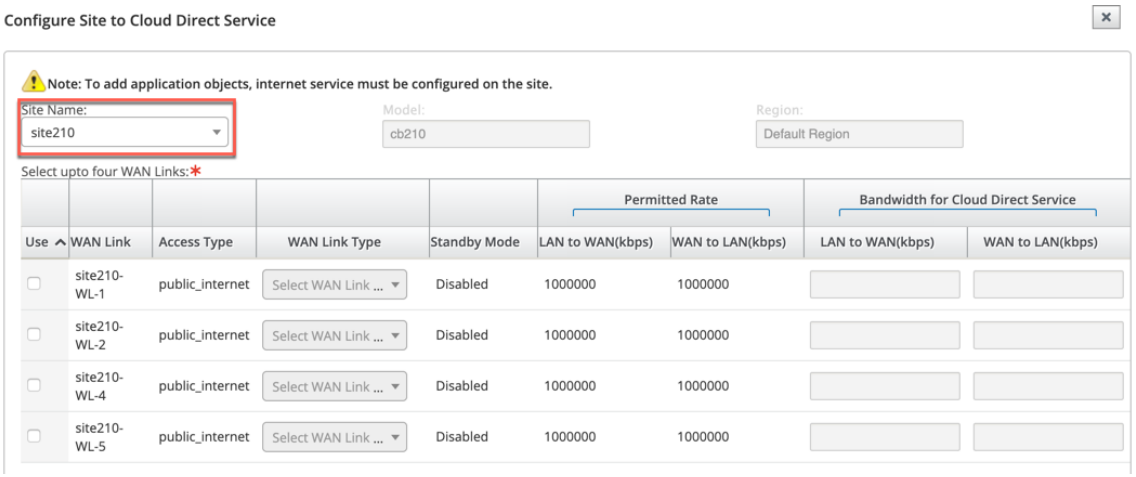
3. Click **Pull Active Config** to retrieve latest active MCN configuration.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



4. Click **Add a new site**. Sites that are eligible for the Cloud Direct service deployment are displayed in the menu.

> **Note**
>
> - The Cloud Direct service feature is supported on 210, 410, and 1100 hardware appliances.
> - From 11.2 release onwards, the Cloud Direct service is supported on SD-WAN 2100, 4100, and 6100 appliances. Both SD-WAN Center and Orchestrator allow the Cloud Direct service feature to be deployed on SD-WAN 2100, 4100, and 6100 appliances. SD-WAN Center supports up to 250 Mbps subscription licenses for Cloud Direct.

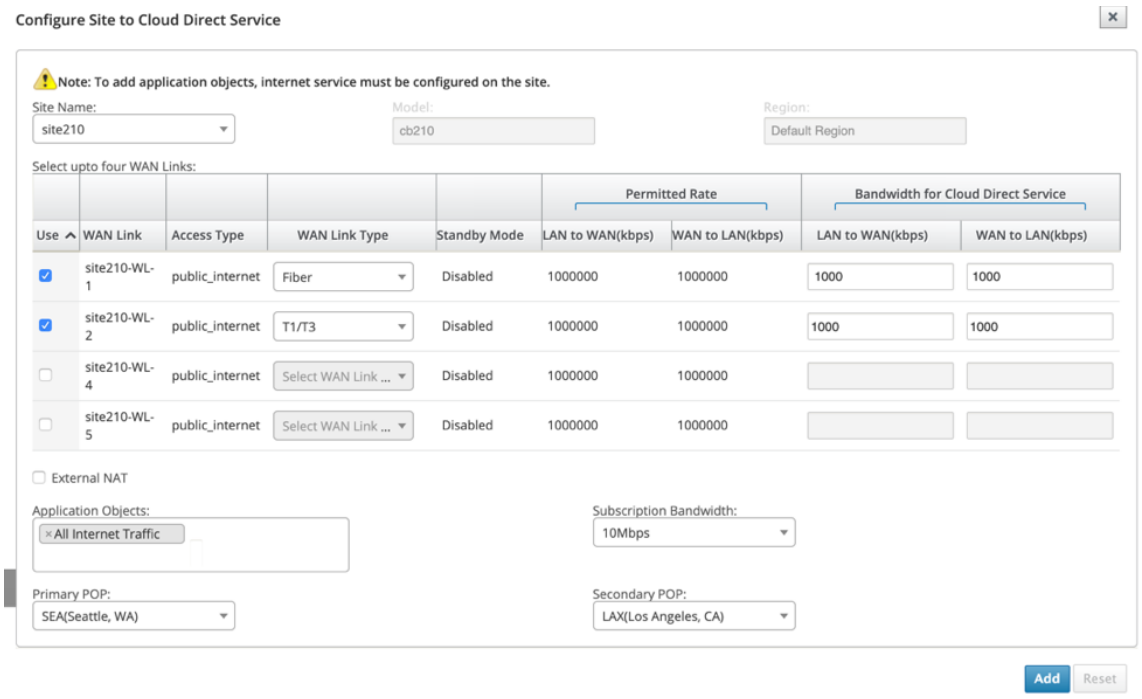


5. When a site is chosen, the public internet WAN links that are associated with the selected site are displayed, along with the appliance model information and the region in which the appliance is deployed.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

6. Select the WAN links that you would like to use for Cloud Direct service traffic, along with the **WAN Link Type**, **Application Objects**, **Subscription Bandwidth**, **Primary POP**, and **Secondary POP** options.

> **Note**
>
> - Up to four WAN links are supported for Cloud Direct service.
> - A WAN link bandwidth is no longer needed to be reserved exclusively for the Cloud Direct service. If the Cloud Direct service is not active then the other services such as virtual path, internet, or intranet services configured on that WAN link can use the bandwidth as per the configured shares.



- **Site Name**: Displays the sites that are eligible for the Cloud Direct feature deployment.
- **Model**: For the selected site, corresponding appliance model name is auto populated.
- **Region**: For the selected site, the appliance specific deployed region details are auto populated.
- **WAN Link**: For the selected site, the associated public internet WAN links are displayed.
- **WAN Link Type**: Select the WAN link type from the menu.
- **Standby Mode**: The standby mode is retrieved from the WAN link configuration.
- **Bandwidth for Cloud Direct Service**: Enter the bandwidth that the Cloud Direct Service can use exclusively. The selected bandwidth must be lesser than the configured permitted

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

bandwidth and would not be available for use by the Virtual Path, Internet, and Intranet services.

- **External NAT**: It is required that the public internet traffic originated from the branch LAN network is source NAT from a specific IP address. By default, this is automatically performed and taken care as part of the SD-WAN network configuration. If you would like to configure the NAT IP (LAN Network) outside the SD-WAN device (for example, in an external firewall), you can choose the External NAT option when deploying sites. The IP to which the LAN traffic has to be the source NAT is available in the **Details** page of the deployed Cloud Direct site.
- **Application objects**: You can choose specific application objects or select "All Internet Traffic"to be redirected through the Cloud Direct service. In case when the specific application objects are selected, the traffic for those applications is sent through the Cloud Direct service, and the rest of the traffic is steered using the internet service configured on the appliance.
- **Subscription bandwidth**: Subscription bandwidth is associated with the licensing for the cloud direct service.
- **Billing Mode**: When a customer plans to deploy a Cloud Direct site as part of validating proof of concept (POC), the **Billing Mode** field must set as **Demo**. For all other cases, set the billing mode as **Production**.

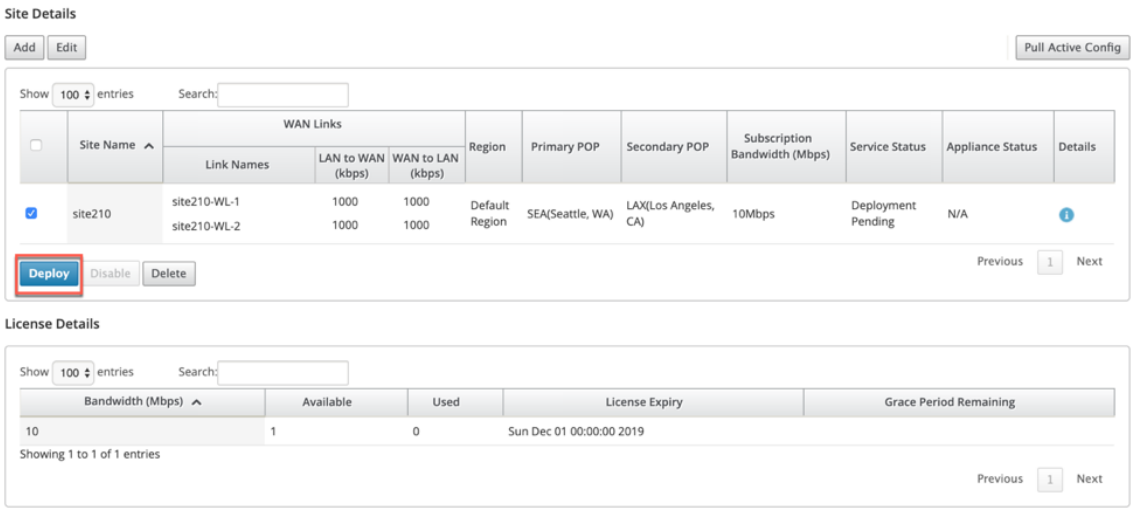
> **NOTE:** The following situation occurs, if the **Billing Mode** is selected as **Demo** or **Production**:
>
> - If a Cloud Direct site is created with **Billing Mode** as **Demo**, the settings can be edited to Production.
> - If a Cloud Direct site is created with **Billing Mode** as **Production**, the setting cannot be edited to **Demo**.

The **Billing Mode** option enables the use of Cloud Direct trial/evaluation licenses, which can be provided by Citrix sales or authorized partners. Sites operating with Cloud Direct evaluation licenses must be set to the **Demo Billing Mode** option. Sites upgrading to full Cloud Direct subscription licenses must be set to the **Production Billing Mode** option.

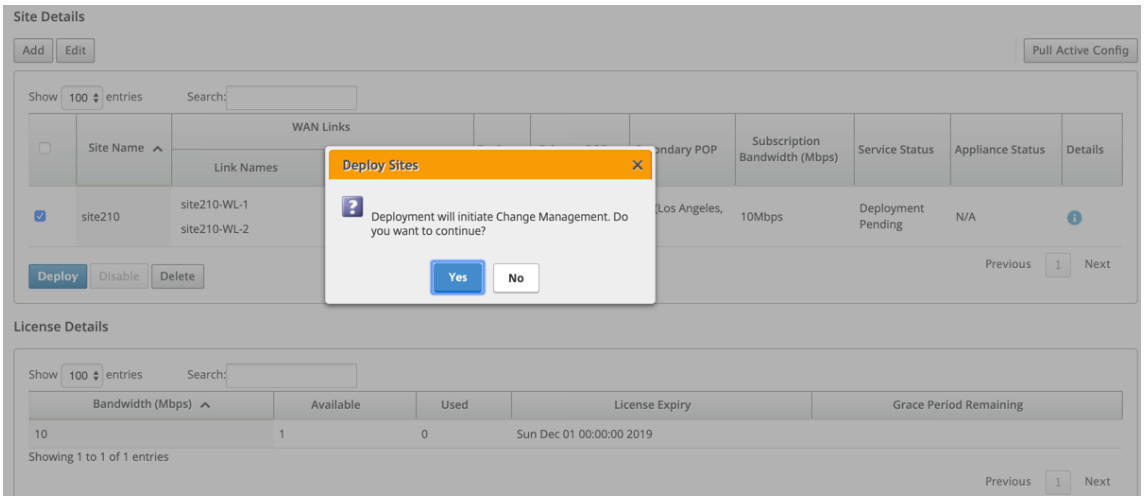
- **Primary/Secondary POP**: Ensure that the primary and secondary POP is not the same. Select the POPs depending on the location proximity. Click **Add**.

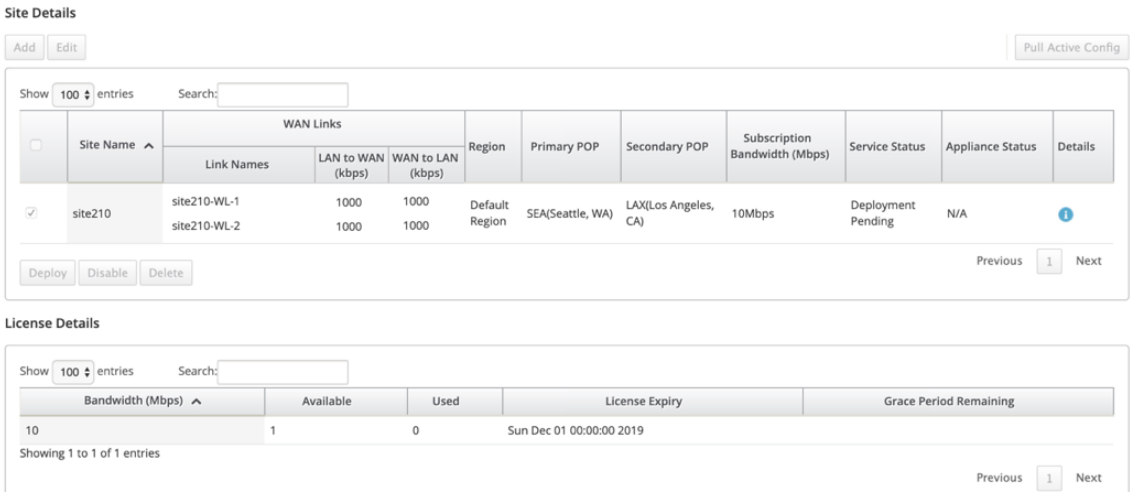
7. After the sites are added, the service status is shown as **Deployment is Pending**. Select the site for which you want to deploy Cloud Direct service and click **Deploy**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

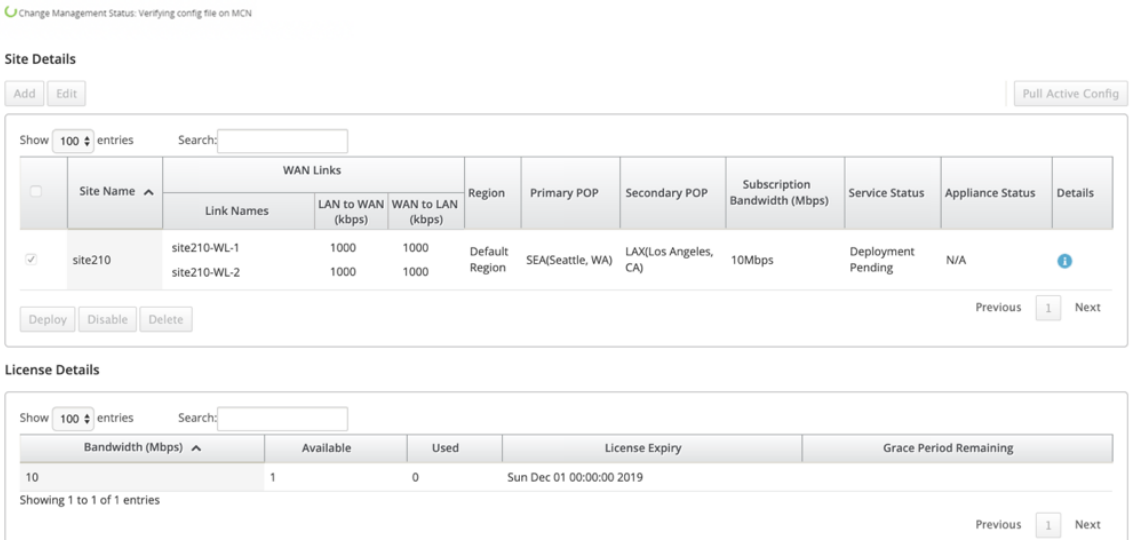


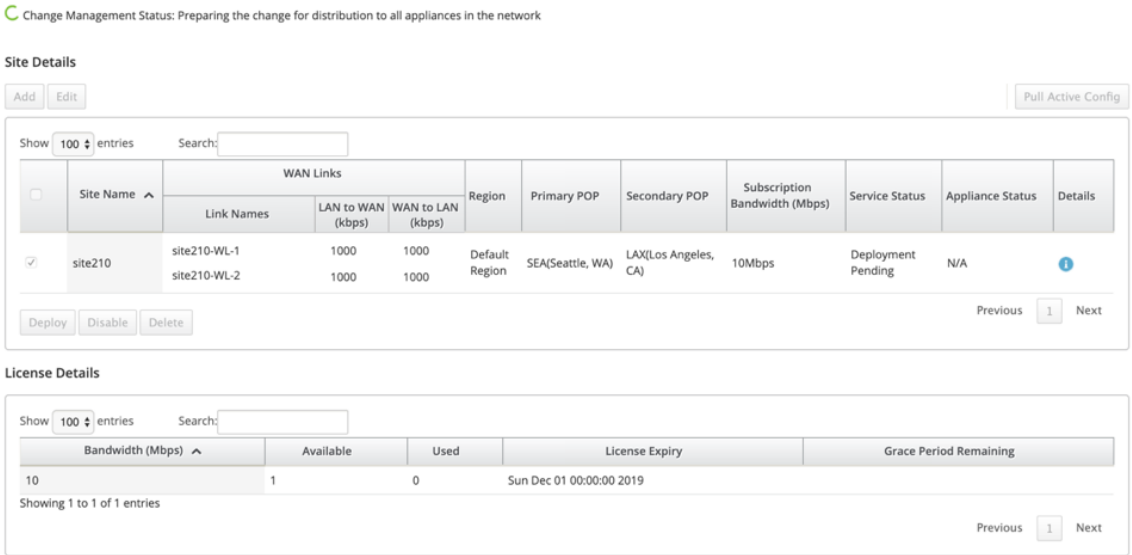
A notification stating that the deploy operation initiates a change management on the MCN appliance is displayed. You can click **Yes** or **No**.

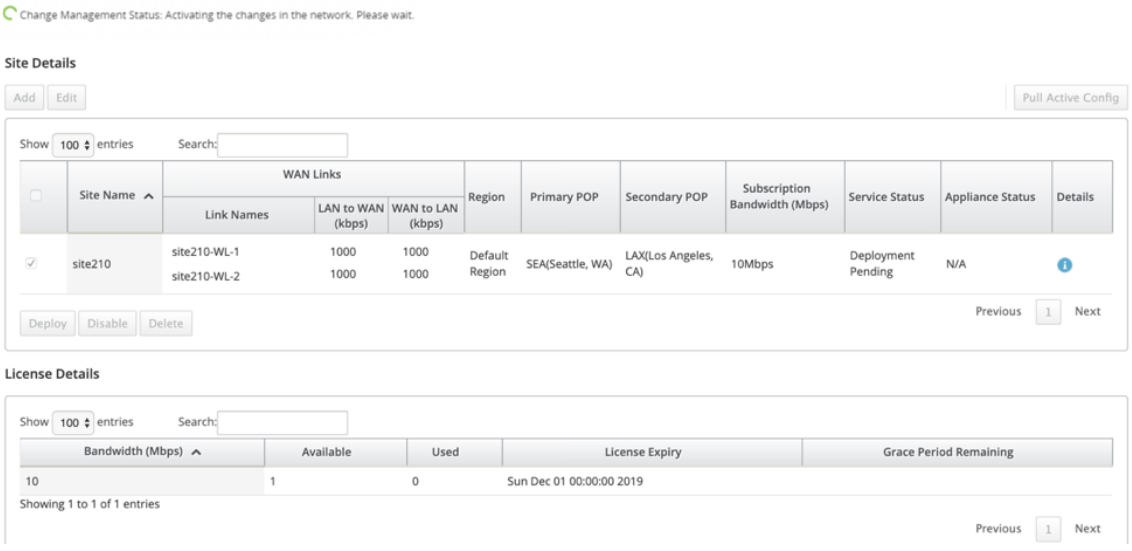




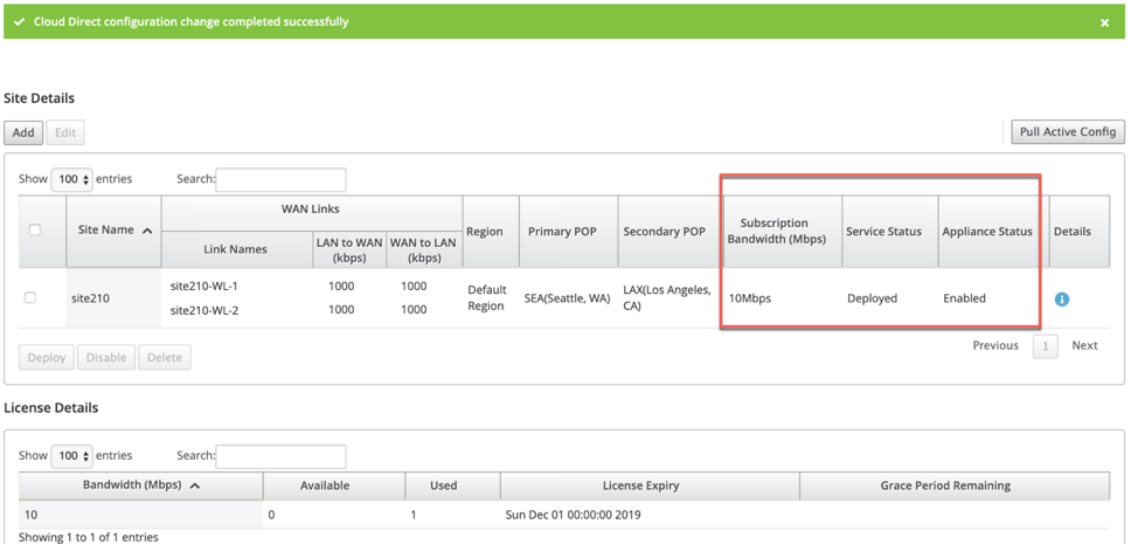
© 1999–2025 Cloud Software Group, Inc. All rights reserved.







© 1999–2025 Cloud Software Group, Inc. All rights reserved.

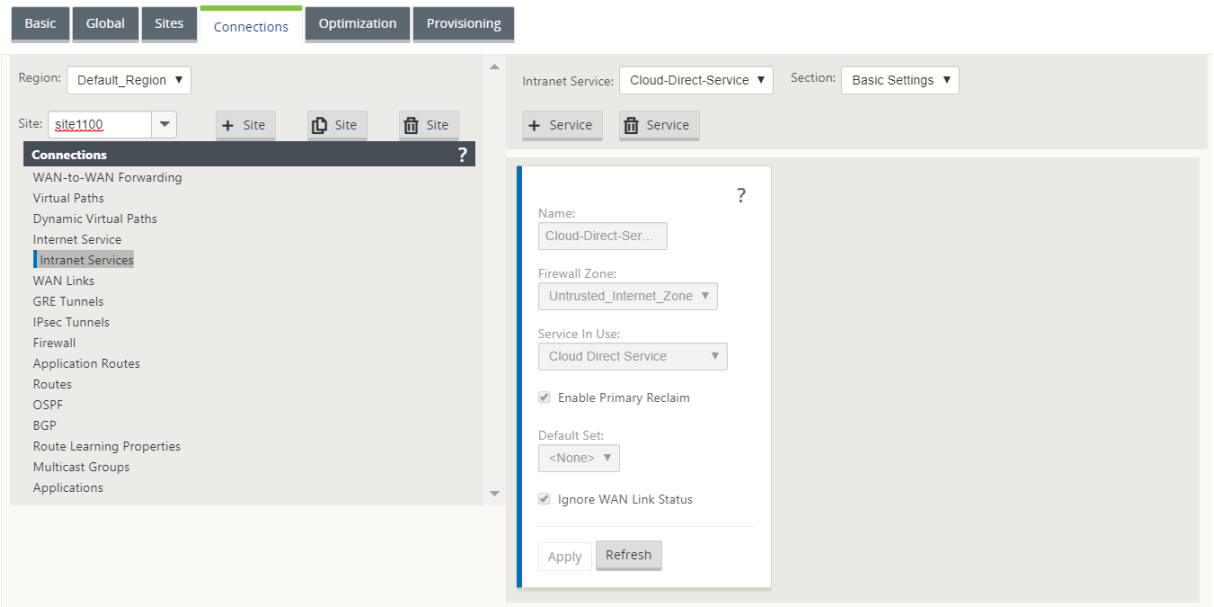


After successfully deploying the sites, the cloud direct service page displays the following:

- **Service status**: Deployed
- **Appliance status**: Enabled
- **Subscription Bandwidth (Mbps)**: 10 Mbps
- **Consumed the installed license**

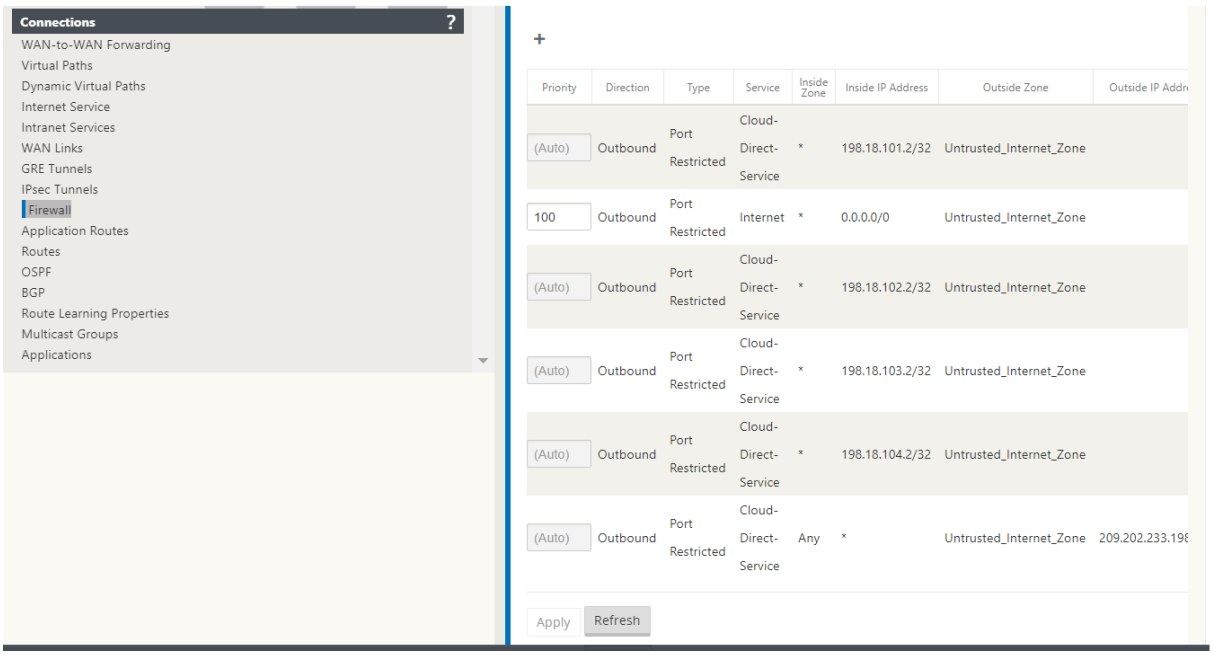
The above change management step auto generate and add the needed Cloud Direct service configurations to the running configuration.

> **Note**
>
> The auto-created **Cloud Direct Service** (intranet service) is associated with the Default_RoutingDomain.

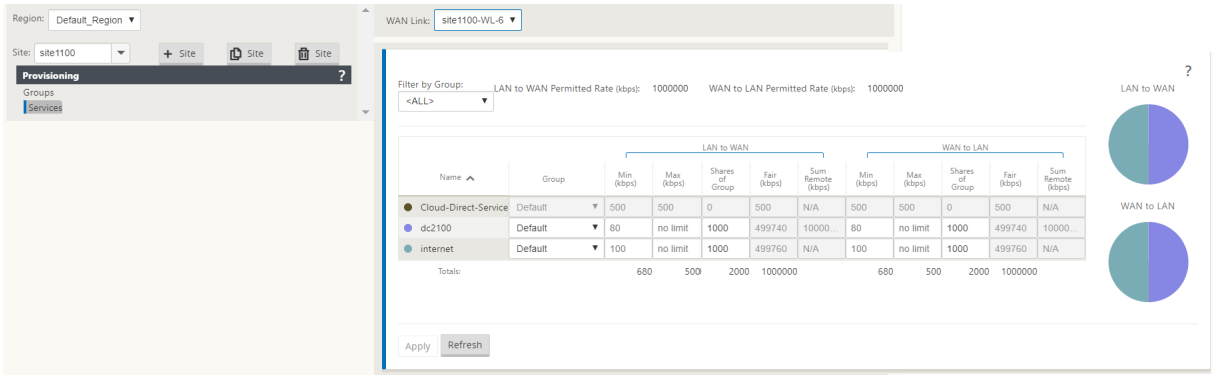


© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Firewall Settings



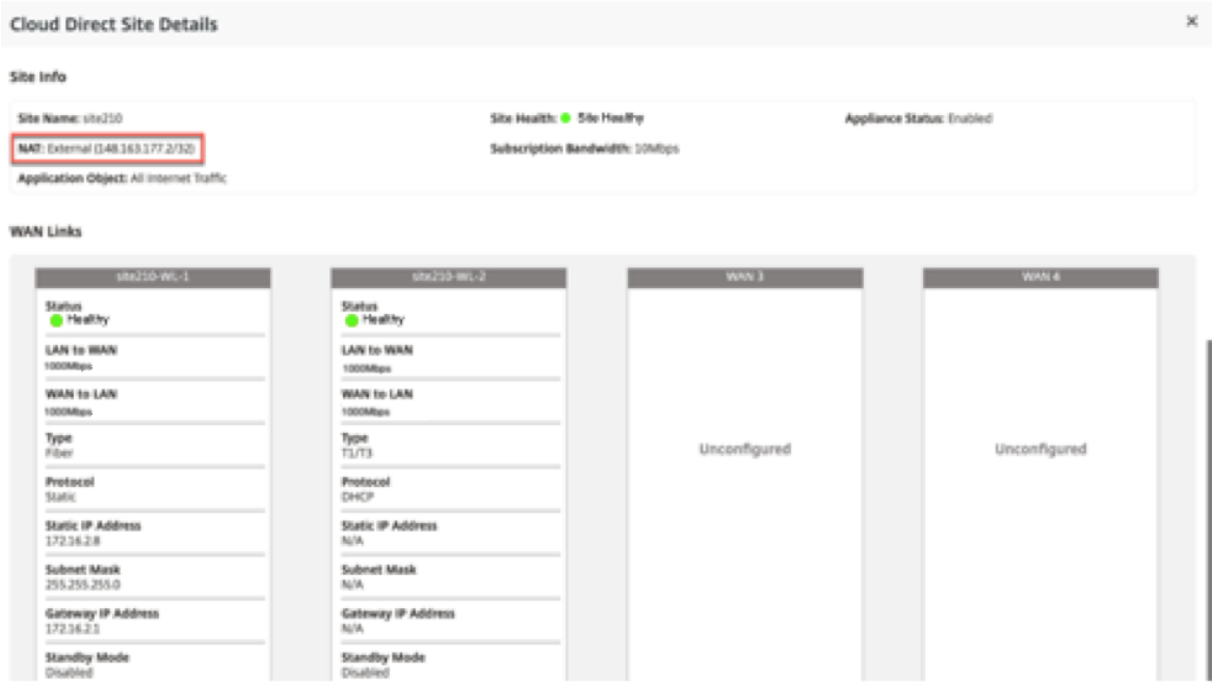
Provisioning Sites in SD-WAN application GUI



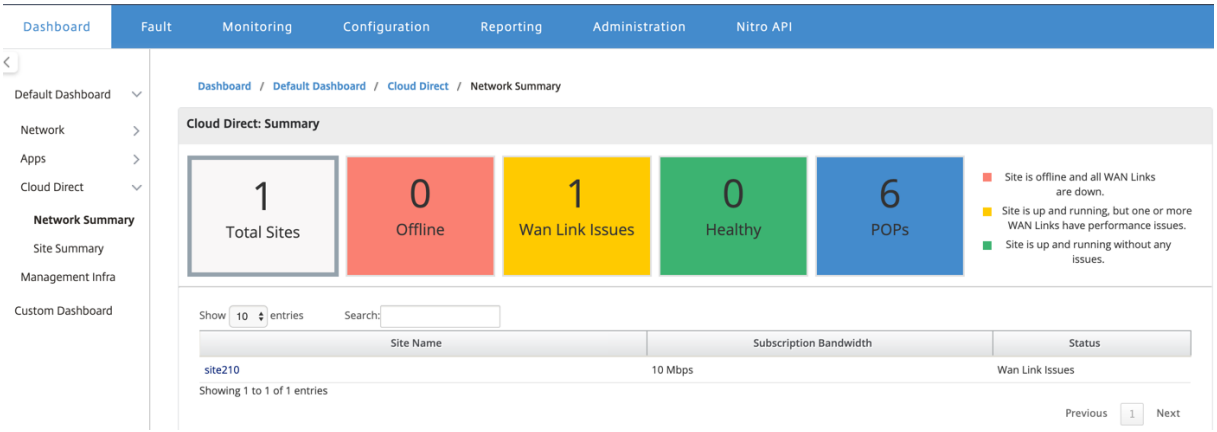
Monitoring Cloud Direct service

You can view the configured Cloud Direct service after the sites are deployed and enabled. Click the exclamation icon in the **Details** column to view the site details.

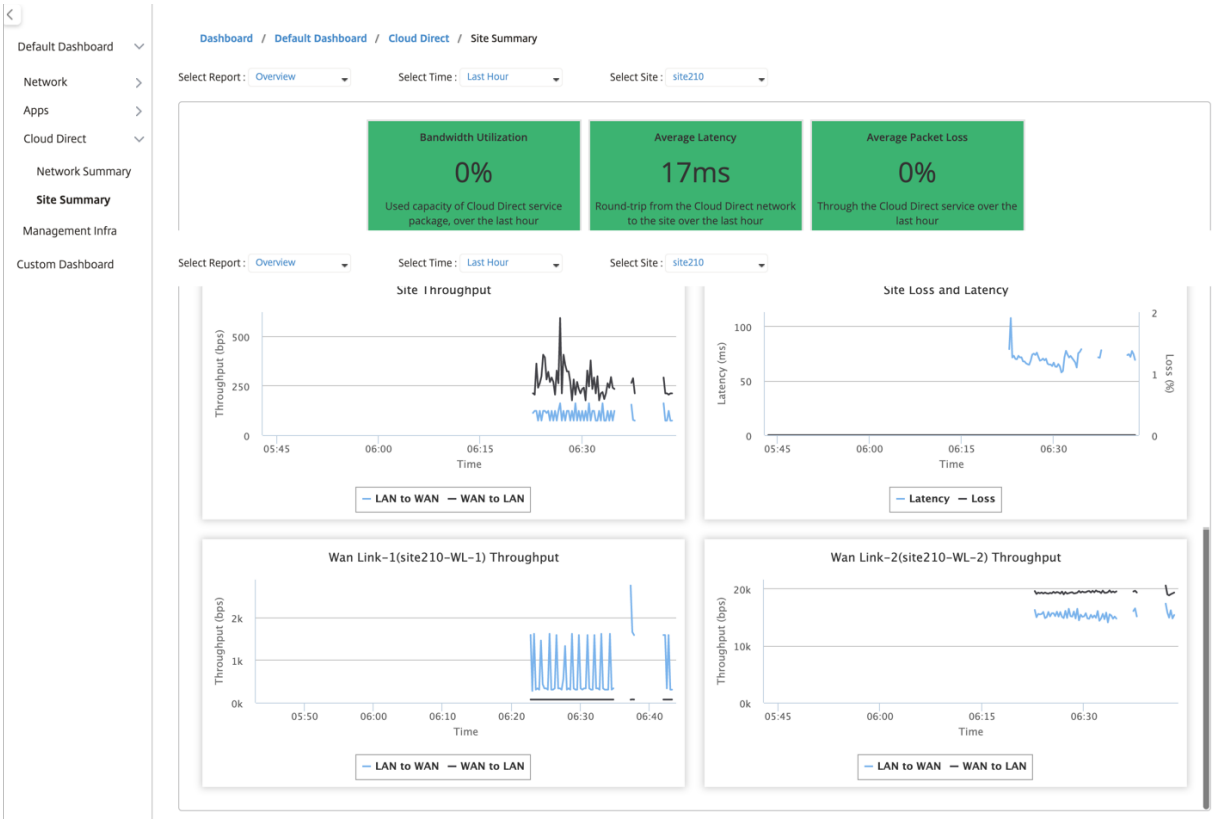
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



You can view the site summary graphs by navigating to **Dashboard** > **Cloud Direct** > **Network Summary** and **Site Summary**.



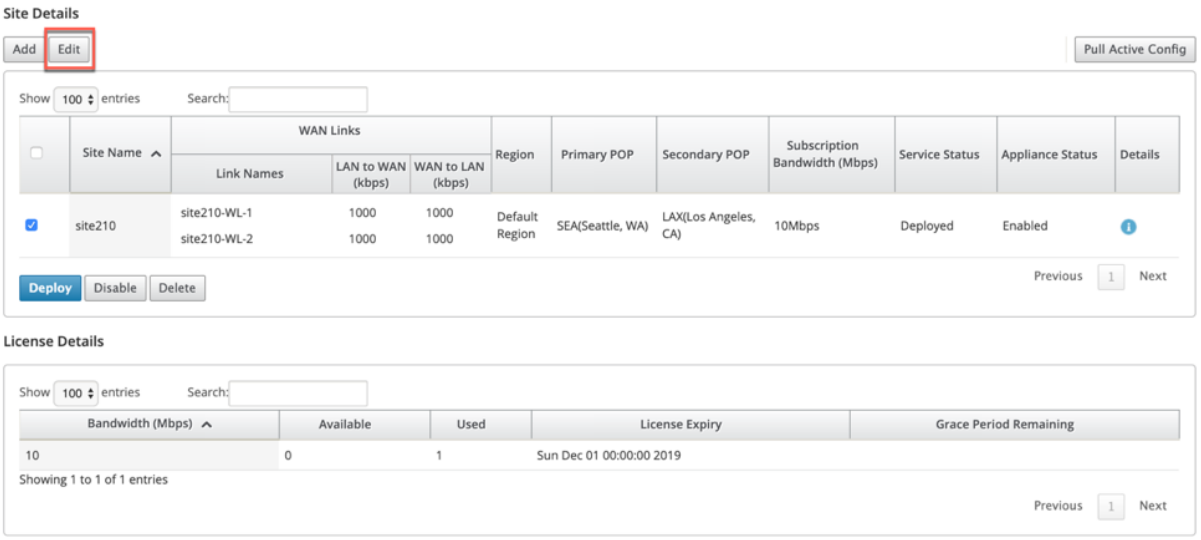
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



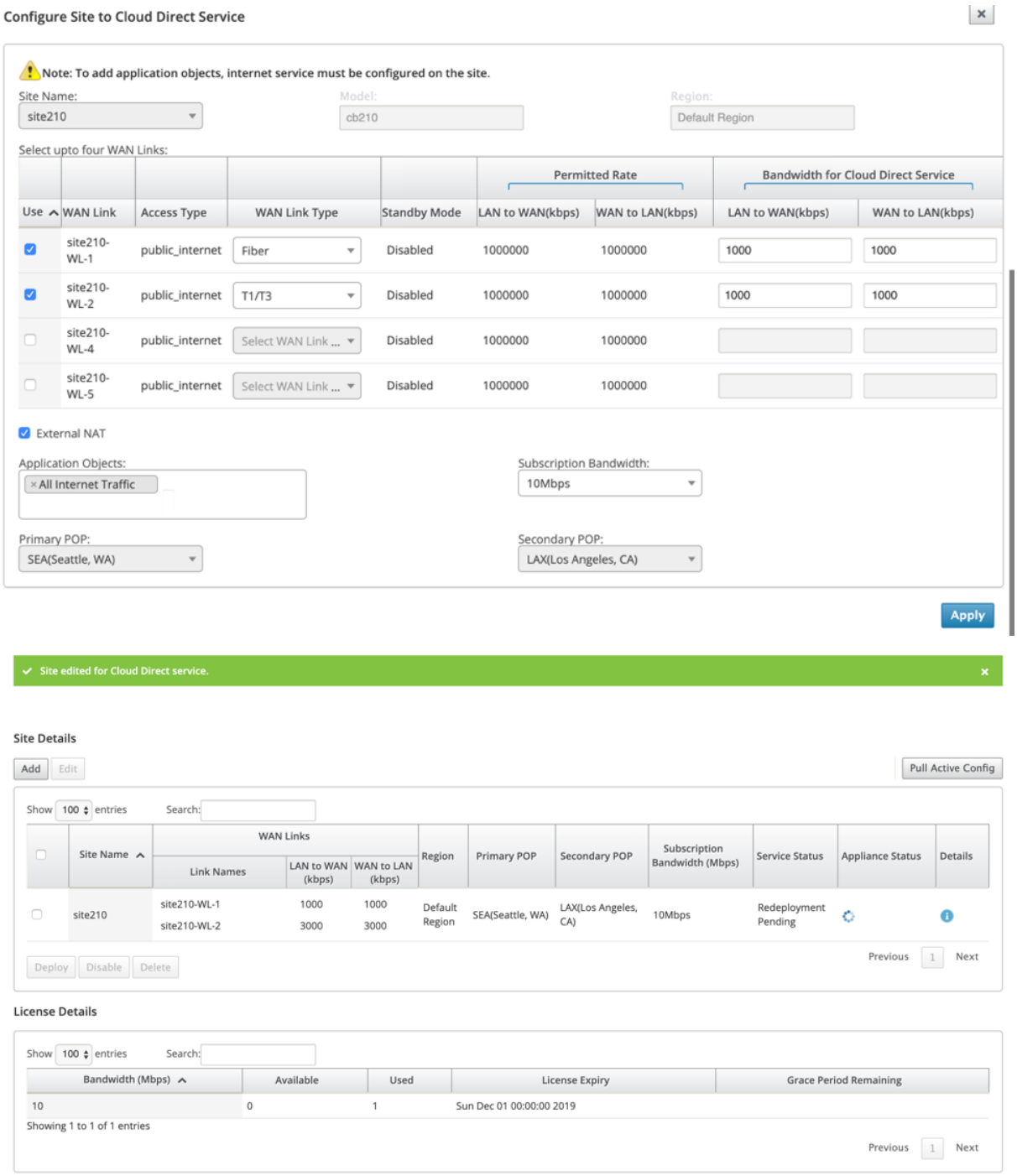
Editing site in SD-WAN Center

You can choose to edit the sites to modify bandwidth and wan link type.

> **Note**
>
> POP selections cannot be edited.

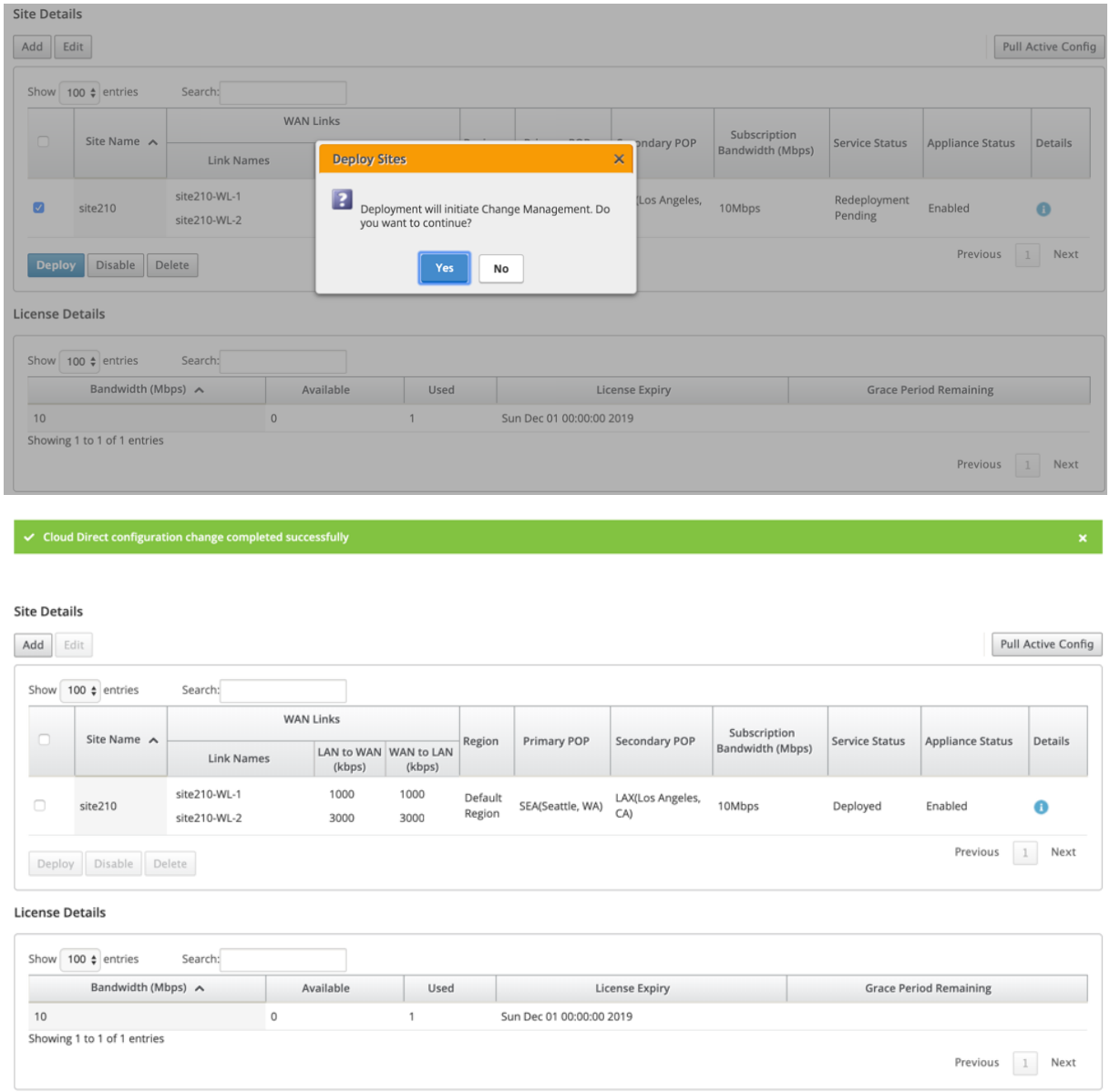


© 1999–2025 Cloud Software Group, Inc. All rights reserved.



The service status displays as redeployment pending. Deploy the site. The deployment process is completed for the edited site.

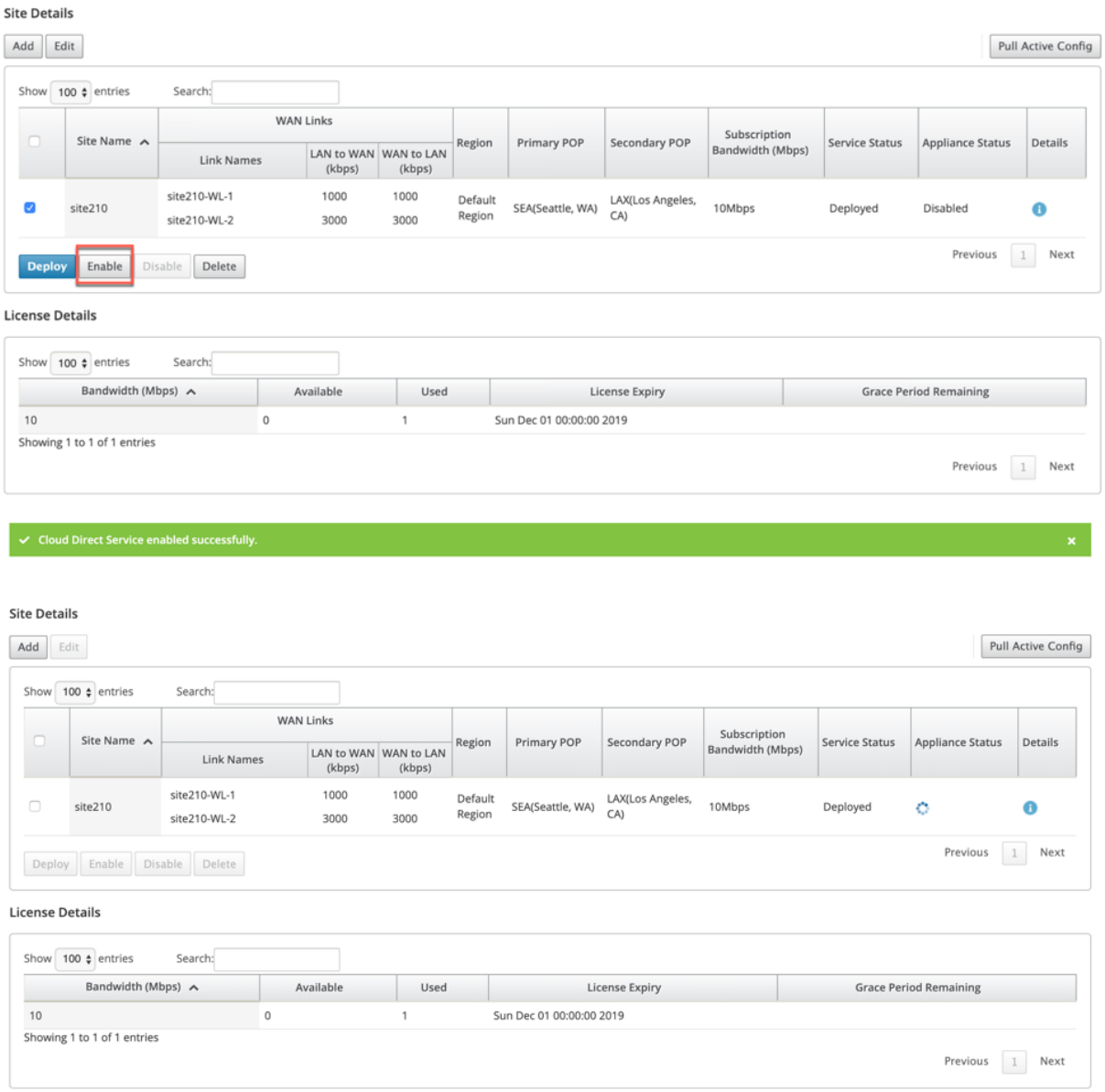
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Enable and Disable Site

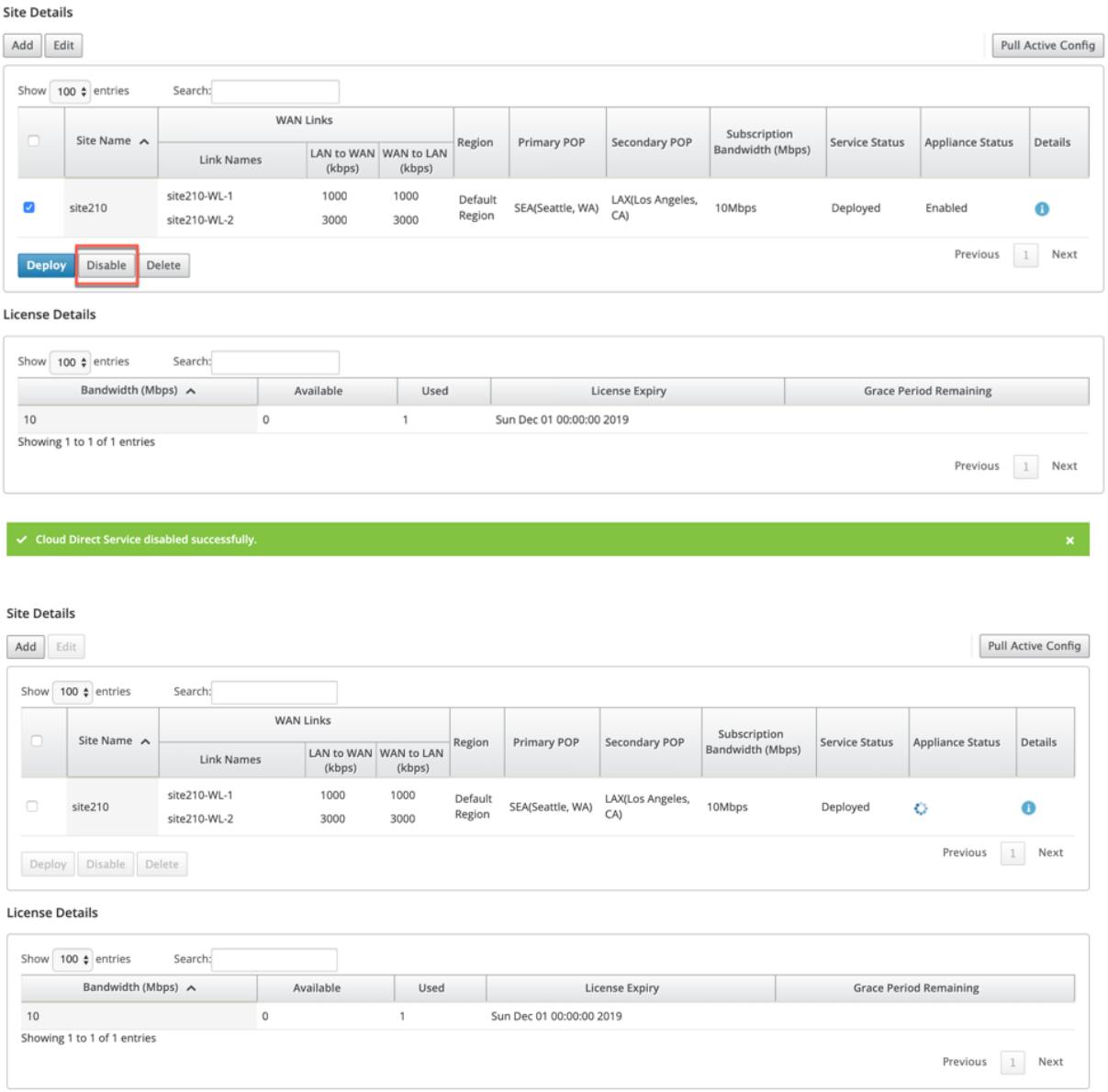
You can enable a deployed site that has an appliance status shown as disabled. To enable a site, click **Enable**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Click **Disable** to disable a deployed site. Disabling site would no longer use cloud direct service to steer the internet traffic. All traffic is redirected through the internet service, if configured on the appliance.

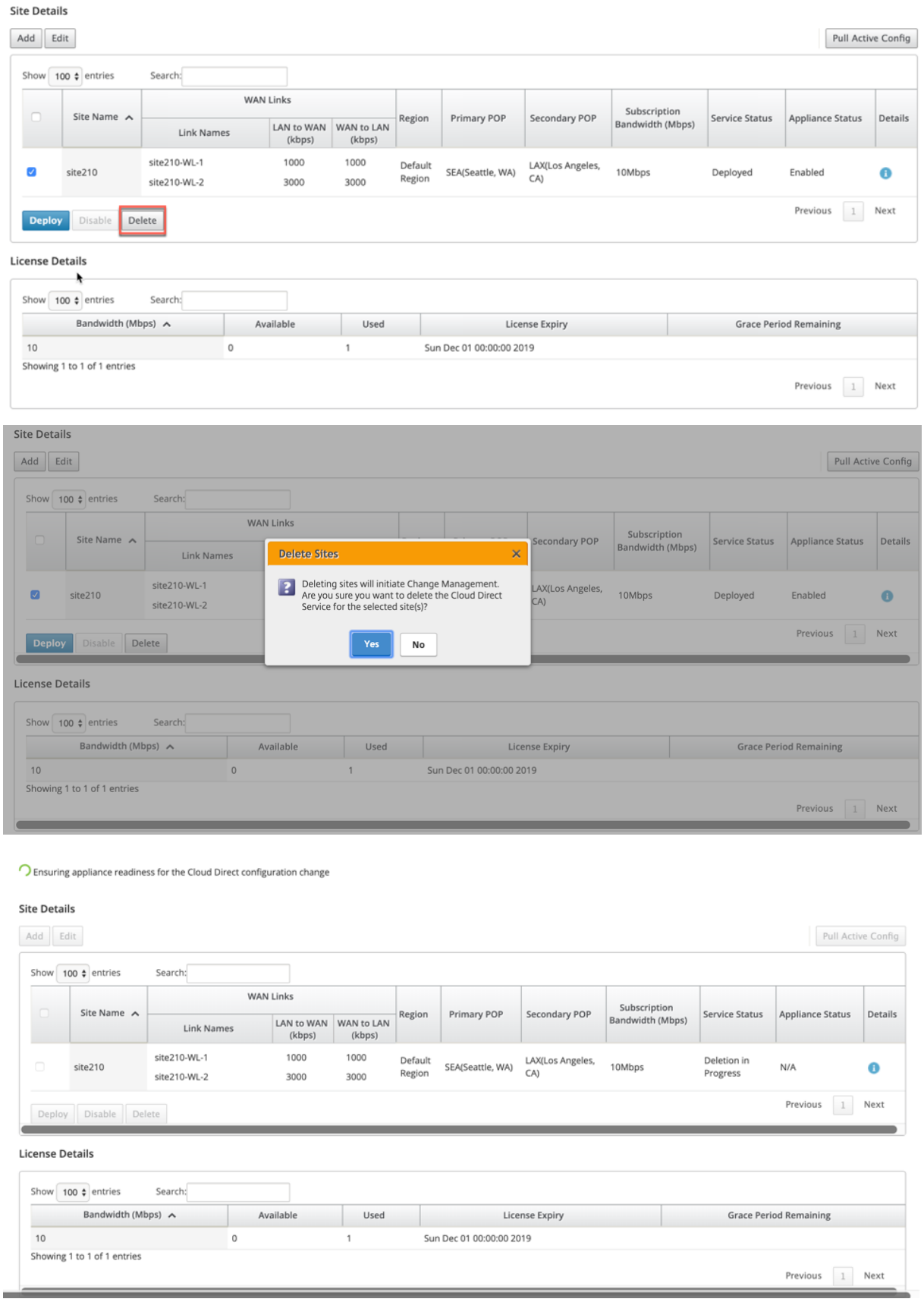
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



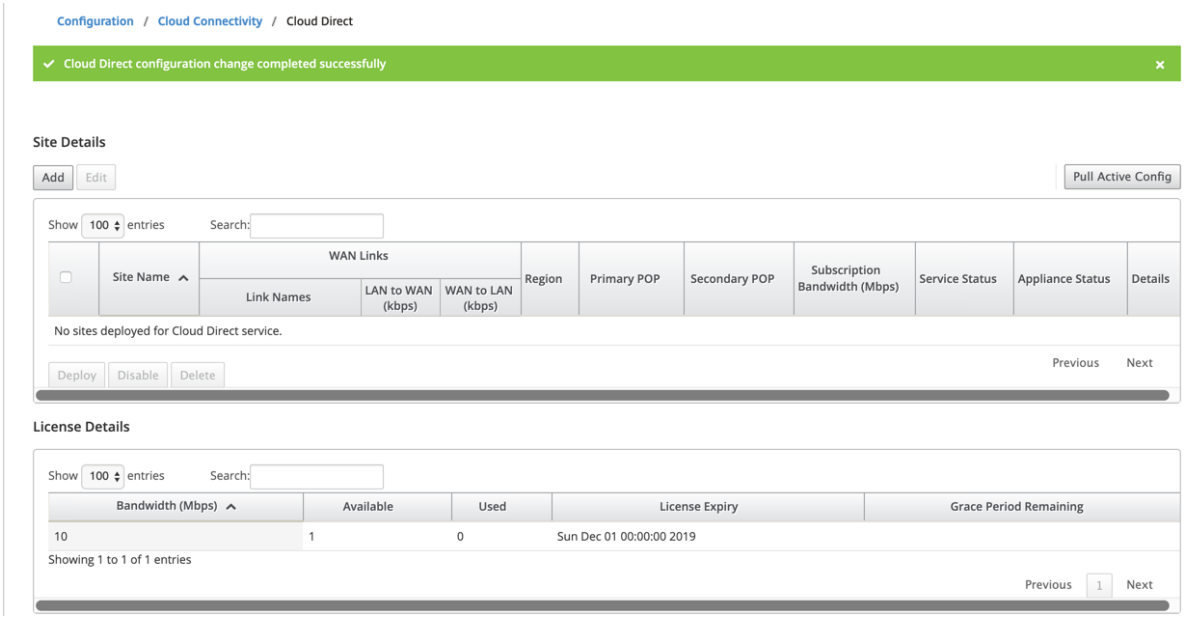
Site Deletion

You can choose to delete the sites that no longer require Cloud Direct connectivity. To delete sites, select the site and click **Delete**. A confirmation message to delete sites is displayed.
All cloud direct service configuration is removed through the change management process.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



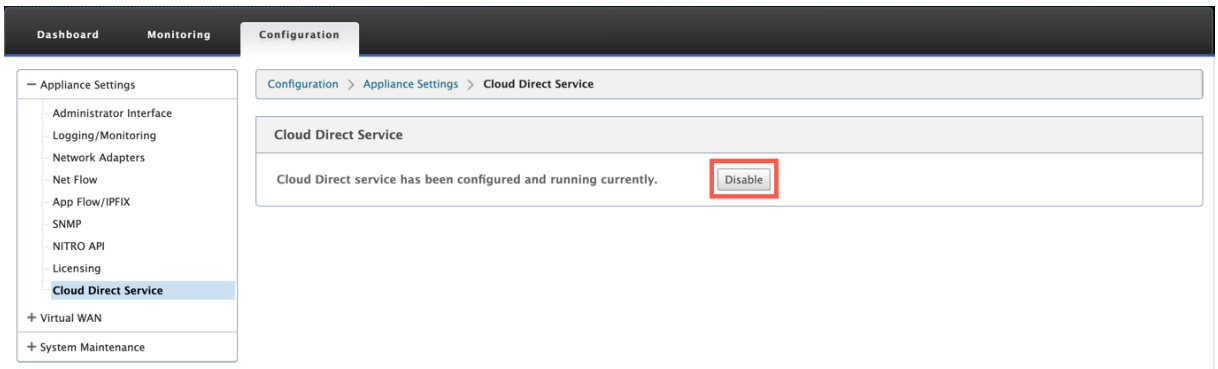
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



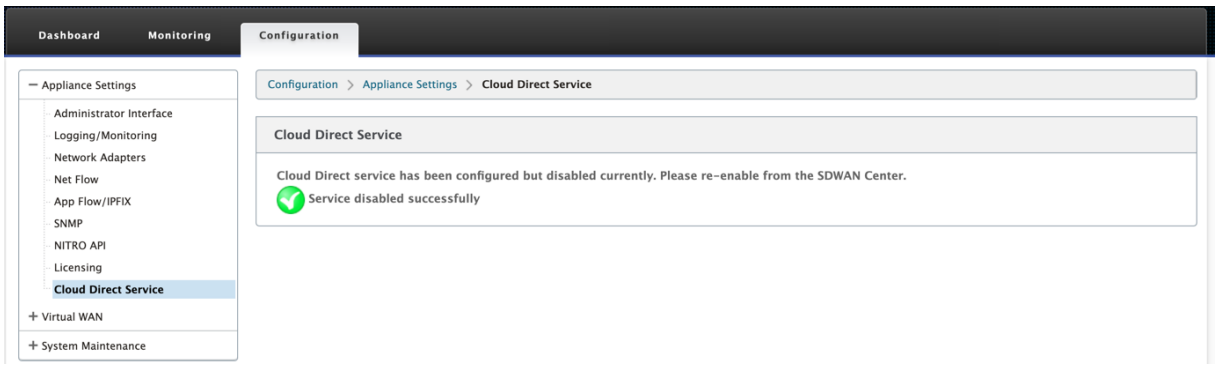
Cloud Direct Service status on Citrix SD-WAN

You can verify the Cloud Direct service status on a local SD-WAN appliance.

Go to the Citrix SD-WAN GUI, navigate to **Configuration** > expand the **Appliance Settings** > select **Cloud Direct Service**.



Click **Disable** option to disable the Cloud Direct service.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Troubleshooting

The most common error messages that might occur on SD-WAN Center when deploying Cloud Direct service are as follows.

Error/status messages are displayed on SDW-AN Center under **Configuration** > **Cloud Connectivity** > **Cloud Direct**.

'Cloud Direct License error! Please upload additional license for {bandwidth} Mbps bandwidth'

- Upload a valid Cloud Direct license on SD-WAN Center by navigating to **Configuration** > **Licensing** > **File Management** option and then proceed with deploying this feature

'Cloud Direct configuration HA due to Citrix Cloud Workspace login issue'

- Reenter credentials for Citrix Cloud Workspace login on SD-WAN Center by navigating to **Configuration** > **Cloud Connectivity** option.

'Cloud Direct configuration processing error! Site: {site_name}(IP: {mgmt_ip}) is not reachable or is missing Cloud Direct support'

- Check if SD-WAN appliance or appliances (in case of HA deployment) are reachable on the management port.

'Cloud Direct configuration HA Config Check error for site: {site_name}'

- Check for connectivity of both appliances in HA pair corresponding to site being deployed.

'Both the HA Pair Appliances have to be reachable to perform Cloud Direct Configuration'

- When deploying Cloud Direct service on SD-WAN appliances in HA pair, both secondary and primary appliances must be reachable on the management port.

'Cloud Direct configuration processing error! Site: {site_name}(IP: {mgmt_ip}) has SSO Login Issue'

- Check if SD-WAN appliance is up/running and reachable on the management port. This error is displayed when SD-WAN Center is unable to perform single sign-on to the SD-WAN appliance.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

'Internal error encountered during Cloud Direct configuration processing'

- This might occur due to multiple error conditions while carrying out configuration check or rest of the processing. A user might need to review the logs and perform the operation again.

'Cloud Direct configuration processing canceled! MCN is not ready for change management'

- Check if MCN is accessible and up and running and that its change management state is "network_staging."

'Cloud Direct configuration processing error! Site: {site_name}(IP: {mgmt_ip}) does not have Cloud Direct support. Please do single step upgrade to have a Cloud Direct support'

- Perform single step software upgrade on the SD-WAN appliance through **MCN** > **Change Management**. After this procedure, reattempt deploying Cloud Direct service for this site.

'Cloud Direct configuration processing error! SD WAN change management operation failed'

- Change management operation somehow did not succeed. Check SD-WAN Center logs for details.

'Cloud Direct configuration processing error! Enabling service at site: {site_name} failed'

- Unable to enable Cloud Direct service on SD-WAN appliance. Check for connectivity of specific appliance or for those in HA pair or for any issue when performing single sign-on. Check logs on SD-WAN Center and appliance for details.

'Cloud Direct configuration processing error! Disabling service at site: {site_name} failed'

- Unable to disable Cloud Direct service on SD-WAN appliance. Check for connectivity of specific appliance or those in HA pair or for any issue when performing single sign-on. Check logs on SD-WAN Center and appliance for details.

'Cloud Direct configuration processing error! Config image push to site: {site_name} failed'

- Unable to upload service-specific image on appliance via REST api or not able to access both appliances in HA pair.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

'Cloud Direct Service encountered an error during configuration processing. Audit errors found in the SD WAN config!'

- Audit errors found when attempting to compile the SD-WAN config. Check SD-WAN Center logs for details.

'Cloud Direct configuration processing error! Create Site failed for Site: {site_name}'

- Service-side error when attempting to create a site for the corresponding SD-WAN appliance. Review SD-WAN Center logs for additional details.

'Cloud Direct configuration processing error! Update Site failed for Site: {site_name}'

- Service-side error when attempting to modify site related settings for the corresponding SD-WAN appliance. Review SD-WAN Center logs for additional details.

Error messages seen in logs (SDWAN_common.log)

Here are few scenarios where Cloud Direct service is deployed on SD-WAN appliance, but might not function as expected. You can download and review the logs on the local SD-WAN appliance using the SDWAN_common.log for more details.

Scenario 1

"Detected Cloud Direct VM is not responding …Disabling Cloud Direct Service now!""Cloud Direct service has been disabled." Underlying KVM running on local SD-WAN appliance is not functioning in expected manner. In such case, Cloud Direct service functionality is disabled on the appliance.

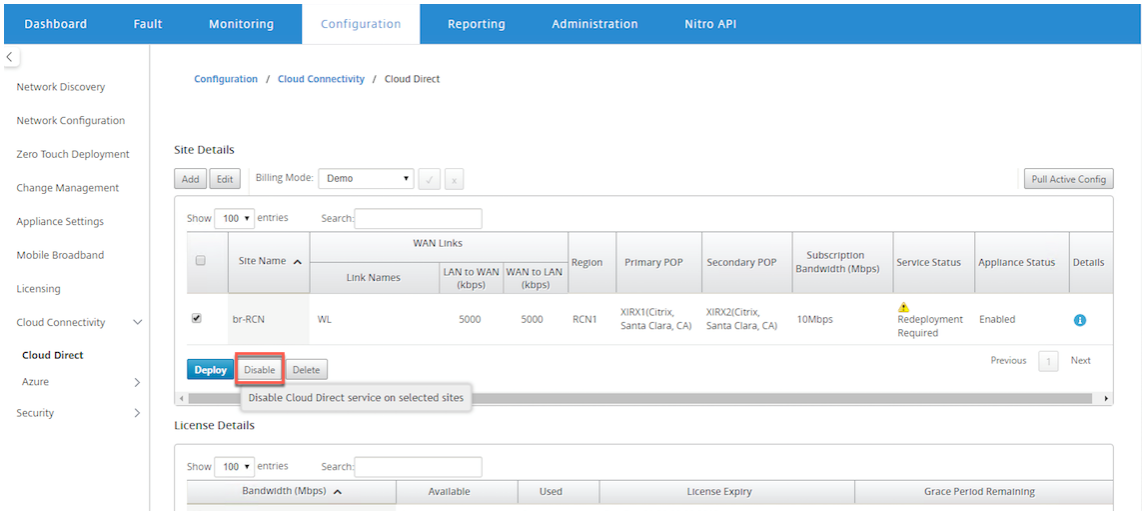
Scenario 2

"No tunneled packets seen for past 5 mins …Disabling Cloud Direct Service now!""Cloud Direct service has been disabled." There is no tunnel established between SD-WAN appliance and tunnel endpoint in-use for Cloud Direct service. This might be due to misconfiguration of wan-link, lack of internet connectivity over configured wan-link, incompatible or invalid data/config image pushed to appliance or any firewall rule that might be dropping UDP tunnel packets when received over wan-link. In such case, Cloud Direct service functionality is disabled on the appliance.

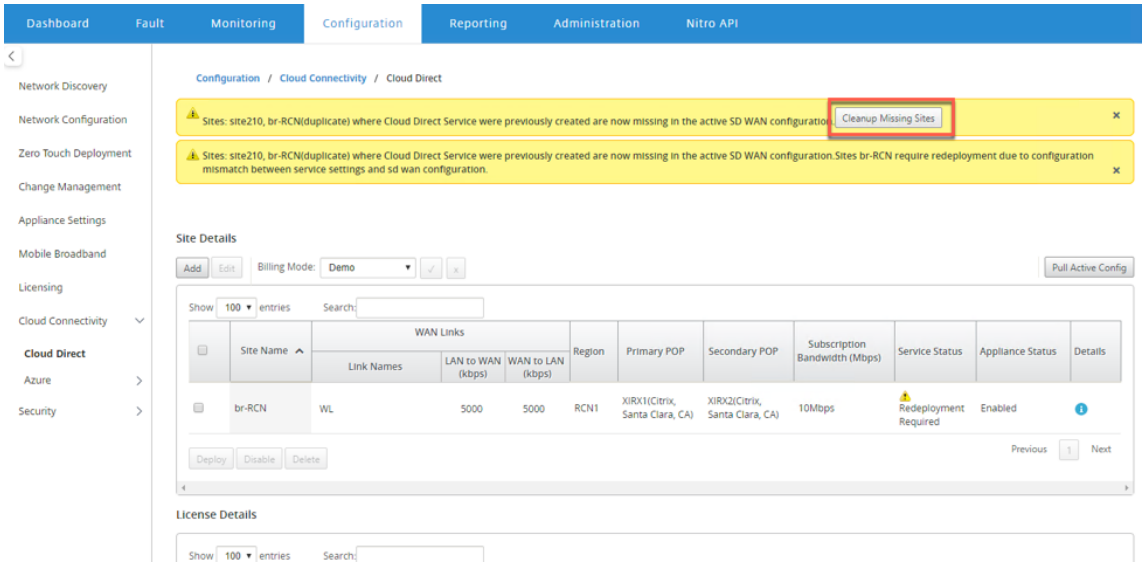
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

When you activate a configuration on MCN with different Cloud Direct configuration (For example: NAT configuration is changed for Cloud Direct) and it might lead to the permanent interruption of traffic. To overcome this block, you can follow either one of the following steps to select the different routes present on the appliance:

1. In the SD-WAN Center GUI, navigate to **Configuration** > **Cloud Connectivity** > **Cloud Direct**. Select the cloud direct appliance and click **Disable** option to disable the cloud direct service.



2. Navigate to **Configuration** > **Cloud Connectivity** > **Cloud Direct** and pull active config to get the clean-up notification. You can click the **Cleanup Missing Sites** notification button shown for the affected cloud direct appliance. This operation disables Cloud Direct service running on the appliance.



3. Redeploy the Cloud Direct service on SD-WAN Center to use the Cloud Direct service for affected appliances.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Integrate Citrix SD-WAN and Zscaler using Citrix SD-WAN Center

March 12, 2021

Citrix SD-WAN and Zscaler help enterprises transform their WAN for cloud migration by providing secure local breakouts to applications and resources hosted on the Internet. New WAN infrastructure technologies such as SD-WAN increase network agility and scale while lowering cost and complexity for an improved user experience in distributed organizations.

SD-WAN solutions simplify routing by allowing traffic destined for the cloud to breakout to the Internet locally. SD-WAN provides flexibility for routing traffic to the Internet (remove central DC environment) by using application steering features. However, exposing the network to the Internet poses significant security risks. A centralized approach to securing local breakout through a cloud service eliminates the overhead of maintaining security infrastructure in the branches. All traffic is reliably and securely routed to Zscaler (cloud-based security platform) with Citrix SD-WAN in the branch network. You can eliminate costly infrastructure and protect your network from threats and vulnerabilities.

Citrix SD-WAN

Citrix SD-WAN helps enterprises move to the cloud by securely enabling local branch-to-Internet breakouts with a built-in stateful firewall for creating policies that can allow or deny Internet access directly from the branch. Citrix SD-WAN identifies applications through a combination of an integrated database of over 4,000 applications, including individual SaaS applications, and uses deep packet inspection technology for real-time discovery and classification of applications. It uses this application knowledge to steer traffic from the branch to the Internet, cloud or SaaS.

Zscaler

Zscaler is the leading cloud-based security platform, which delivers superior security without the need for on-premises hardware, appliances, or software. Zscaler puts a perimeter around the Internet, so that enterprises do not need to put a security perimeter around every office. The Zscaler Cloud Security Platform acts as a series of security check posts in more than 100 data centers around the world. By redirecting internet traffic to Zscaler, enterprises can instantly secure stores, branches, and remote locations. Zscaler connects users and the Internet, inspecting every byte of traffic—even if it is encrypted or compressed—so that users are secure and all hidden threats are identified before they can infiltrate the enterprise network.

Citrix SD-WAN allows creating policies that enable direct Internet breakout from the branch and Zscaler's Cloud Security Platform ensures security for IT by inspecting all internet-bound traffic in a cloud service close to where users connect.

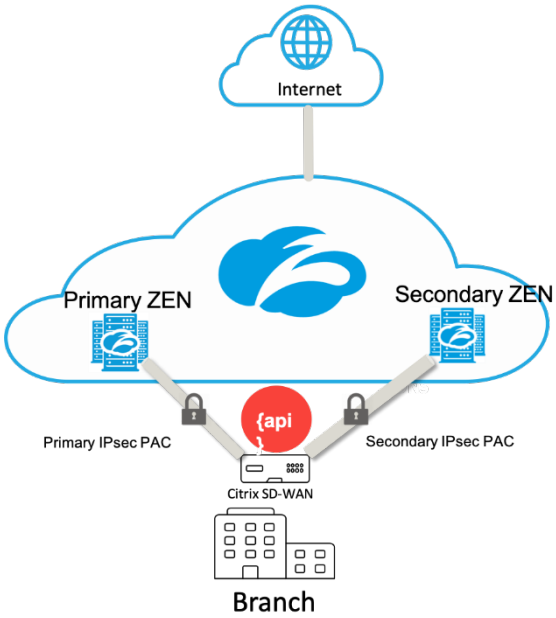
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Zscaler enforcement nodes (ZENs)

Citrix SD-WAN supports Zscaler APIs for automating creation of IPsec tunnels between Citrix SD-WAN and Zscaler Enforcement Nodes (ZENs) in Zscaler's cloud network. ZENs are full-featured, inline Internet security gateways that inspect all Internet traffic bi-directionally for malware, and enforce security and compliance policies.

The Zscaler API provides the two closest data center locations to each branch, allowing SD-WAN to steer traffic effectively. Organizations can allow Zscaler to automatically pick the closest ZEN to the branch by having ZEN look at IP addresses of WAN links configured on Citrix SD-WAN or can manually select the **ZENs**.

> **NOTE**
>
> Both the routes always be in active mode if the tunnel is UP. If any tunnel goes down the corresponding route becomes unreachable and the other route stay UP in that case.



Benefits

The benefits of integrating Citrix SD-WAN and Zscaler include:

- Faster adoption of SaaS and cloud in a distributed enterprise.
  - Centralizing security as a cloud service eliminates the need to have it in each branch.
  - Eliminating the need to backhaul internet-destined traffic allowing local Internet breakout at the branch.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- Simplified IT management with automated connectivity to a Secure Web Gateway.
  - API support automates configuration of secure tunnels to Zscaler
- Improved user experience by reducing latency from backhauling SaaS traffic.
  - Eliminates hub-and-spoke model dependency for security purposes
- Elimination of costly security stacks at branches
  - Reduce the overhead of having to deploy and manage firewalls at the branches.
- Assurance that internet-bound traffic is always secure.
  - Security policies do not tie users to a physical location.
  - Provides sandboxing, inspection of all ports and protocols, including SSL, URL filtering, advanced threat protection, and more to protect against zero-day attacks.

Supported functionality

A Zscaler deployment using SD-WAN appliances supports the following functionality:

- Forwarding user-defined Internet traffic to Zscaler, thereby enabling direct Internet breakout.
- Direct internet access (DIA) using Zscaler on a per customer site basis.
  - On some sites, you might want to provide DIA with on-premises security equipment and not use Zscaler.
  - On some sites, you might choose to backhaul the traffic another customer site for internet access.
- Virtual routing and forwarding deployments.
- One WAN link as part of internet services.

Zscaler is a cloud service. You must set it up as a service and define the underlying WAN links:

- Configure a trusted Public internet wan link at the data center and the branch sites.
- Auto configure IPsec Tunnels for intranet services.

Deploying Zscaler in Citrix SD-WAN Center workflow

The following are the high-level steps that define the workflow to deploy Zscaler in SD-WAN Center.

1. Configure Zscaler subscription to SD-WAN Center (onetime). Log into the Zscaler site to obtain subscription information.
2. Select **Deploy** in Citrix SD-WAN Center GUI.

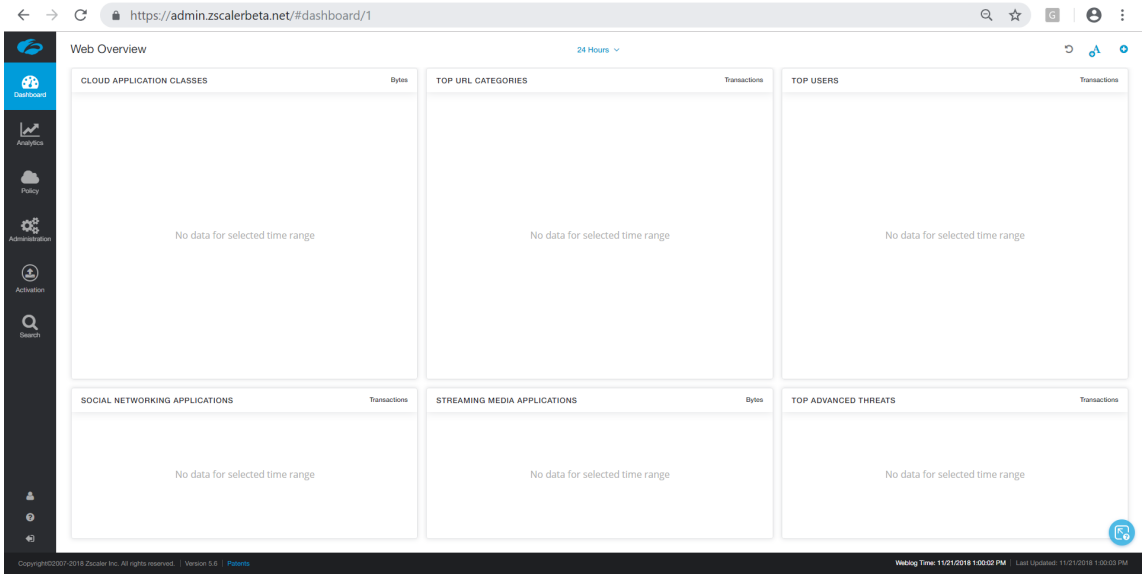
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- Deploy configuration for site using internet wan-link and preconfigured application object.
- Establish Connectivity.
- Get/Update of IPsec status.

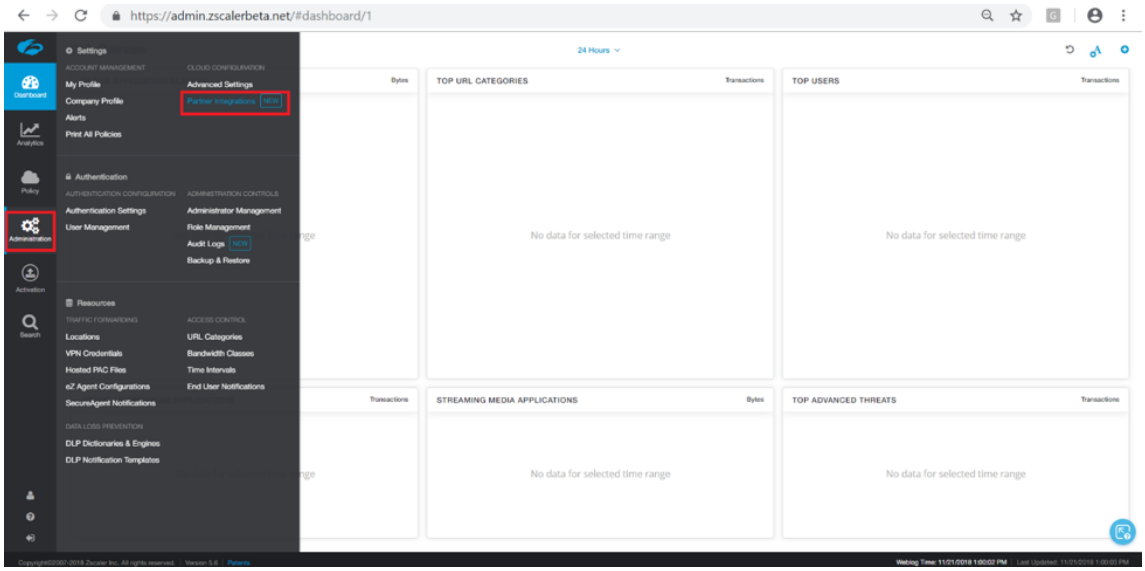
Zscaler subscription

Before you proceed with configuring Zscaler in SD-WAN Center, you need to log into the Zscaler portal.

1. Log into the Zscaler site to obtain subscription information. The Dashboard page opens.

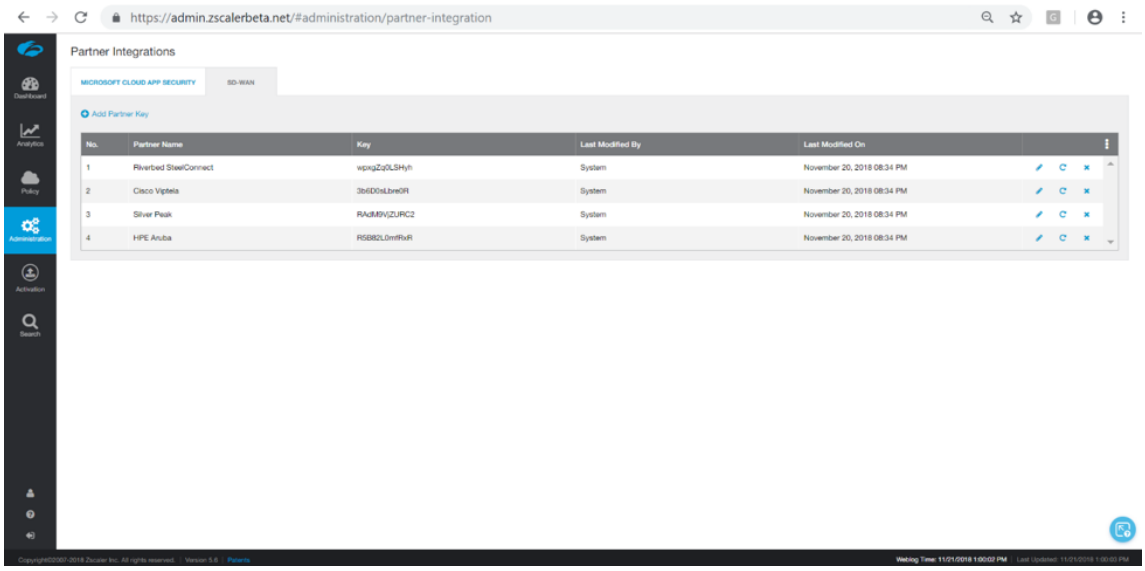


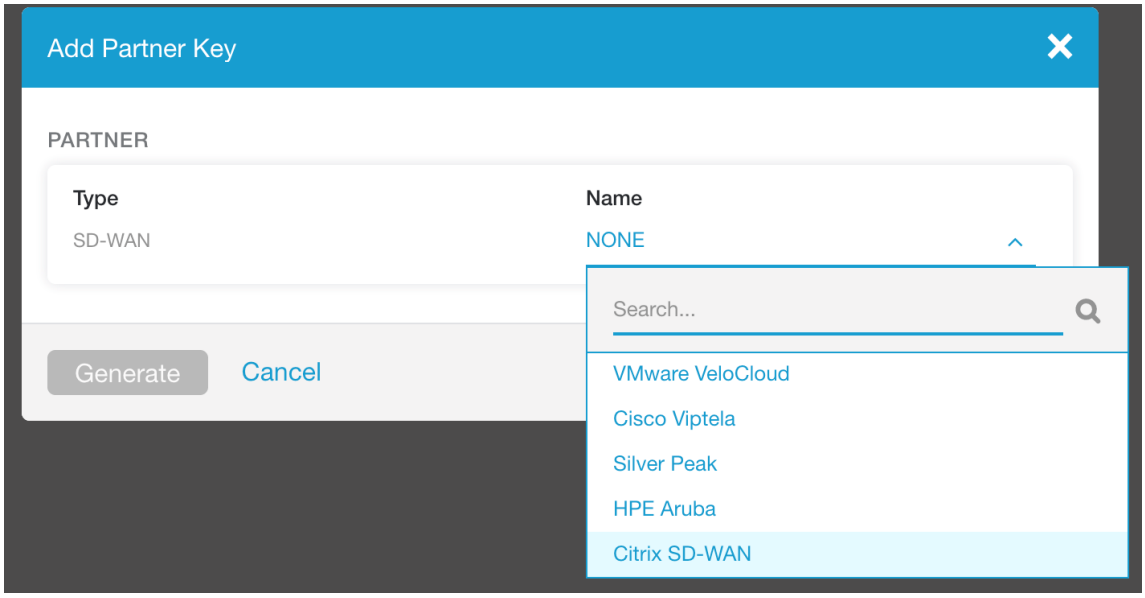
2. Click **Administration > Partner Integrations**.



3. Select **SD-WAN** on the **Partner Integrations** page. Click **Add Partner Key**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



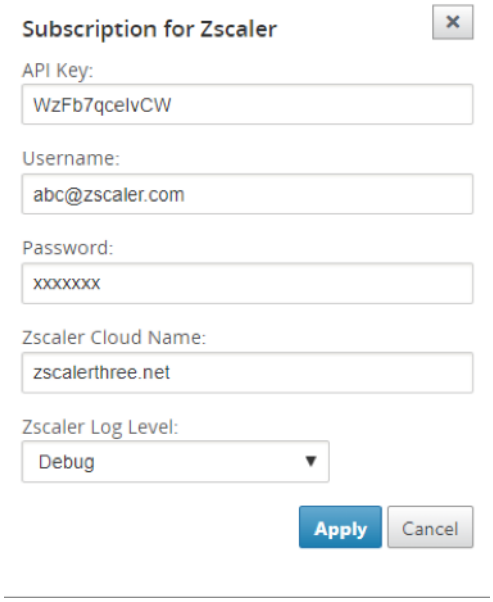


4. Choose **Citrix SDWAN** for the partner key and click **Generate**. Store the key.

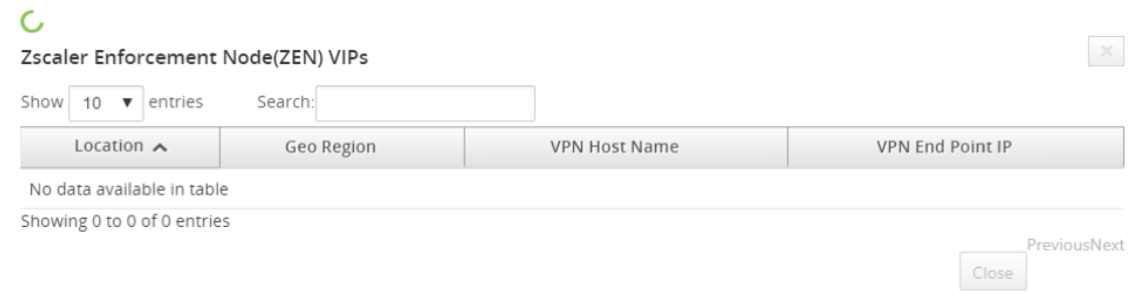
Configure Zscaler in Citrix SD-WAN Center

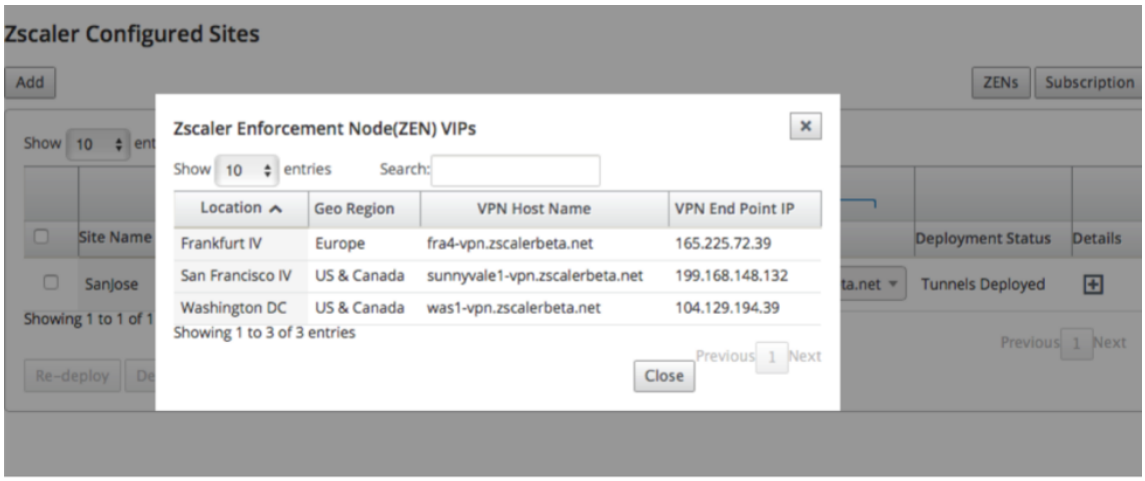
1. In the Citrix SD-WAN Center GUI, navigate to the **Configuration > Security** page. The **Zscaler Configured Sites** page opens.
2. Click **Subscription**. Enter the Zscaler API (partner key) which created in the preceding steps. Provide your Zscaler **Username** and **Password**. Select the **Zscaler Cloud Name**, **Zscaler Log Level**, and click **Apply**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



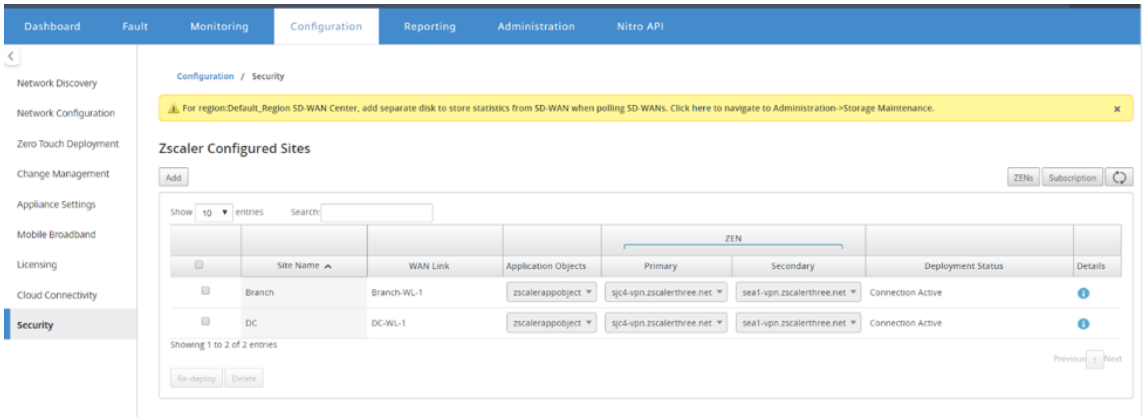
3. Zens provides the list of available VPN endpoints for this Zscaler cloud subscription.



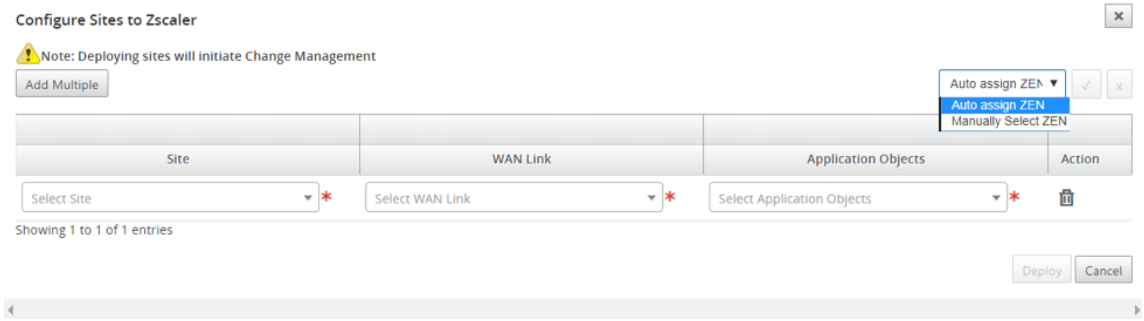


4. After entering the Zscaler subscription and ZEN details, you can start adding sites to Zscaler. Click **Add**.

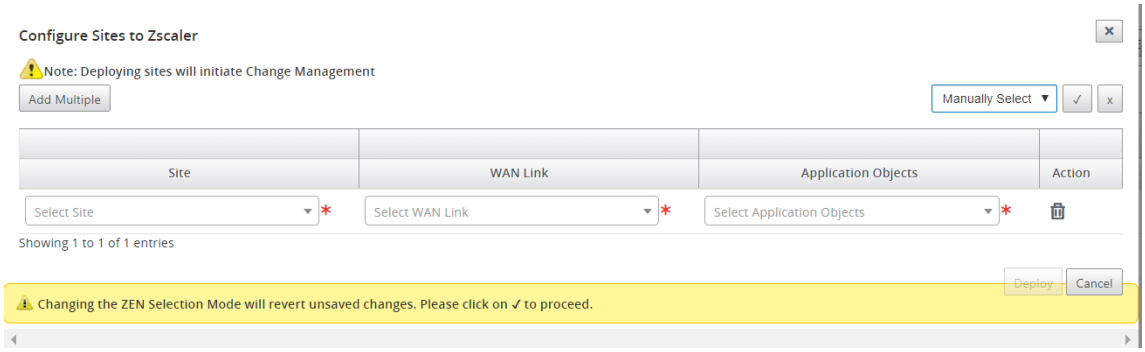
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



5. In the **Configure Sites to Zscaler** dialog box, add **Site, WAN Link,** and **Application Objects**. By default, the **Auto assign ZEN** option is selected.

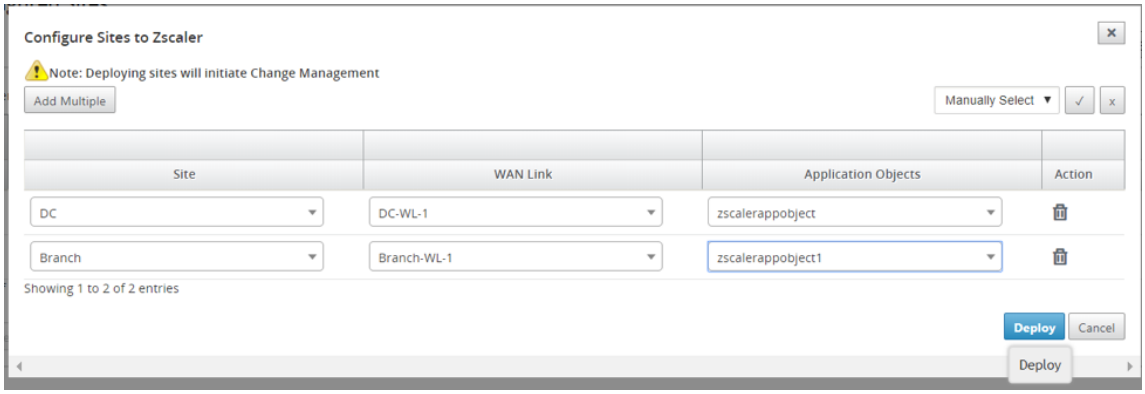


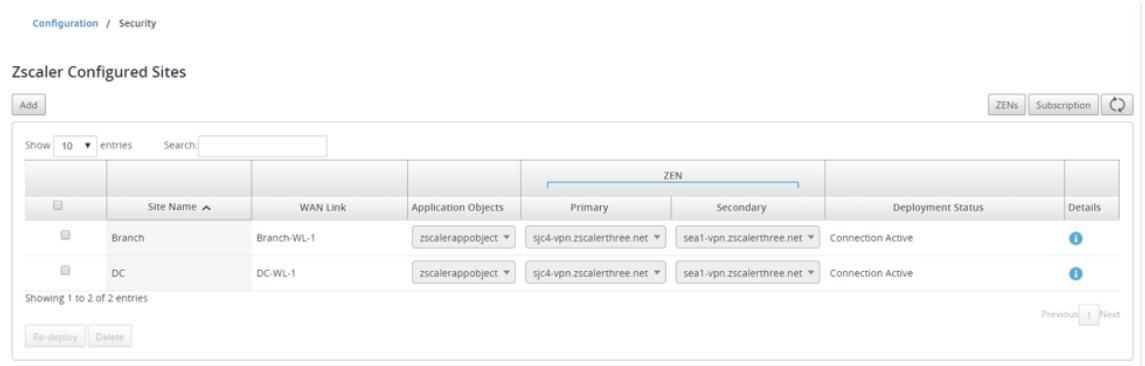
You can **Manually Select ZEN**. However, the following message appears notifying that unsaved changes are lost.



6. Select required sites and click **Deploy**. You can choose to add multiple sites by selecting **Add Multiple**. The selected sites are deployed and the configuration page is displayed.

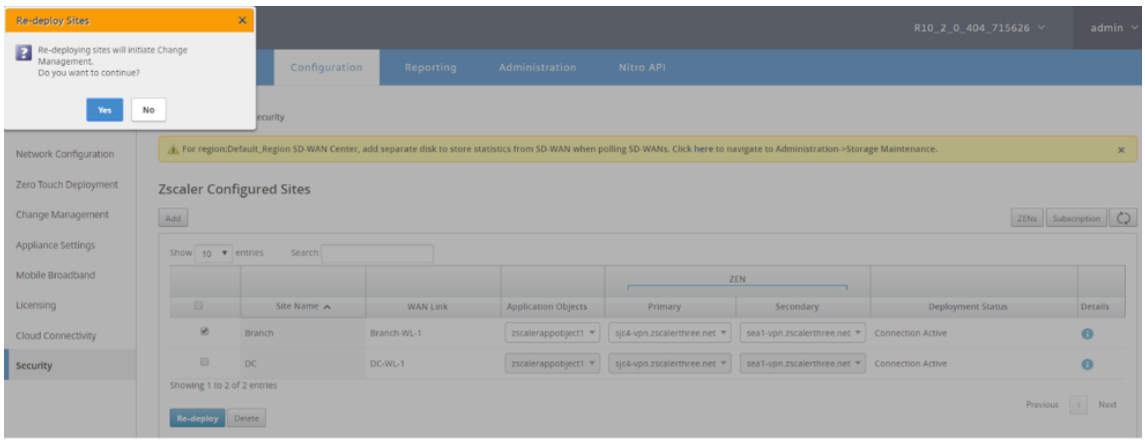
© 1999–2025 Cloud Software Group, Inc. All rights reserved.





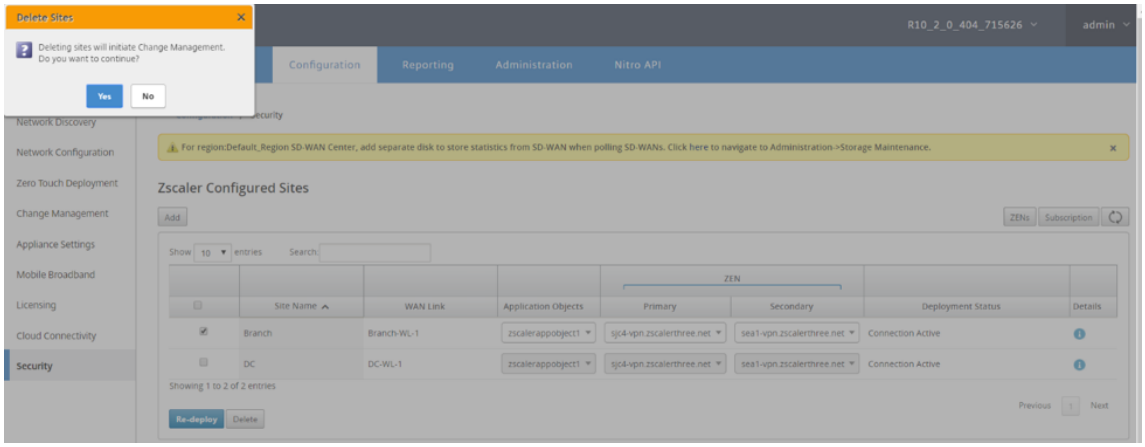
Observe that the primary and secondary ZEN IP addresses are populated and the deployment status is **Connection Active**.

7. Click **Re-Deploy**, if you make changes to the configured site's VPN endpoints or application objects. Any changes to the configured sites in the SD-WAN Center trigger a **Change Management** process on the appliances configured at the branch sites and DC sites.



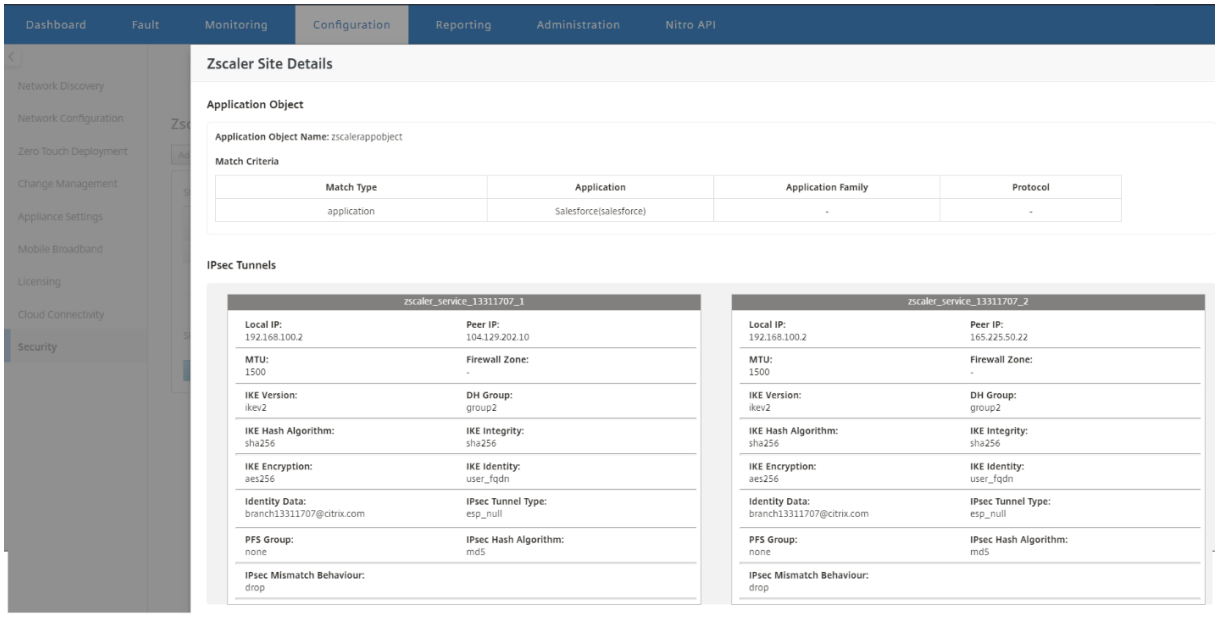
Deleting sites also triggers the change management process.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Monitoring and troubleshooting

Select configured sites to view more information about Application Objects and Primary/Secondary IP addresses. You can click the **Details** icon to view complete information about the configured sites.

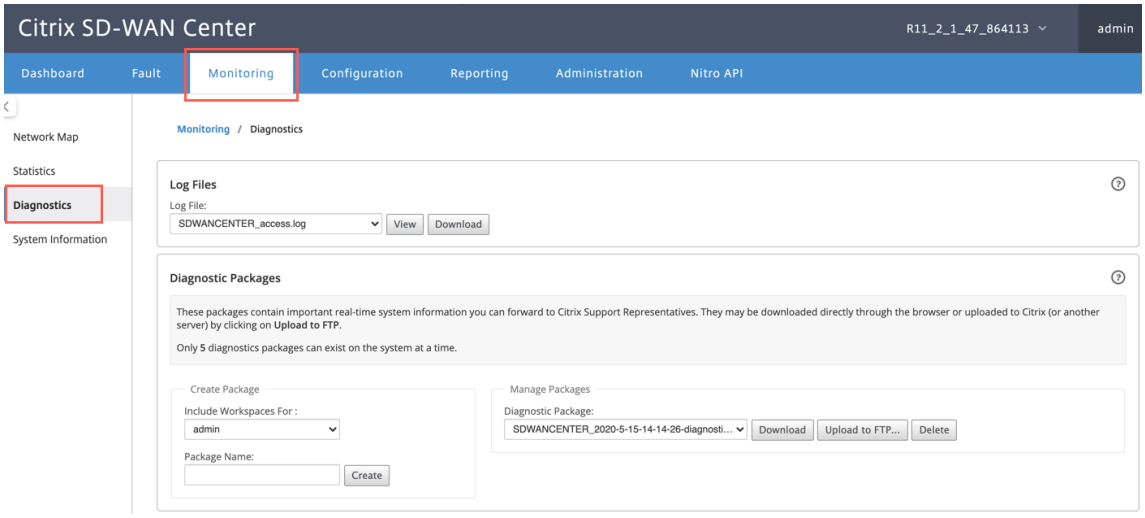


You can view and download the Zscaler logs that can be used to troubleshoot issues in the Citrix SD-WAN Center.

To view Zscaler log files:

1. In the Citrix SD-WAN Center web interface, click the **Monitoring** tab > **Diagnostics**.

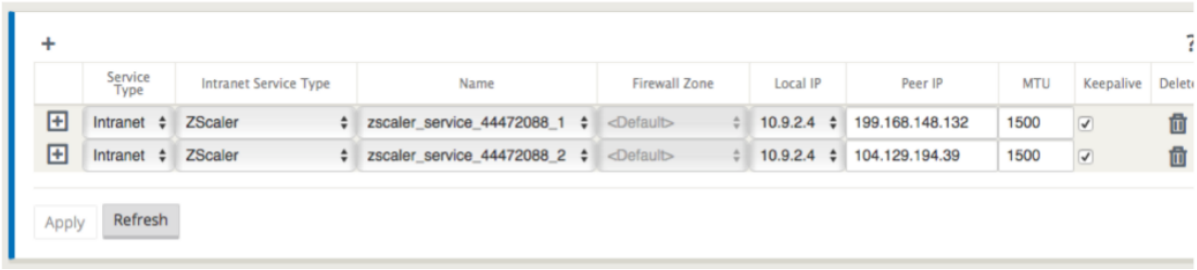
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



2. From the **Log File** drop-down list, select the Zscaler log file you want to view. Click **View**.
3. If you want to download the log files to your computer, click **Download**.

IPsec tunnel configuration

The Details page in SD-WAN Center GUI provides information about the IPsec tunnel configuration to Primary and Secondary endpoints. The Peer IP is obtained from Zscaler. Verify IPsec tunnel configuration in the SD-WAN appliance GUI configuration editor.



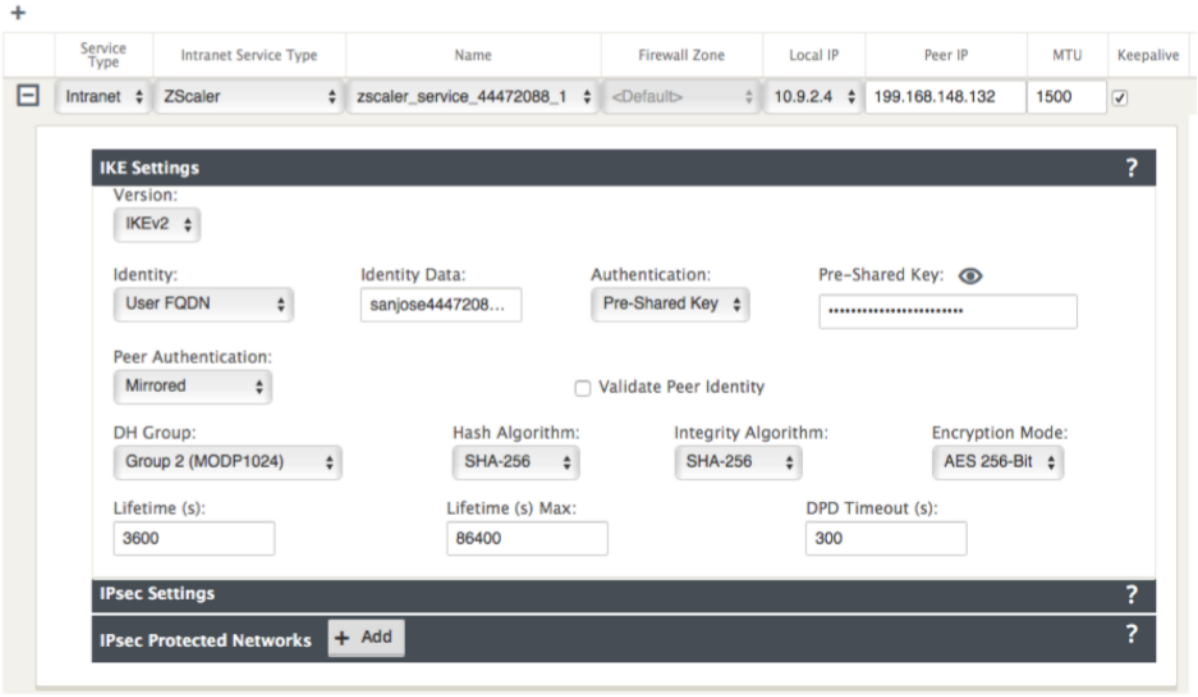
IKE settings

The following IKE/IPSec settings are chosen for IPsec tunnel configuration in the SD-WAN appliance. For more information about configuring IPsec tunnel –IKE settings, see; How to configure IPsec tunnel between SD-WAN and third-party devices topic.

- IKE version - IKEv2
- IKE Identity –User FQDN
- Hash Algorithm - SHA-256
- Integrity Algorithm –SHA-256
- Encryption Mode –AES 256 Bits

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

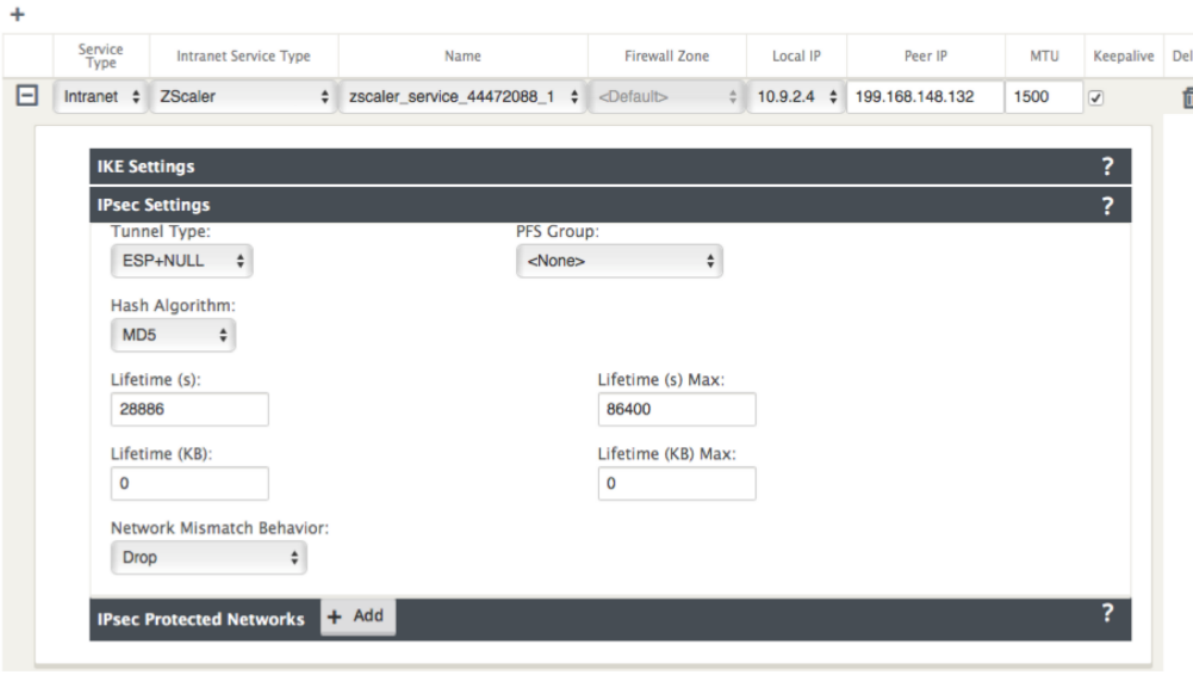
- IPsec –Tunnel Mode
- IPsec Encryption –Null



IPsec settings

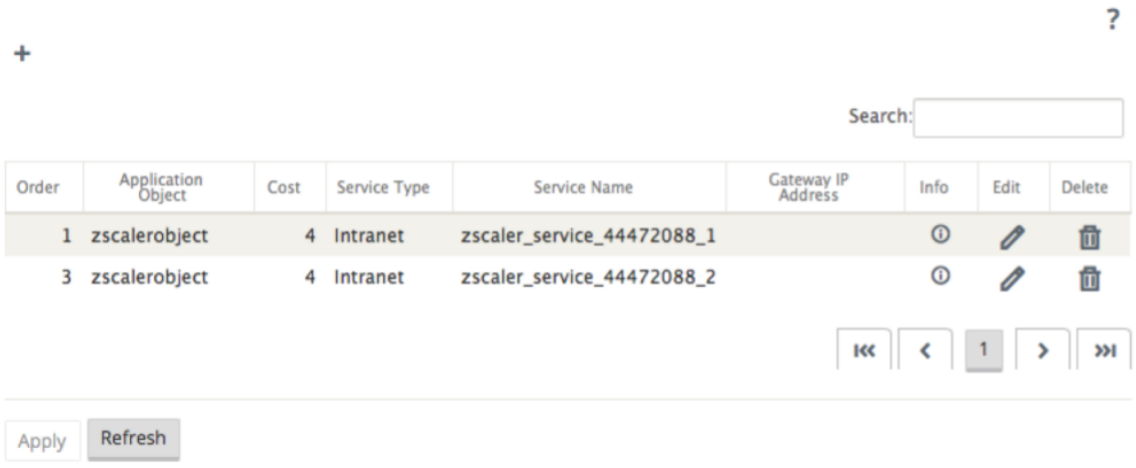
For more information about configuring IPsec tunnel settings, see How to configure IPsec tunnel between SD-WAN and third-party devices topic.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Application objects

Ensure that application objects are configured. For more information about configuring application routes, see Application classification topic.



> **Note**
>
> The GRE tunnel configuration is not supported as part of the automated workflow. However, the manual configuration is still allowed. For more information, see Zscaler Integration by using GRE tunnels and IPsec tunnels.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Monitoring

March 12, 2021

The Citrix SD-WAN Center Dashboard allows you to view the SD-WAN network statistics and graphs on a single pane. For more information, see Dashboard.

You can also view the SD-WAN network Events and Reports in Citrix SD-WAN Center.

Monitoring related articles:

Diagnostic Packages

Event Notifications

Log Files

Memory Dumps

Polling Interval

Statistics

System Information

Dashboard

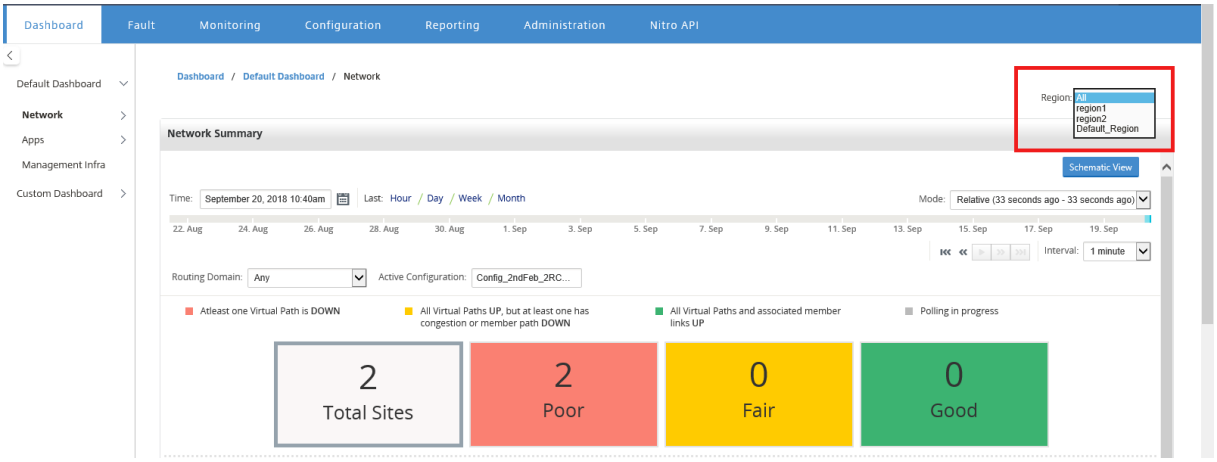
April 22, 2021

The Citrix SD-WAN Center Dashboard displays a subset of the common statistics at a glance. For a single-region deployment, the statistics are obtained from the MCN that is discovered in Citrix SD-WAN Center. For a multi-region deployment, the statistics are obtained from all the regional Citrix SD-WAN Center collectors for the selected time interval. You can view the following statistics:

- Network Summary
- Network QoE
- Top Sites
- Inventory
- Events and Alarms
- Top Apps
- HDX QoE
- Management Infra

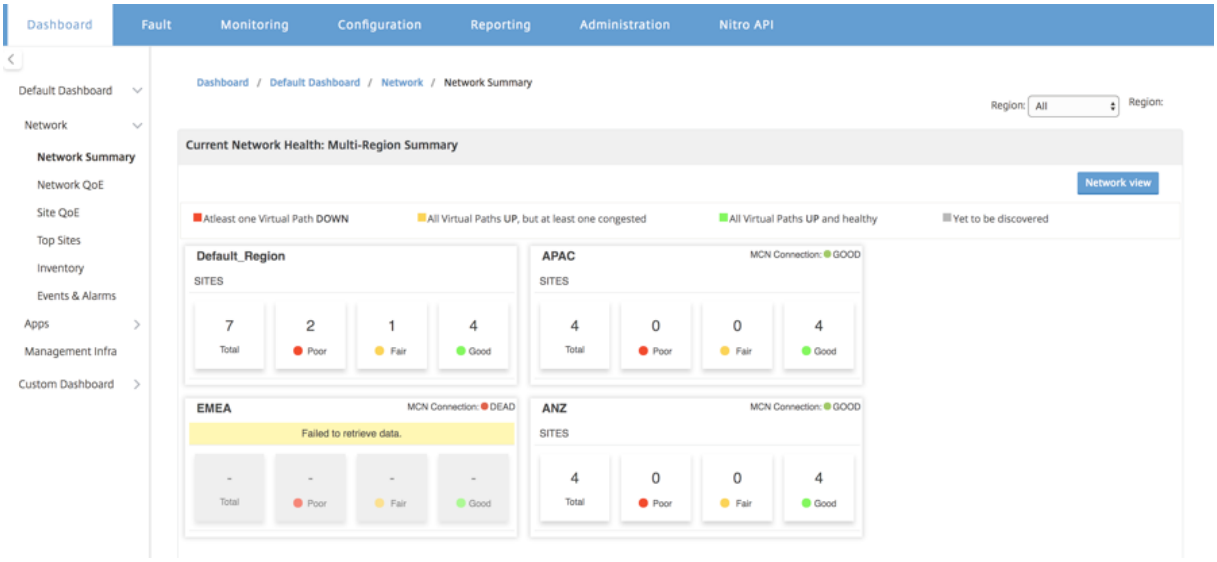
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

For a single-region deployment, the default region statistics are displayed on the dashboard. For a multi-region deployment, you can choose to view the multi-region dashboard or the regional dashboard. To view the multi-region dashboard, in the **Region** menu select **All**. However, you cannot view the multi-region summary dashboard when more than 300 sites are configured.



You can view the MCN Connection status on each region tile. The MCN Connection status is the health status of the virtual path between an RCN and the MCN.

> **Note**
>
> For a multi-region deployment, the default region statistics include statistics of all the sites managed by the MCN. It might also include RCN statistics since the RCNs have virtual paths to the MCN.
>
> The **Region** drop-down menu is not available in Citrix SD-WAN Center Collectors.



The Citrix SD-WAN Center Dashboard is refreshed based on the configured polling interval. The default polling interval is five minutes. For more information, see Polling Interval.

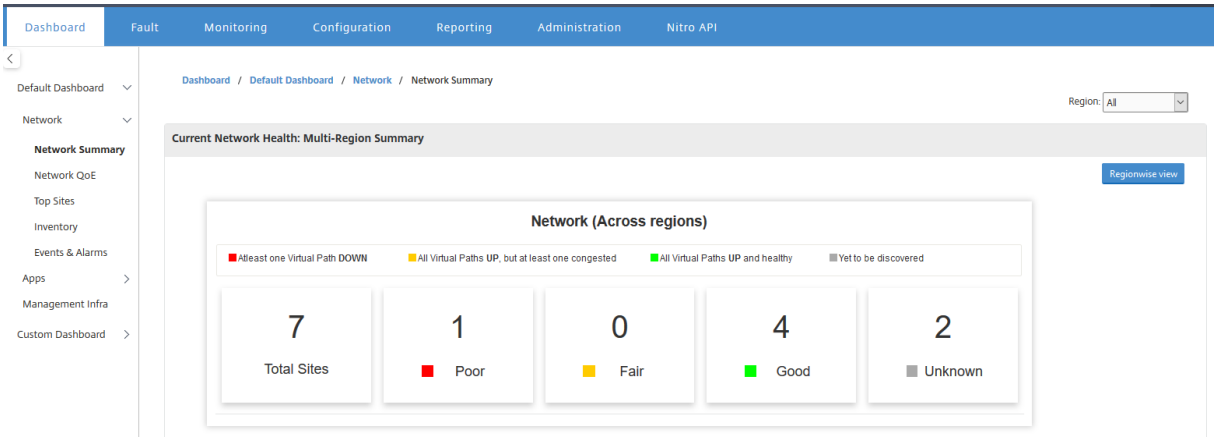
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Network summary

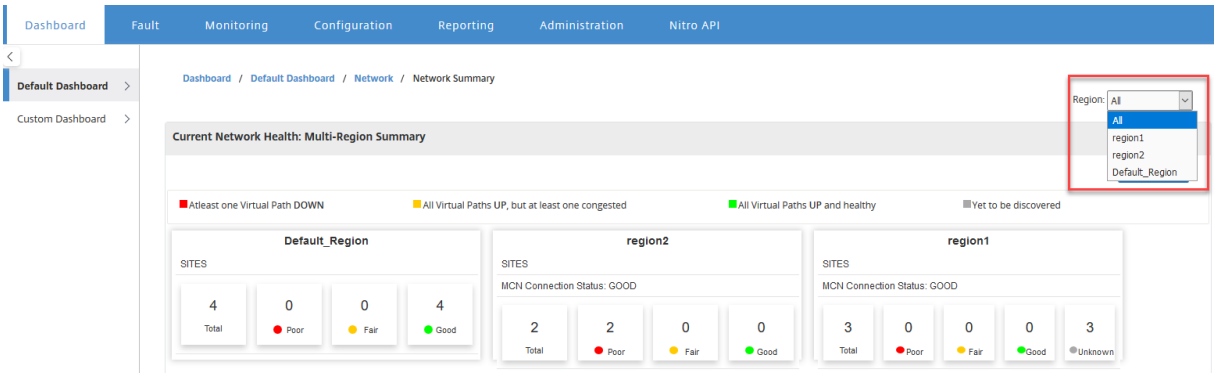
For a multi-region deployment, the **Network Summary** widget provides an overview of the network health at all the various regions. A region card for every region in the network is displayed with the following information:

- The total number of sites in the region.
- The number of sites in the Poor state. A site is in the Poor state when at least one virtual path is DOWN.
- The number of sites in the Fair state. A site is in the Fair state when all the virtual paths in the site are UP, but at least one path has congestion issue or a member path is DOWN.
- The number of sites in the Good state. A site is in the Good state when all the virtual paths and the associated member paths are UP.
- The number of sites in the Unknown state. A site is in the Unknown state when polling is in progress.

To view multi-region network summary, navigate to **Dashboard** > **Default Dashboard** > **Network** > **Network Summary** and in the **Region** drop-down menu, select **All**.



By default the screen appears in **Network view**. You can see the current network health of the multi-region network summary by clicking the **Region wise view**. You can also see the MCN Connection status on each region tile.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Click a region card to drill down into the regional dashboard.

For an individual region, the **Network Summary** widget provides an overview of the network health of the selected region.

To view regional network summary, navigate to **Dashboard** > **Default Dashboard** > **Network** > **Network Summary** and in the **Region** drop-down menu, select **a region**.

You can view the regional network summary in either the tile view or the schematic view.

You can use the timeline control to view the network status summary for a selected period. You can also play or pause the network status over a time range.

Mode helps to see the time as a relative or an absolute concept.

For more information on Timeline and mode see Timeline controls.

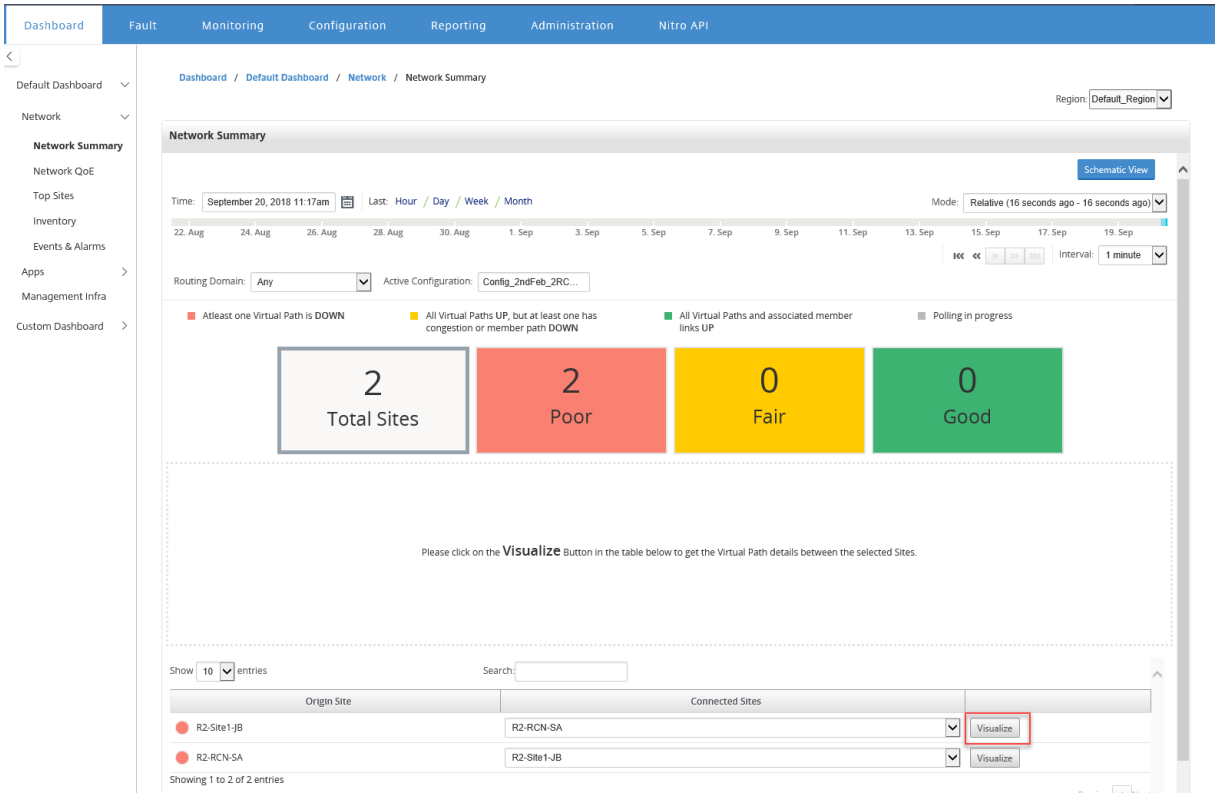
Tile view

The tile view provides the following information:

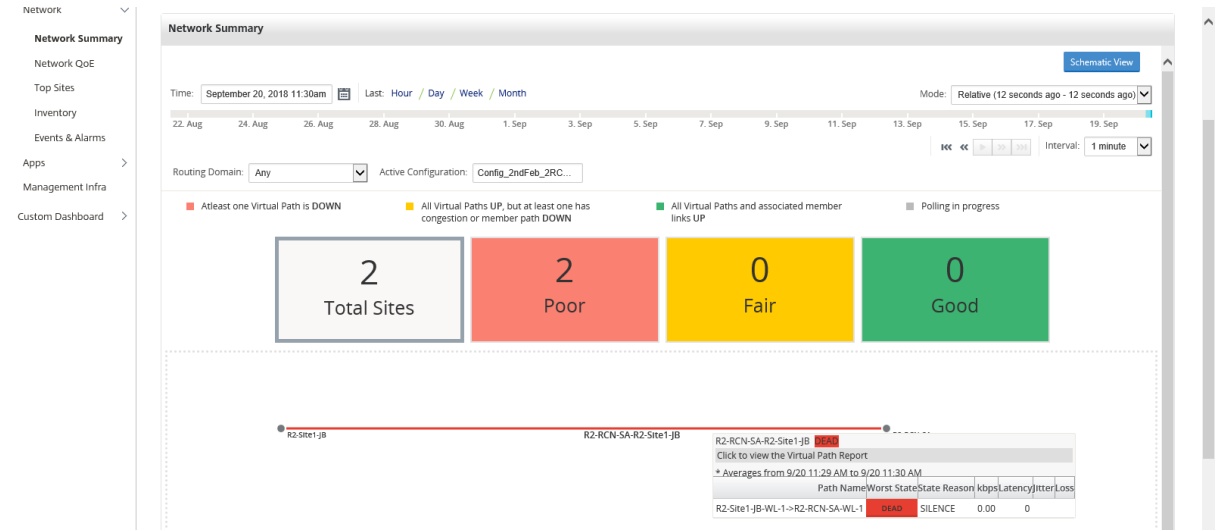
- The total number of sites in the region.
- The number of sites in the Poor state. A site is in the Poor state when at least one virtual path is DOWN.
- The number of sites in the Fair state. A site is in the Fair state when all the virtual paths in the site are UP, but at least one path has congestion issue or a member path is DOWN.
- The number of sites in the Good state. A site is in the Good state when all the virtual paths and the associated member paths are UP.
- The number of sites in the Unknown state. A site is in the Unknown state when polling is in progress.

To view a graphical representation of a path between two sites, select the path and click **Visualize**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Hover the mouse cursor over the sites or the path to view more details. Click the sites to view and select report options.



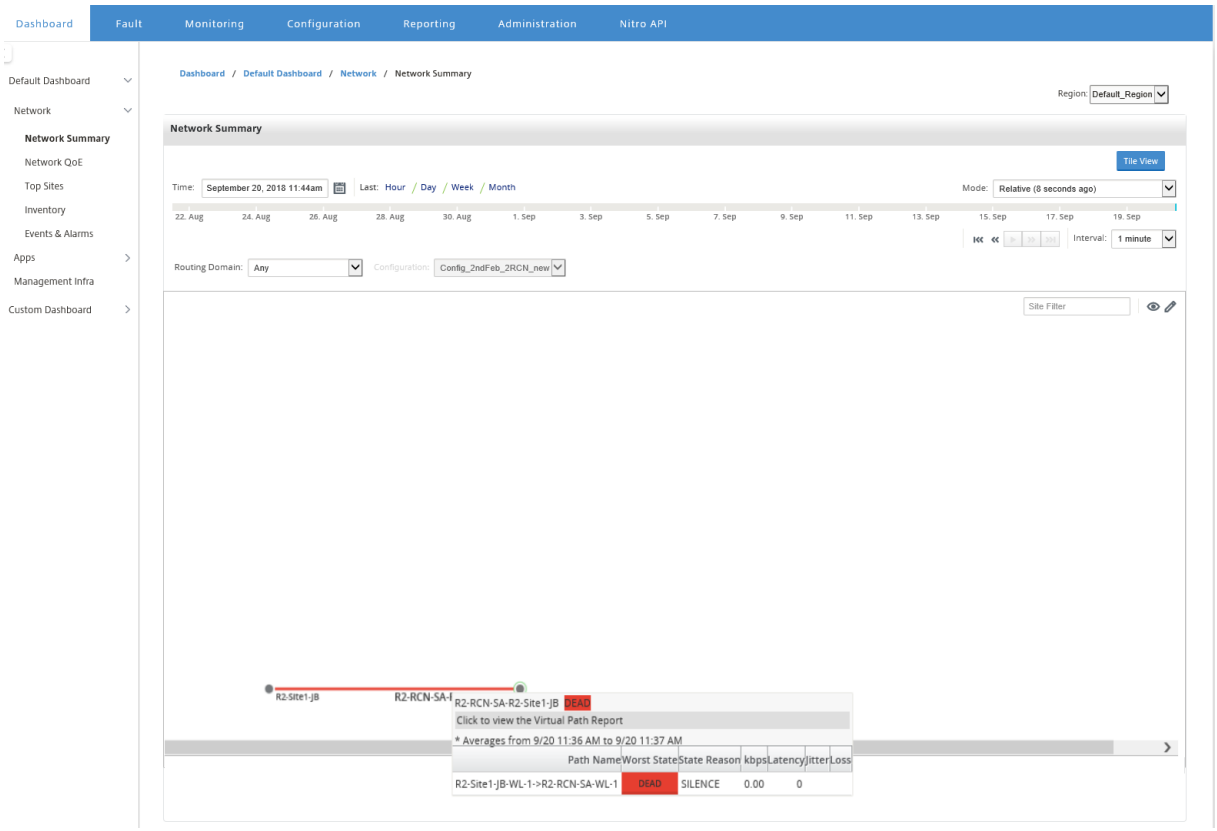
Schematic view

The schematic view provides a graphical view of the SD-WAN network. The information displayed in this section is updated depending on the selected configuration and routing domain. To view a network map here, you must import the network configuration and Network maps from the Master

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Controller Node (MCN). For more information, see Import MCN configuration.

Hover the mouse cursor over the sites or the path to view more details. Click the sites to view report options.



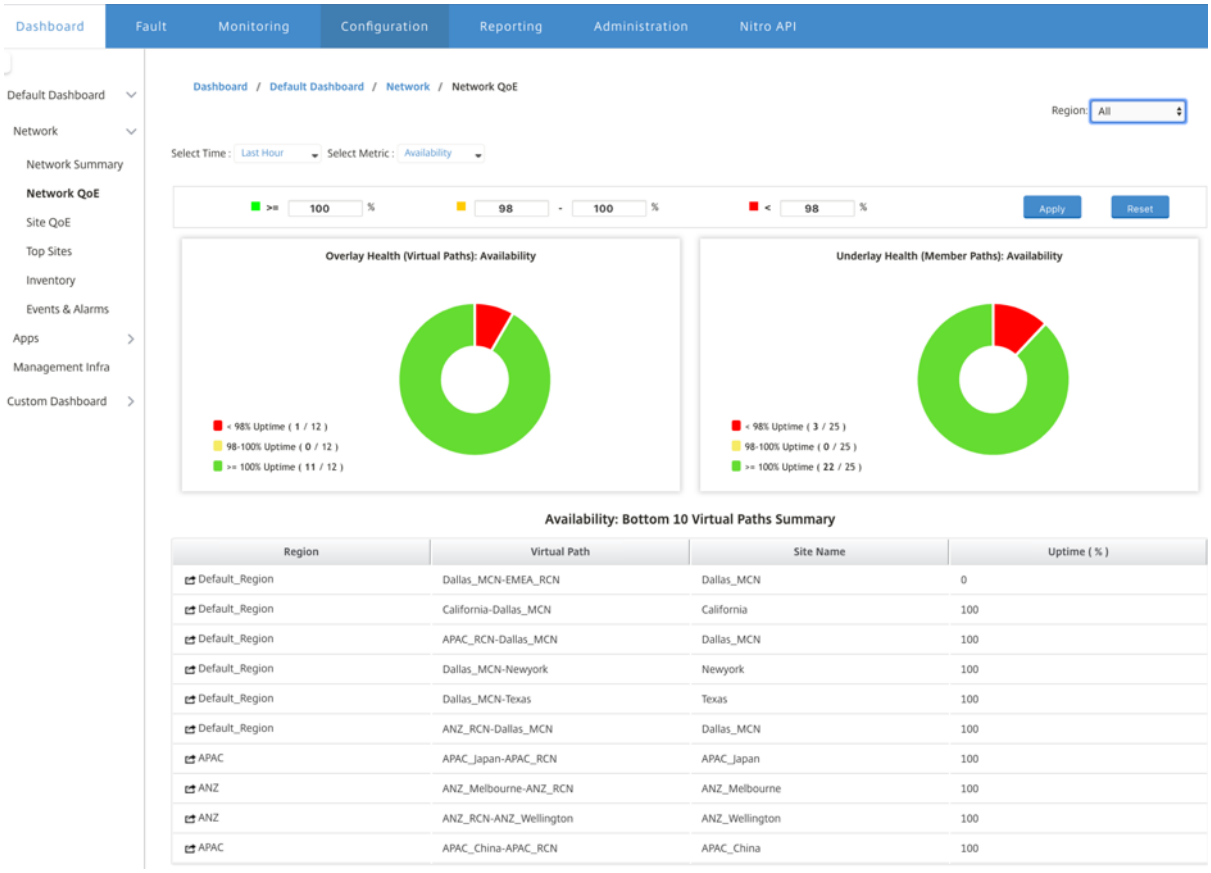
Network QoE

The **Network QoE** widget provides a graphical representation of the availability, loss, latency, and jitter parameters of a virtual path. It provides the statistics for both overlay virtual path and the underlay member paths.

For a multi-region deployment, you can view a list of the bottom 10 virtual paths depending on the selected metric. The virtual path data is collected from all the regional collectors for the selected time interval. You can view the bandwidth, jitter, loss, and congestion details of the virtual paths that need your attention the most.

To view multi-region virtual path health, navigate to **Dashboard** > **Default Dashboard** > **Network** > **Network QoE** and in the **Region** drop-down menu select **All.**

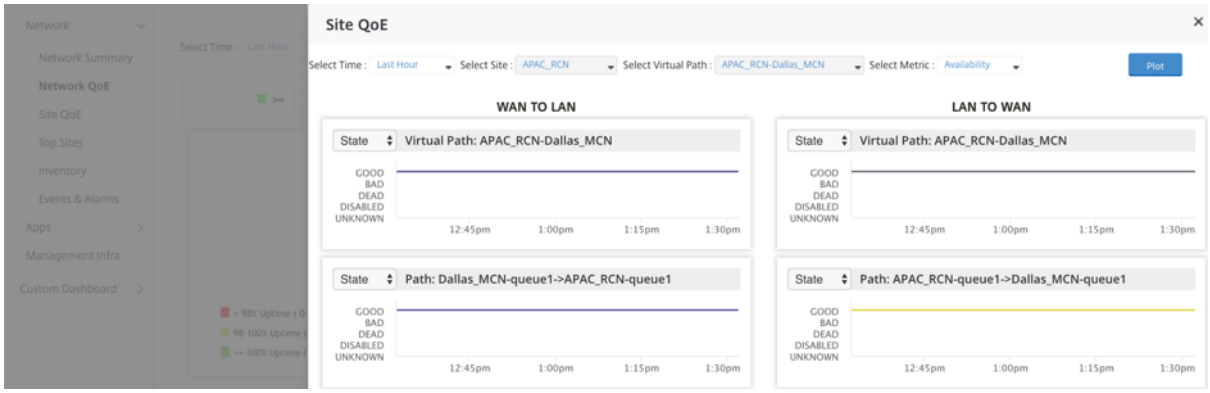
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



For an individual region, you can view a list of the bottom 10 virtual paths depending on the selected metric. The statistics are collected for the selected time interval. You can view the bandwidth, jitter, loss, and congestion details of the virtual paths that need your attention the most.

You can compare the overlay and underlay paths for the selected metric (availability, loss, jitter, latency) over the selected time interval. You can also set custom thresholds for the metrics and save them on click **Apply**. Click **Reset** to store the default thresholds.

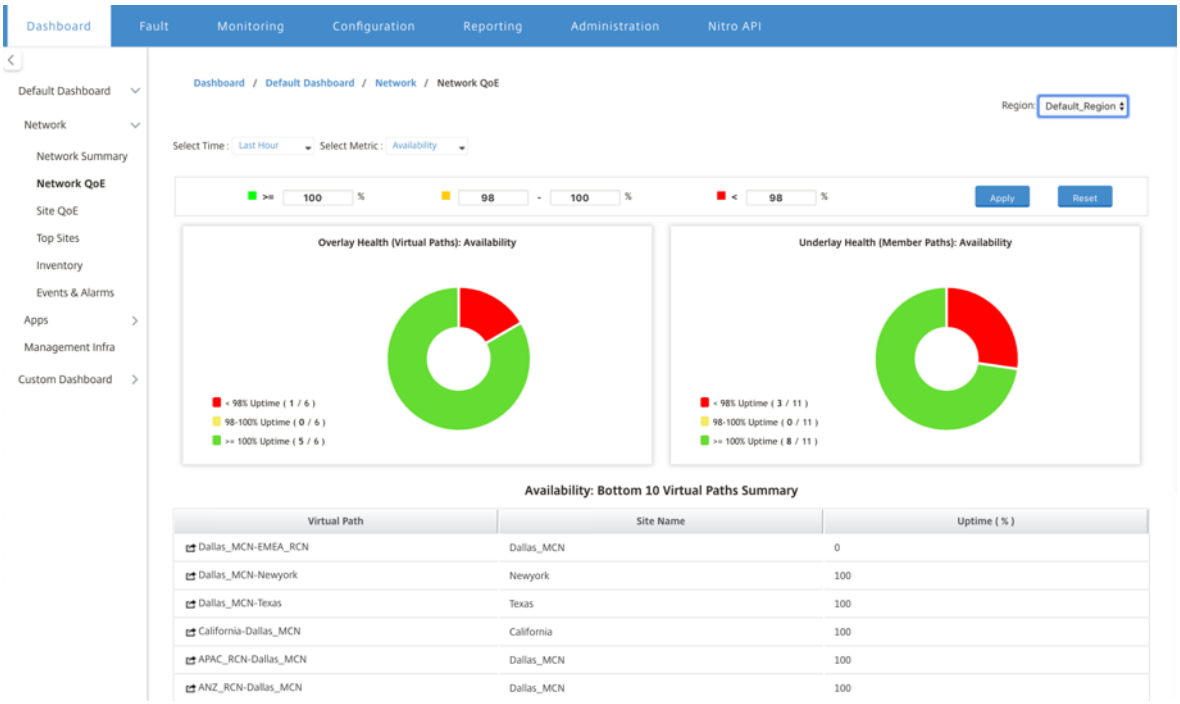
The user can also drill down to any virtual path in the table by using on the **drill down** button on the left of each row. A **Site QoE** appears with the detailed comparison between the conduit and its underlying member paths.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

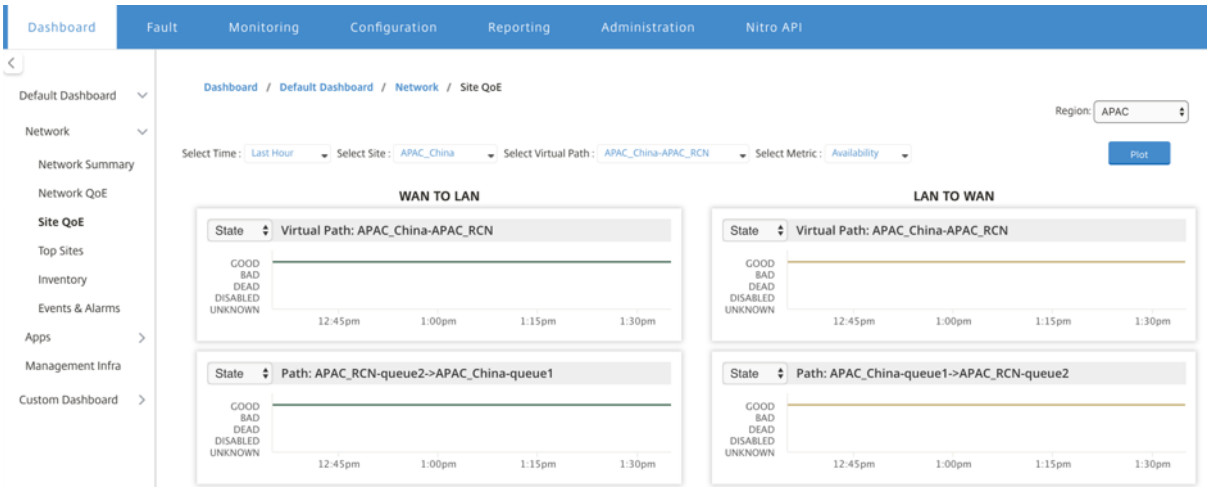
In the slider, the site name and virtual path are selected by default depending on the row that you clicked and it will be disabled. However the user can select a different time range and metric and click **Plot** option to plot the new graphs.

To view regional virtual path health statistics, navigate to **Dashboard** > **Default Dashboard** > **Network** > **Network QoE** and in the **Region** drop-down menu select a region.



Site QoE

You can use Site QoE as a tool to compare the virtual path and it's underlying member paths. You need to select a site and any virtual path from this site and metric. Click **Plot**.



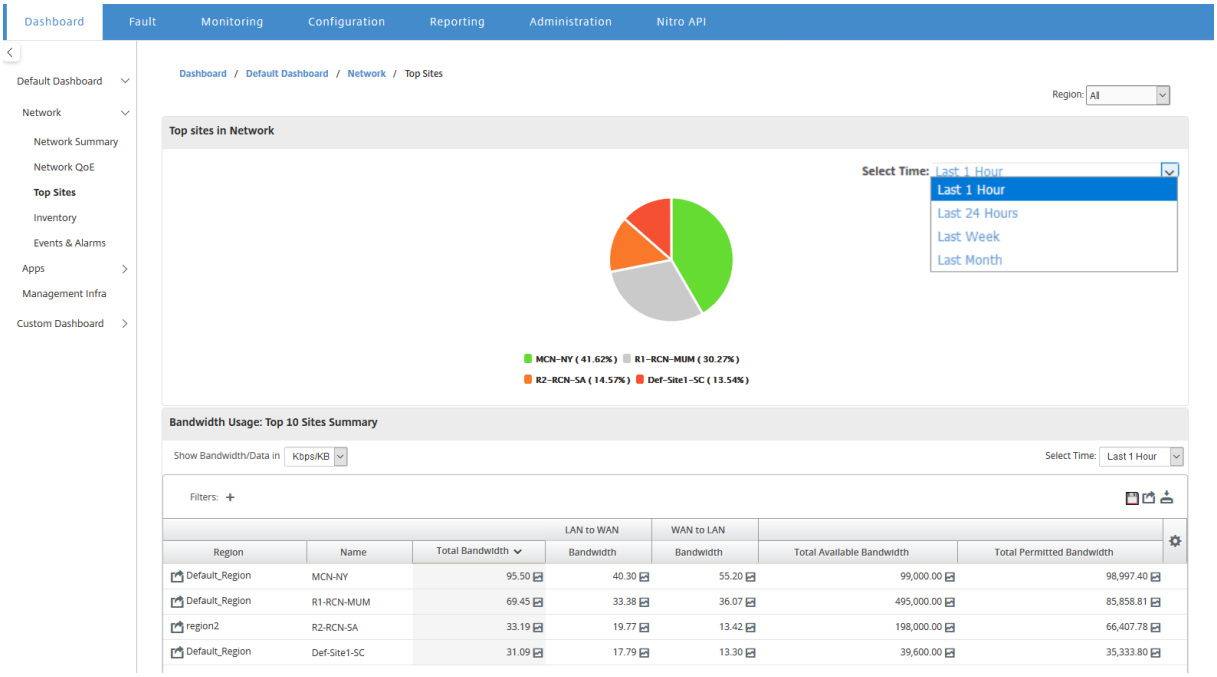
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

In the first section, it plots the virtual paths statistics in both **WAN to LAN** and **LAN to WAN** direction. Below section plots all the underlying member paths graphs. Both these things are present at both region and network level.

Top sites

For a multi-region deployment, the **Top Sites** widget lists the top 10 sites across all the regions, which have the highest bandwidth usage, in the selected time interval.

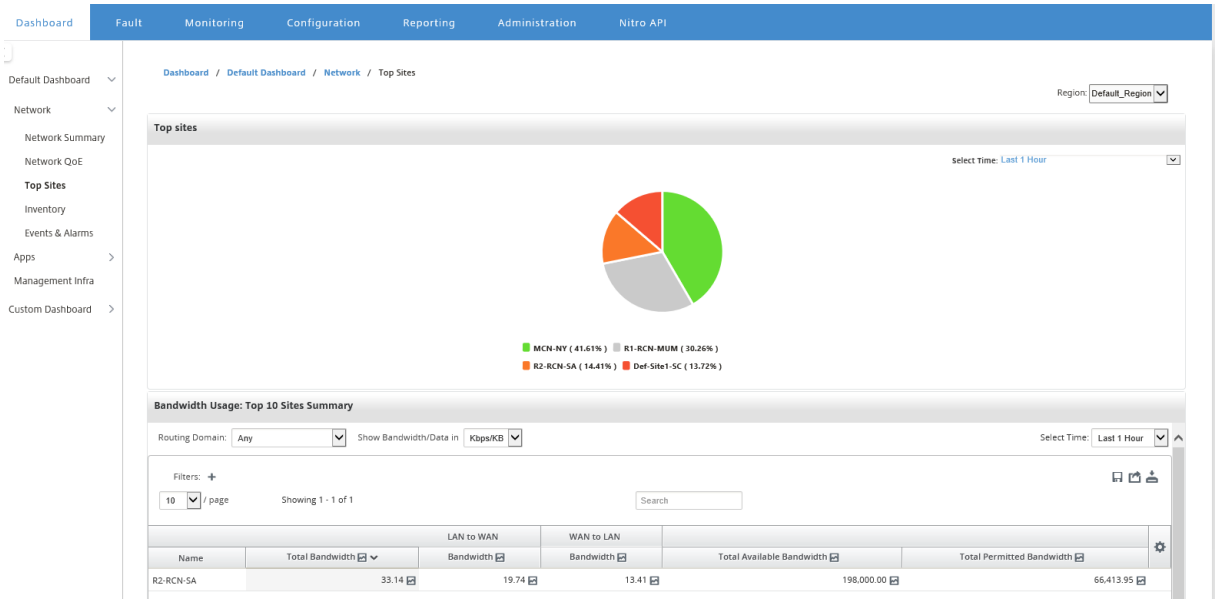
To view the top sites across all regions, navigate to **Dashboard** > **Default Dashboard** > **Network** > **Top Sites** and in the **Region** drop-down menu select **All.**



Click a site or metric to view detailed reports and statistics.

For an individual region, the Top Sites widget displays the bandwidth usage statistics for all the sites in the region. The statistics are collected for the selected time interval. You can filter the sites based on the routing domain.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Inventory

Every 30 minutes, the Inventory manager gathers the hardware information from all the Citrix SD-WAN appliances that are discovered on Citrix SD-WAN Center.

To view the multi-region inventory statistics, navigate to **Dashboard** > **Default Dashboard** > **Network** > **Inventory** and in the **Region** drop-down menu select.

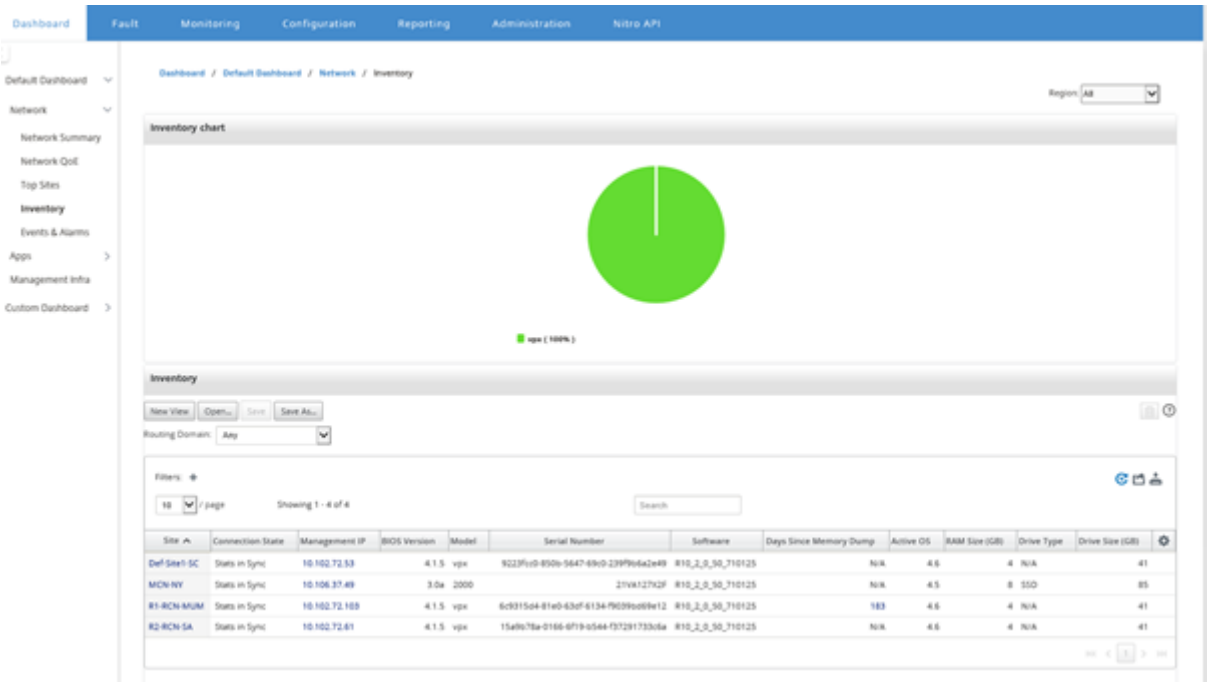
To view inventory statistics of a specific region, in the **Region** drop-down menu select the region.

You can view the following inventory statistics:

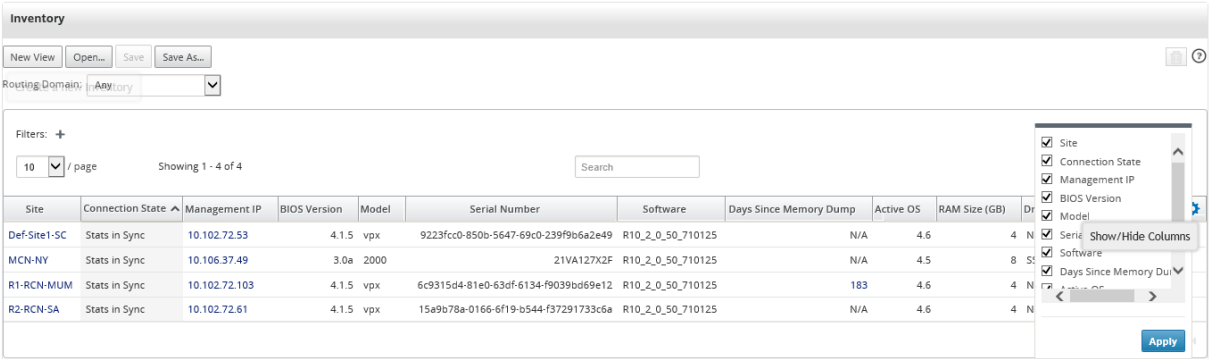
- **Site**: Name of the site found in the configuration running in the MCN. If the appliance is a secondary MCN, "(secondary)"appears next to the name. You can click the name to access the appliance web console.
- **Connection Status**: Connectivity state to the appliance. A red icon appears when the connection is not reachable or not authenticated.
- **Management IP**: Management IP address of the appliance. You can click the IP address to access the appliance web console.
- **BIOS Version**: BIOS version of the appliance.
- **Model**: Hardware model of the appliance.
- **Serial Number**: Serial Number of the appliance.
- **Software**; SD-WAN software version number.
- **Days Since Memory Dump**: Time since last system-error memory dump. If the appliance dumped its memory in the past four days, an error icon appears next to the time. If the memory dump occurred between 5 and 10 days ago, a warning icon appears. N/A appears if no dump is available. Clicking the time opens the log page of the SD-WAN.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- **Active OS**: The OS currently running on the appliance.
- **RAM Size (GB)**: Amount of RAM currently installed on the appliance in GB.
- **Drive Type**: Type of data-storage drive installed on the appliance. The value can be SSD (Solid State Drive) or HDD (Hard Disk Drive).
- **Drive Size (GB)**: Size of the data-storage drive currently installed on the appliance in GB.



> **Note**
>
> You can arrange the columns for the inventory statistics table by using the **Show/Hide Columns** option.



Events and alarms

For a multi-region deployment, you can view the events and alarms of all the regions in the network. This information is collected for the selected time interval. To view multi-region events and statistics,

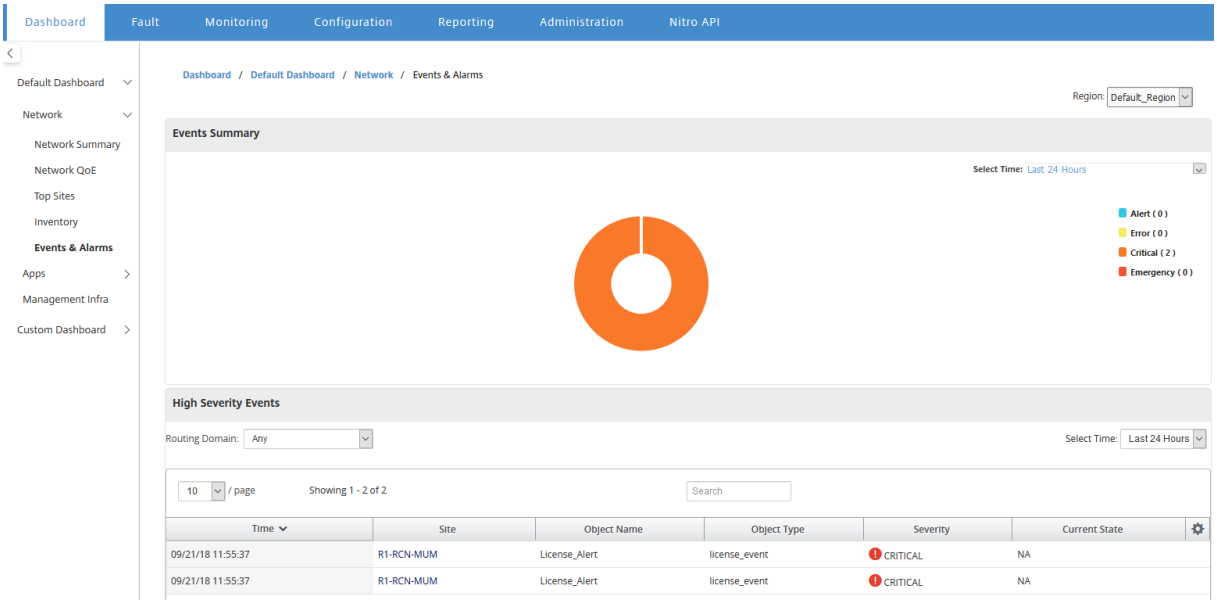
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

navigate to **Dashboard** > **Default Dashboard** > **Network** > **Events & Alarms** and in the **Region** drop-down menu select **All**.

You can also view all the events and alarms of an individual region. This information is collected for the selected time interval. To view events and alarm statistics, navigate to **Dashboard** > **Default Dashboard** > **Network** > **Events & Alarms** and in the **Region** drop-down menu select a region.

The **Event Summary** section gives a graphical overview of the event type and quantity of events. You can click the graph to view the events on the **Fault** page. The display also outlines how many events are in each category. Alarm triggers can be configured on the individual SD-WAN Appliances. For more information see, Event notifications.

The **High Severity Events** section displays a list of the severe events. You can filter the events based on the routing domain. The information displayed in this section is gathered from the **Fault** tab. For more information, see Events.



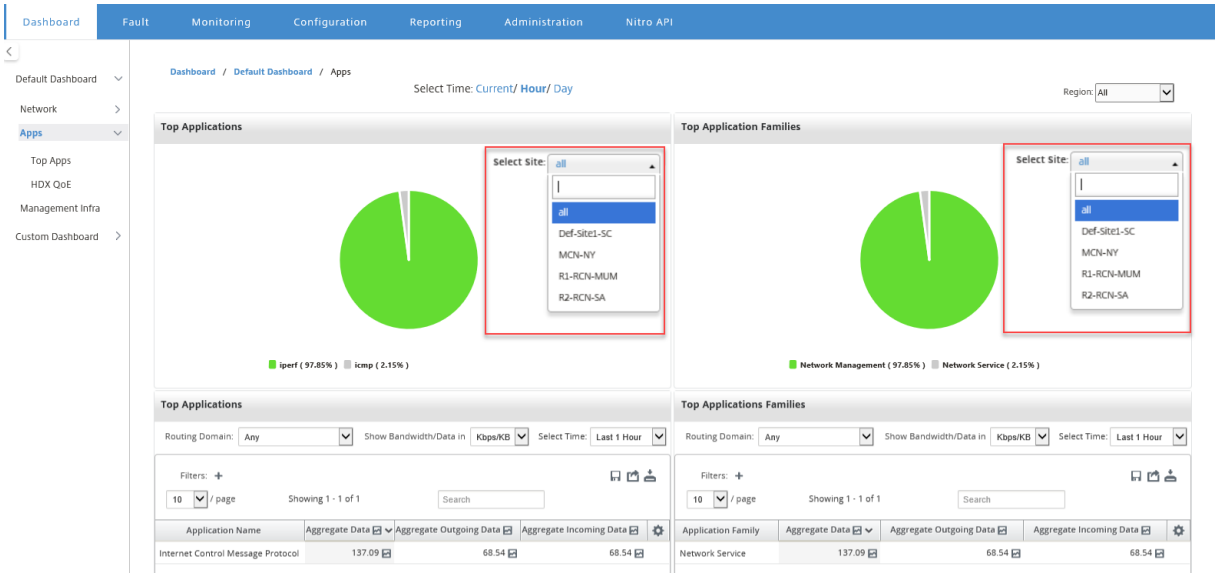
Apps

Top apps

Deep packet inspection (DPI) allows the SD-WAN appliance to parse the traffic passing through it and identify the application and application family types. For a multi-region deployment, you can view the top applications and top application families across all the regions in the network. This information is collected for the selected time interval.

To view top application statistics across all the regions in the network, navigate to **Dashboard** > **Default Dashboard** > **Apps > Top Apps,** and in the **Region** drop-down menu select **All.**

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

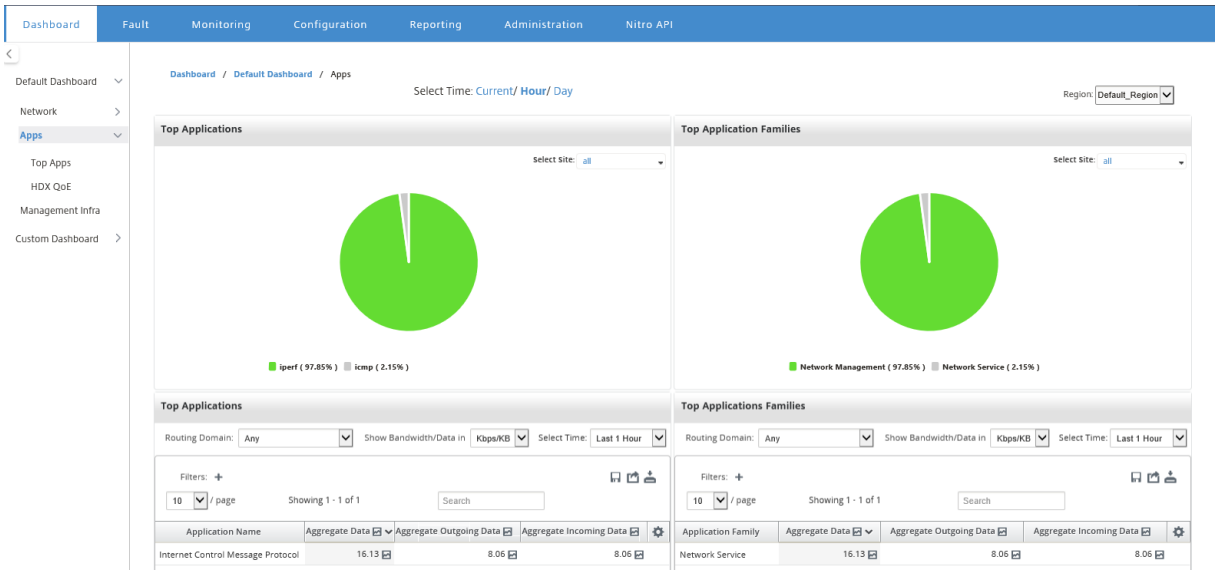


You can view the searchable drop-down list for site selection for both **Top Application** and **Top Application Families**.

You can also view the top applications and top application families of a particular region.

To view the application statistics of a region, navigate to **Dashboard** > **Default Dashboard** > **Apps > Top Apps** and in the **Region** drop-down menu select a region**.**

You can select the site and time interval as last 24 hours, last 1 hour, or current.



HDX QoE

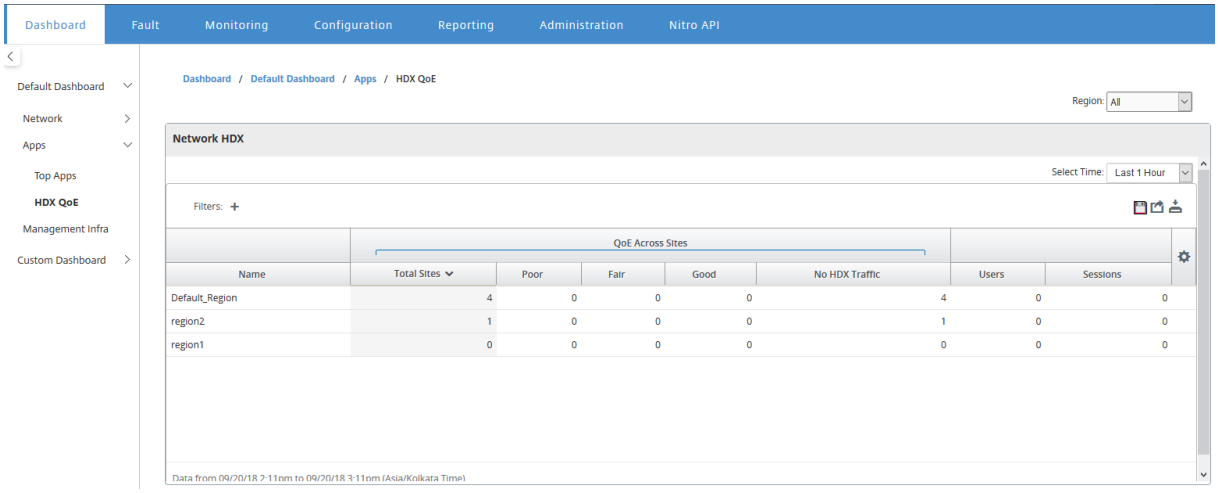
Quality of Experience (QoE) is a calculated index that helps you understand your ICA quality of experience. This index is calculated for all ICA application traffic traversed from WAN to the site. Statistics of

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

packet drop, jitter, and latency are used in the QoE calculation. The QoE is an integer between [0, 100], the higher the number, the better the user experience. The jitter, latency, and packet drop statistics are tracked on data paths during packet processing.

Sites in the entire network are categorized as good, fair, poor, or no HDX traffic based on the QoE of HDX traffic. For more information, see HDX QoE.

To view HDX QoE, of sites, across all the regions in the network, navigate to **Dashboard** > **Default Dashboard** > **Apps > HDX QoE,** and in the **Region** drop-down menu select **All.**

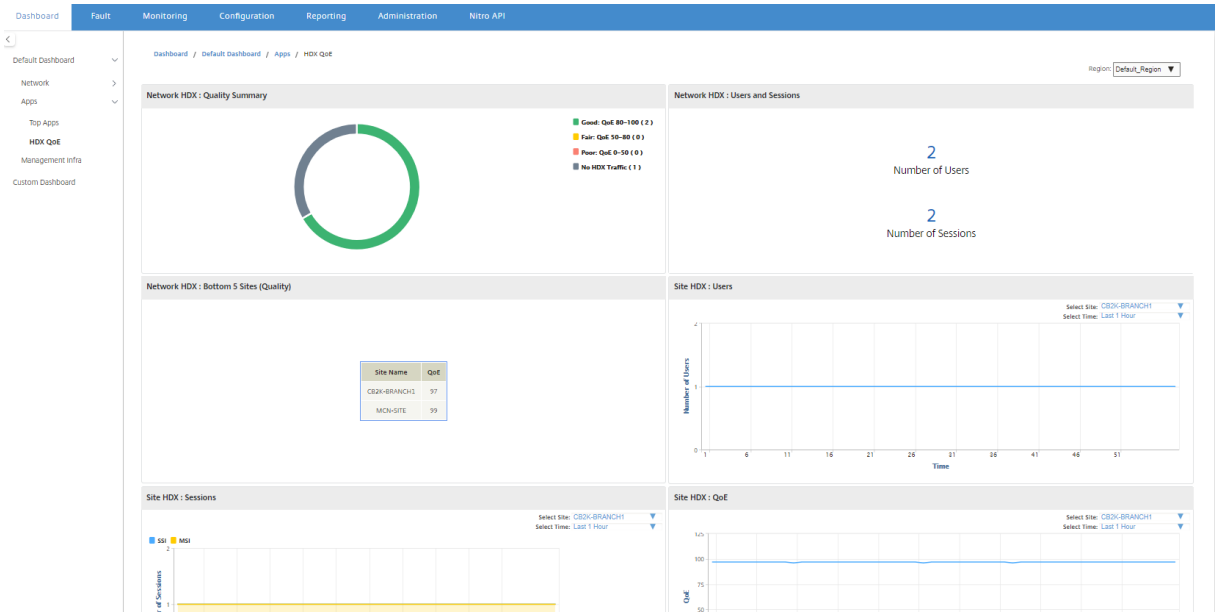


You can view the following HDX QoE metrics for the individual regions.

- Network HDX: Quality Summary
- Network HDX: Users and Sessions
- Network HDX: Bottom five Sites (Quality)
- Site HDX: Users
- Site HDX: Sessions
- Site HDX: Quality of Experience

To view HDX QoE statistics, navigate to **Dashboard** > **Default Dashboard** >**Apps > HDX QoE** and in the **Region** drop-down menu select a region.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



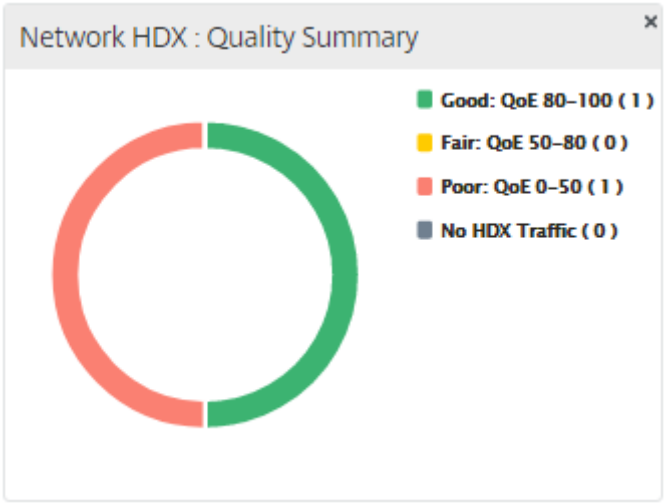
> **Note**
>
> Sometimes, the HDX dashboard data and HDX reports from different sites might not seem to be in-sync because each site statistic is polled independently.
>
> On HDX dashboard widgets, you might see a site with no HDX traffic, but there might be a non-zero number of HDX sessions and users. It happens when the HDX sessions remain idle for that polling period and still stay in open state.

Network HDX: Quality summary

The HDX traffic is classified into the following quality categories:

Quality	QoE Range
Good	80–100
Fair	50–80
Poor	0–50
No HDX Traffic	N/A

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

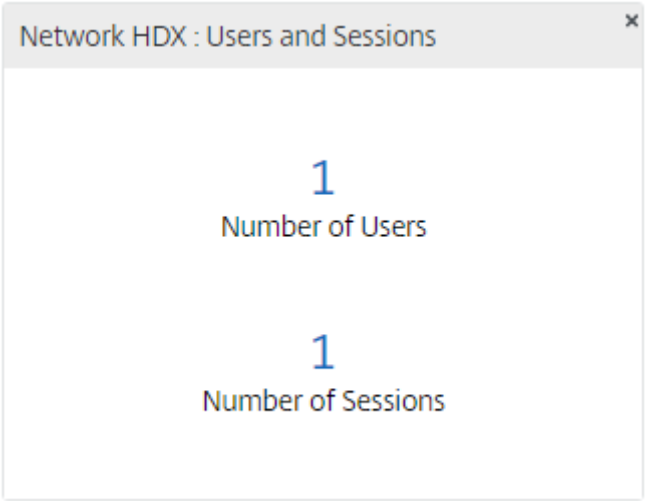


You can click the chart to view HDX reports per site. For more information, see How to View HDX Reports.

Network HDX: Users and Sessions

This widget provides information on the number of active HDX users and sessions. The number of sessions is the total number of active Single Session ICA (SSI) and Multi-Session ICA (MSI) sessions.

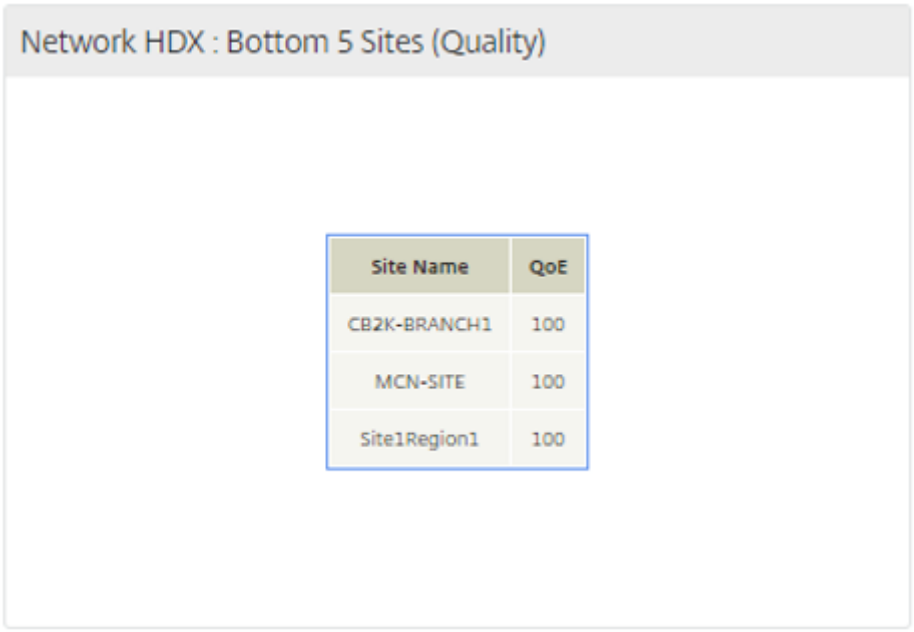
> **Note**
>
> In the current release, the number of users is not based on distinct user names. That is, two sessions started by a single user on two different machines is counted as two users.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

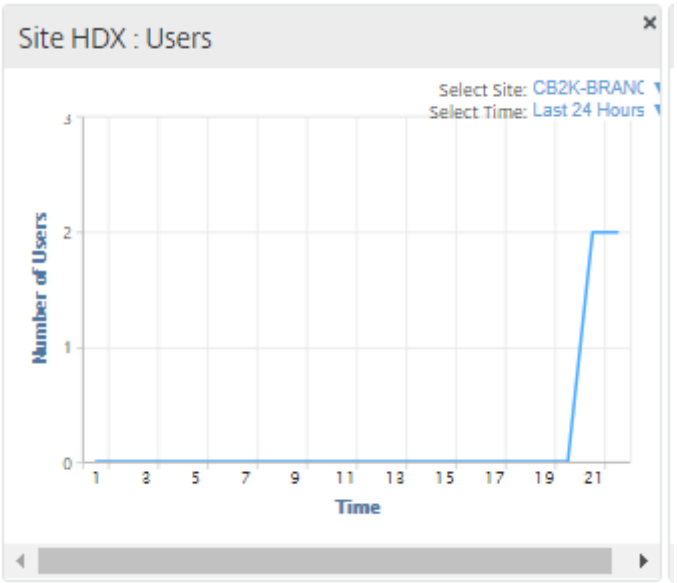
Network HDX: Bottom 5 Sites (Quality)

This widget provides a list of the bottom 5 sites that have the least QoE score. It helps drive better end-user experience initiatives.



Site HDX: Users

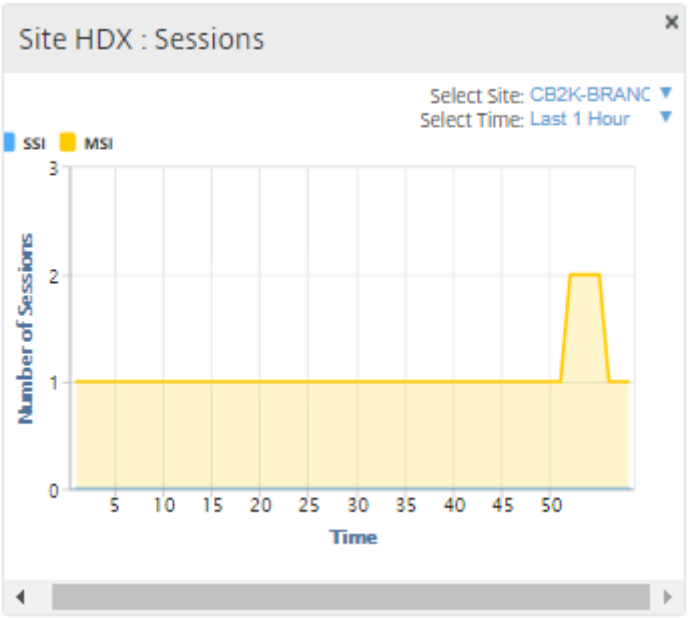
This widget provides a graphical representation of the number of users that were active at a particular site for the selected time interval. You can select the site and the time interval as last 24 hours, last 1 hour, or last 5 minutes.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Site HDX: Sessions

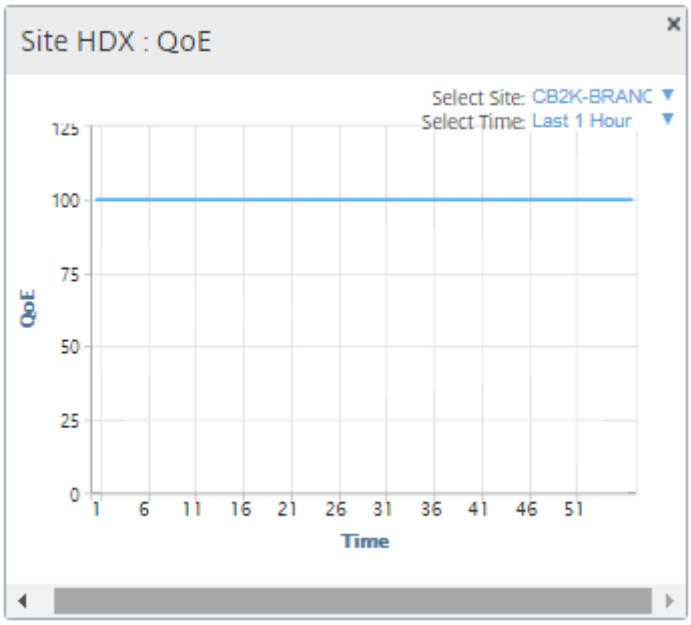
This widget provides a graphical representation of the number of MSI and SSI sessions that are active at a particular site for the selected time interval. You can select the site and the time interval as last 24 hours, last 1 hour, or last 5 minutes.



Site HDX: Quality of experience

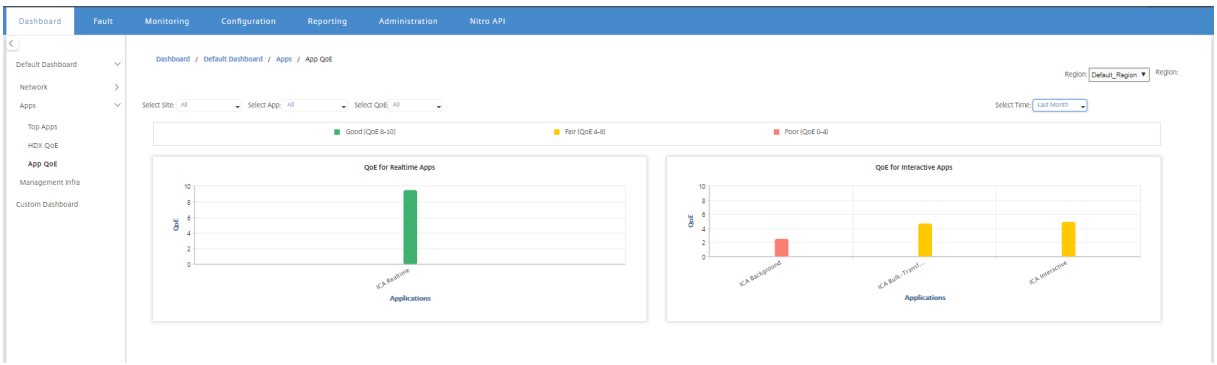
This widget provides a graphical representation of the overall QoE at a particular site for the selected time interval. You can select the site and the time interval as last 24 hours, last 1 hour, or last 5 minutes.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Application QoE

Application QoE is a measure of Quality of Experience for an application. The Application QoE score range is 0–10, where 10 represents excellent quality and 0 represents poor quality. For more information, see Application QoE. You can view application QoE score for real-time and interactive traffic.



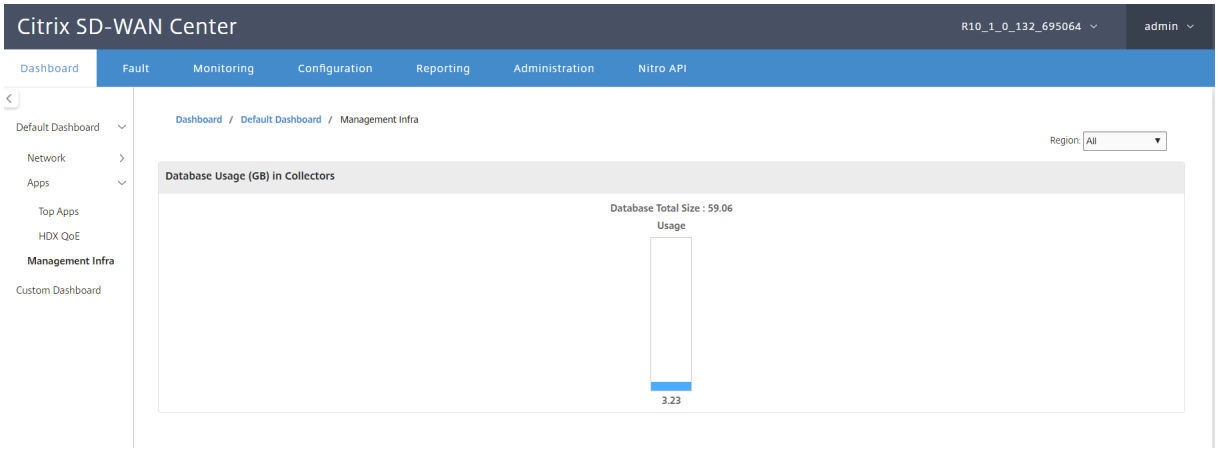
You can filter the application QoE statistics by site, application, or QoE type.

Management infra

The Management Infra page allows you to view the Citrix SD-WAN Center database usage and storage statistics.

For a multi-region deployment, you can view the database usage of all the collectors in the network. To view multi-region database statistics, navigate to **Dashboard** > **Default Dashboard** > **Management Infra** and in the **Region** drop-down menu select **All**.

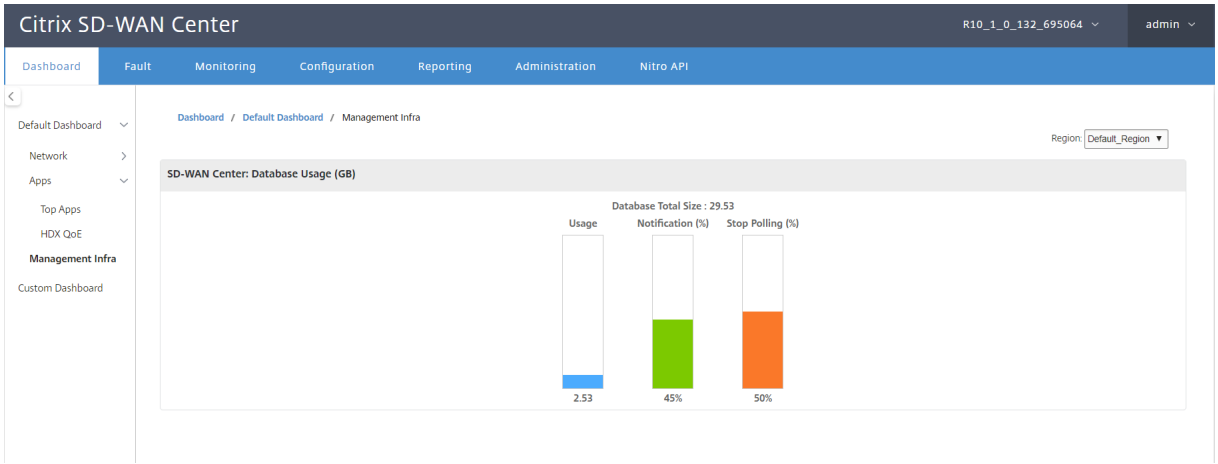
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



To view Citrix SD-WAN Center database statistics for a particular region, navigate to **Dashboard** > **Default Dashboard** > **Management Infra,** and in the **Region** drop-down menu select a region.

The **Database Usage** section displays a graphical overview of the database resource usage and the thresholds for sending notifications, or halting the collection of data. You can click the graph to view the details on the Database Maintenance page.

- **Usage**: Database capacity currently being used, in GB.
- **Notification**: Threshold for generating a database usage notification. The threshold is a percentage of the maximum size of the database. If an email alert is configured, an email notification is sent when the size of the database exceeds this threshold. For more information, see Event notifications.
- **Stop Polling**: Threshold for halting statistics polling. The threshold is a percentage of the maximum size of the database. Polling stops when the size of the database exceeds this threshold. For more information, Manage database.

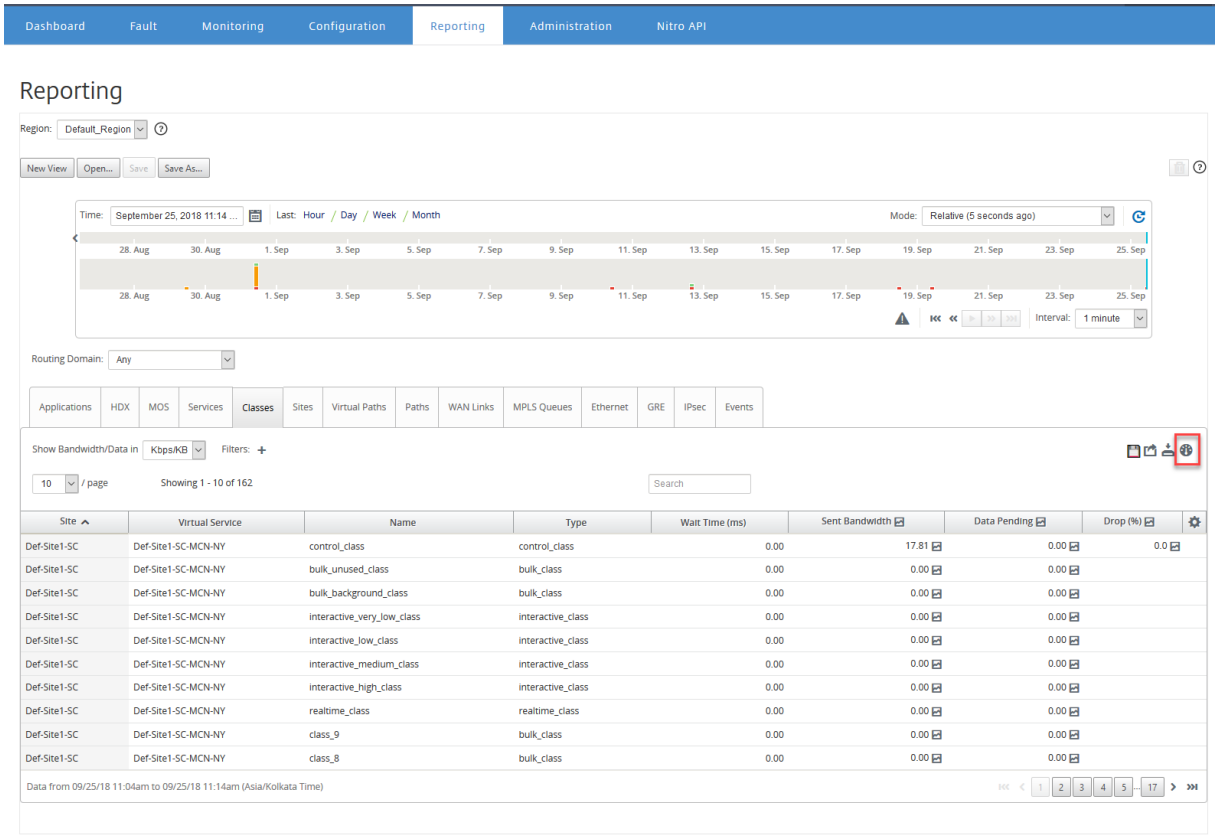


© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Custom dashboard

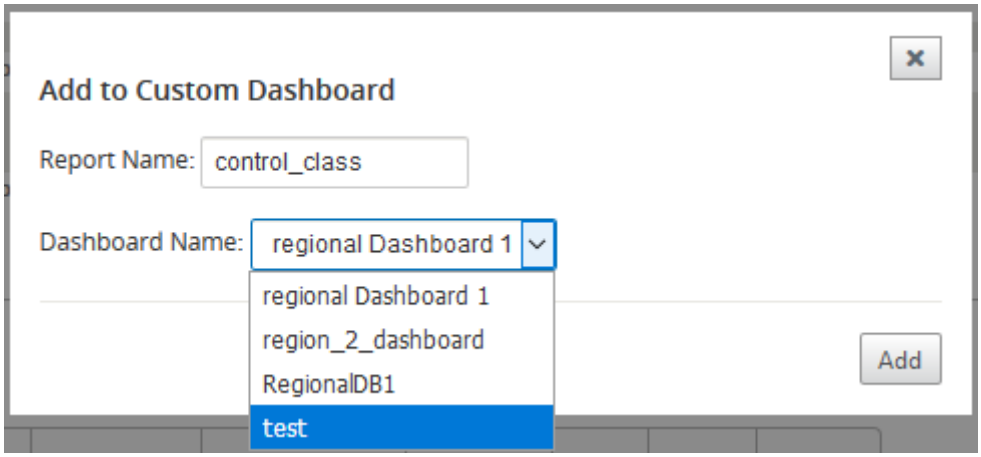
You can customize the Citrix SD-WAN Center dashboard and choose the statistics that you want to view on the dashboard based on your analytical needs. Create a custom dashboard of regional details or a global summary. You can also customize an existing report.

> **Note**
>
> You can now pin a report as widget to your custom dashboard, by using the **Add to Dashboard** option on the Reports page.



Enter the report name and select the custom dashboard.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



For Regional Details custom dashboard, you can choose from the following region level widgets:

- Site Summary
- Virtual Path
- Region Events
- Region Alarm Summary
- Inventory Manager (Per Region)
- Top Sites Per Region
- Paths
- MPLS Queues
- Ethernet
- LAN GRE Tunnels
- IPsec Tunnels
- Service Summary
- Classes
- Site Events
- Top Applications Per Region
- Top Application Family Per Region
- Site HDX: Users
- Site HDX: Sessions
- Site HDX: QoE
- MOS Applications
- Database Usage

For a Global Summary custom dashboard, you can choose from the following network level widgets:

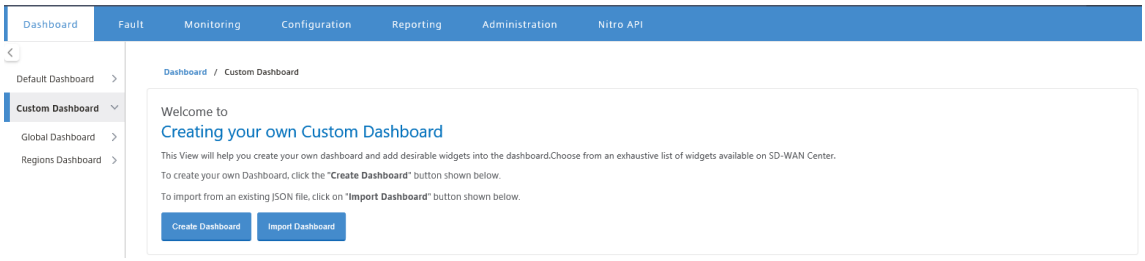
- Multi-region Summary
- Virtual Path Health in Network
- Events

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- Alarm Summary
- Inventory Manager
- Top Sites in Network
- Network HDX
- Database Usage in Collectors
- Top Applications
- Top Application Families

To create a custom dashboard:

1. Navigate to **Dashboard** > **Custom Dashboard** and click **Create Dashboard**.



> **Note**
>
> You can also import an existing dashboard in JSON format by clicking **Import Dashboard**.

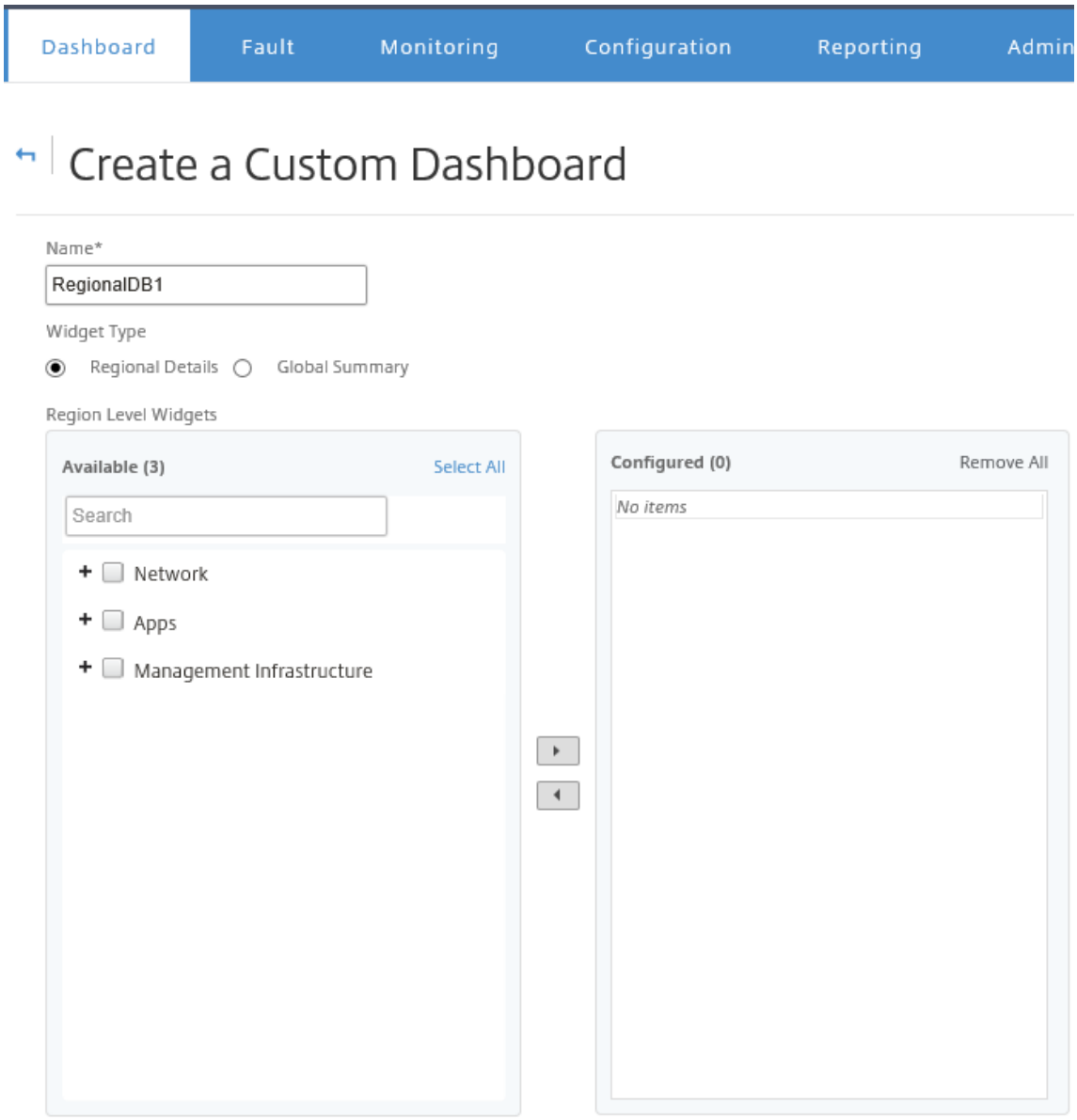
2. In the **Name** field, enter a name for the custom dashboard.
3. Select the widget type. Select **Global Summary** to view network level widgets, select **Regional Details** to view regional level widgets.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

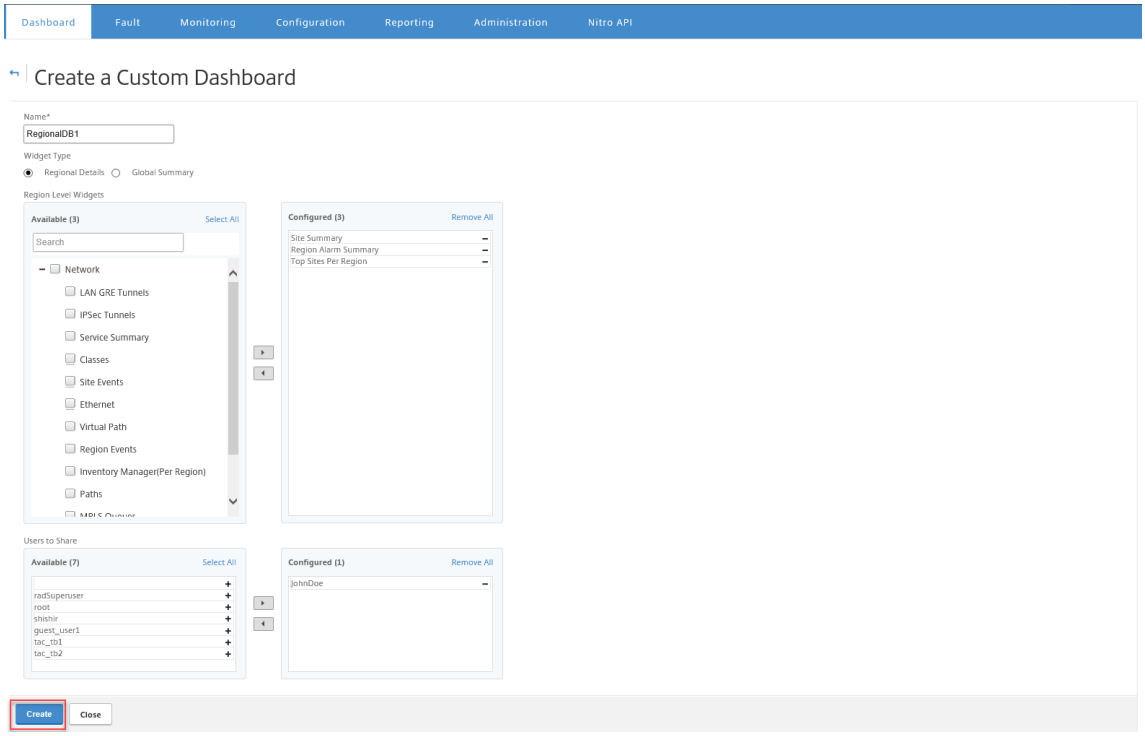
4. Click **Add** and select the required widgets.

   The widgets are categorized into three levels: Network, Apps, and Management Infrastructure.



> Note
>
> In single-region deployment, only the **Region Level Widgets** are available.

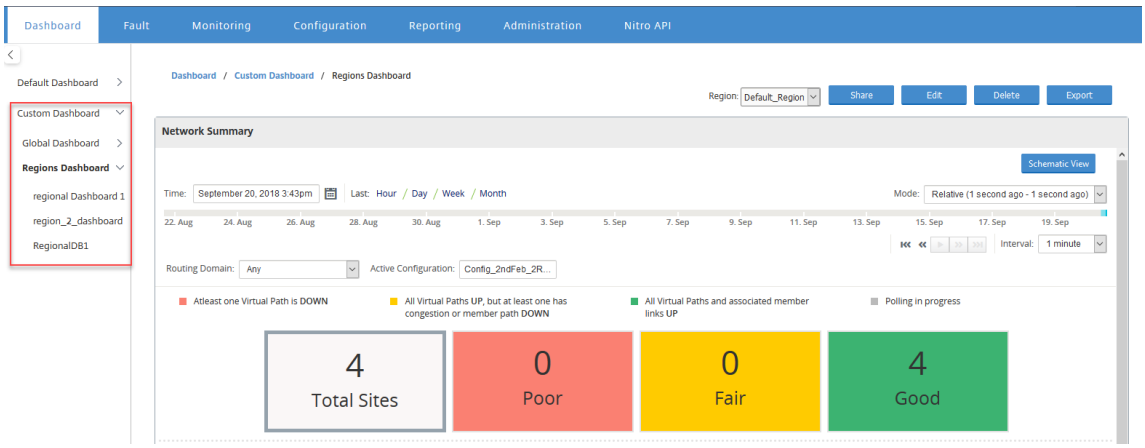
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



You can also share the custom dashboard with multiple users. For more information on users, see User accounts.

5. Click **Create**. The newly created custom dashboard is listed under **Custom Dashboard**.

> **Tip**
>
> You can edit or delete the custom dashboard.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Diagnostic packages

March 12, 2021

A diagnostic package consists of all of the system log files, system information, and other necessary details that will assist the Citrix SD-WAN Support team in diagnosing and resolving issues with your system.

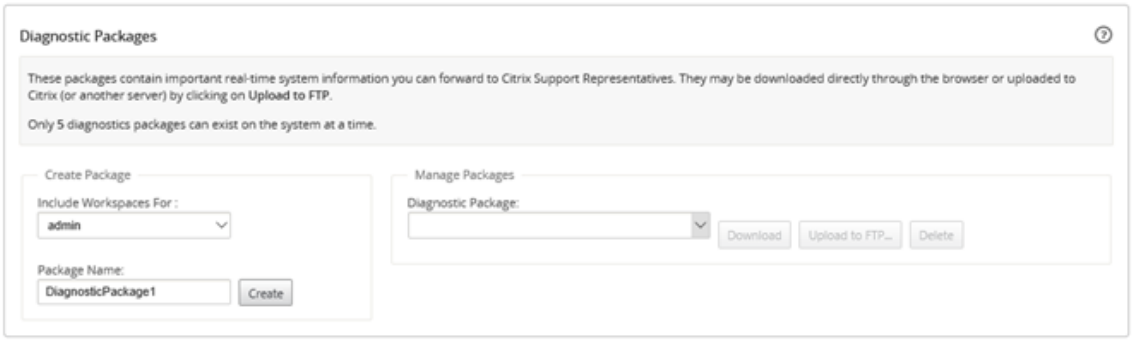
After creating the package you can download it to your computer and then mail the diagnostic package to Citrix Customer Support or you can directly upload it to the Citrix Customer Support sever (or another server).

> **Note**
>
> Citrix SD-WAN Center can store a maximum of five diagnostic packages at a time.

To create a diagnostic package:

1. In the Citrix SD-WAN Center web interface, click the **Monitoring** tab and then click **Diagnostics**.
2. In the **Diagnostics Packages** section, under **Create Package**, from the **Include Workspaces For** drop-down list select a user whose workspaces will be copied into the diagnostics.

   > **Note**
   >
   > The diagnostics package will include the five configurations most recently modified by the selected user.

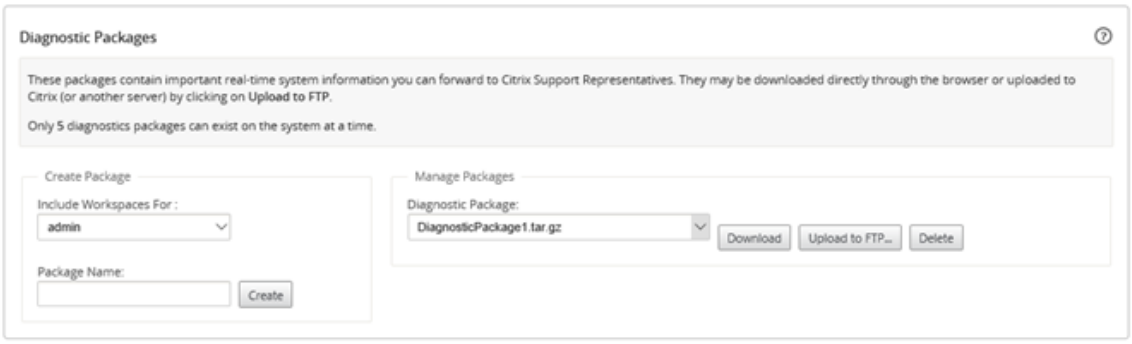


3. In the **Package Name** field, enter a name for the diagnostic package.
4. Click **Create**. This runs a system diagnostics and generates a diagnostic package.

To download a diagnostic package:

1. In the **Diagnostics Packages** section, under **Manage Package**, from the **Diagnostic Packages** drop-down list select the package that you want to download.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



2. Click **Download**. The diagnostic package is downloaded to your local computer.

To upload a diagnostic package to an FTP server:

1. In the **Diagnostics Packages** section, under **Manage Package**, from the **Diagnostic Packages** drop-down list select a package that you want to upload.
2. Click **Upload to FTP**. This opens the **Upload to FTP Server** dialog box for specifying your FTP authentication information and uploading the package to the Citrix Customer Support FTP server, or to another FTP host.

3. In the **Customer Name** field, enter a name to assist Citrix SD-WAN Support in identifying the diagnostic packages.
   A directory with this name will be created on the Citrix FTP server, and your files will be uploaded to that location.
4. In the **FTP Host** field, enter the IP address or host name (if DNS is configured) of the FTP server.
5. In the **Username** field, enter a user name to be used to log onto the FTP server.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

6. In the **Password** field, enter the password associated with the user name.
7. Click **Upload**.

> **Note**
>
> It is recommended to periodically delete old diagnostic packages, to prevent exceeding the limit for the maximum allowable packages. To delete an existing diagnostic package, select a diagnostic package from the **Diagnostic Package** drop-down list, and then click **Delete**.

Events

March 12, 2021

Citrix SD-WAN Center collects event information from all the discovered appliances in the network. This event information can be filtered and viewed in the **Event Viewer** page.

The event details include the following information.

- **Time:** The time the event was generated.
- **Site:** The name of the site on which the event originated.
- **Appliance ID:** Shows whether the appliance from which the event originated is a primary (**0**) or secondary (**1**) appliance.

  > **Note**
  >
  > The Appliance ID column is hidden by default. To display the column, click **Show/Hide** (gear icon) and select the **Appliance ID** checkbox from the drop-down menu

- **Object Name:** The name of the object generating the event.
- **Object Type:** The type of object generating the event.
- **Severity:** The severity level of the event.
- **Previous State:** The state of the object before the event. The state will be listed as **unknown** if not applicable.
- **Current State:** The state of the object at the time of the event.
- **Description:** A text description of the event.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

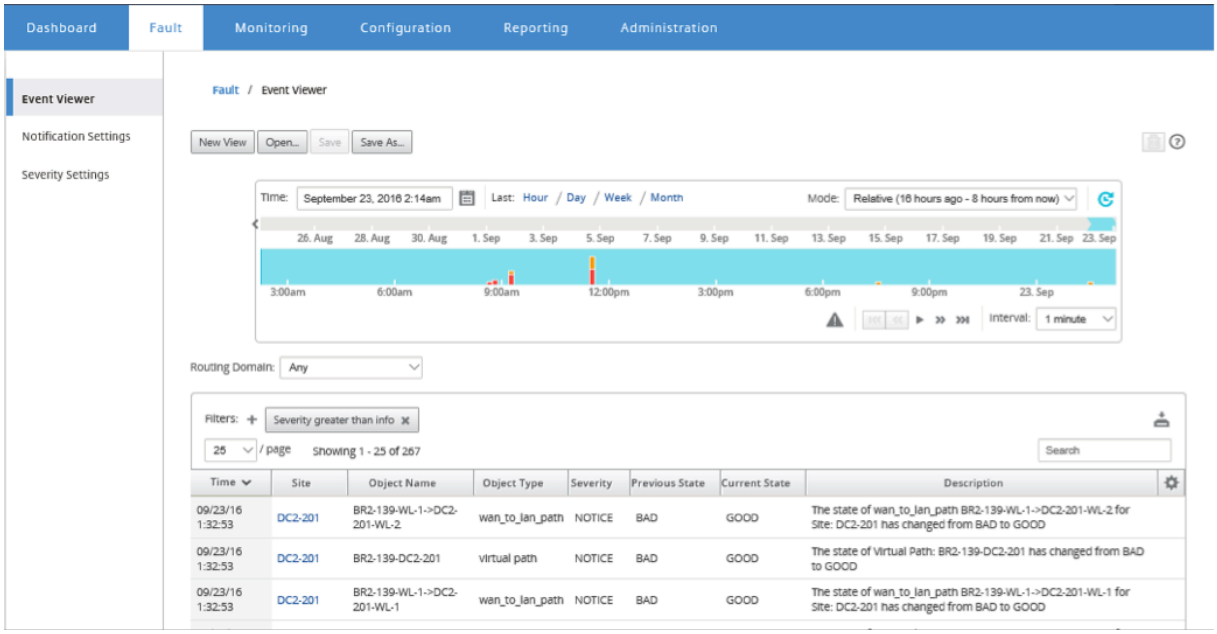
Viewing events

You can view the events, filter it and download it from the Event Viewer page.

To access the event viewer page.

In the Citrix SD-WAN Center web interface, click the **Fault** tab.

The Event Viewer page appears by default.



You can select and view reports of a particular period by using the timeline controls. For more information, see, Timeline controls.

> **Note**
>
> You can view the events data of last 30 days. Any data beyond this period is automatically removed from the SD-WAN Center collector and the respective regional collectors.

You can also create, save and open report views. For more information, see, Manage views.

Using Filters

You can create custom filters for narrowing the Events table results.

To create and apply a filter:

1. Click **+** icon to the right of the **Filters** section label.
2. Select a category form the drop-down menu.

   The options available are:

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- Size
- Object Name
- Object Type
- Severity
- Previous State
- Current State

3. Select an operator from the middle drop-down menu.

   The options are as follows:

   - is
   - is not
   - is one of
   - contains
   - does not contain
   - less than
   - less than or equal to
   - greater than
   - greater than or equal to

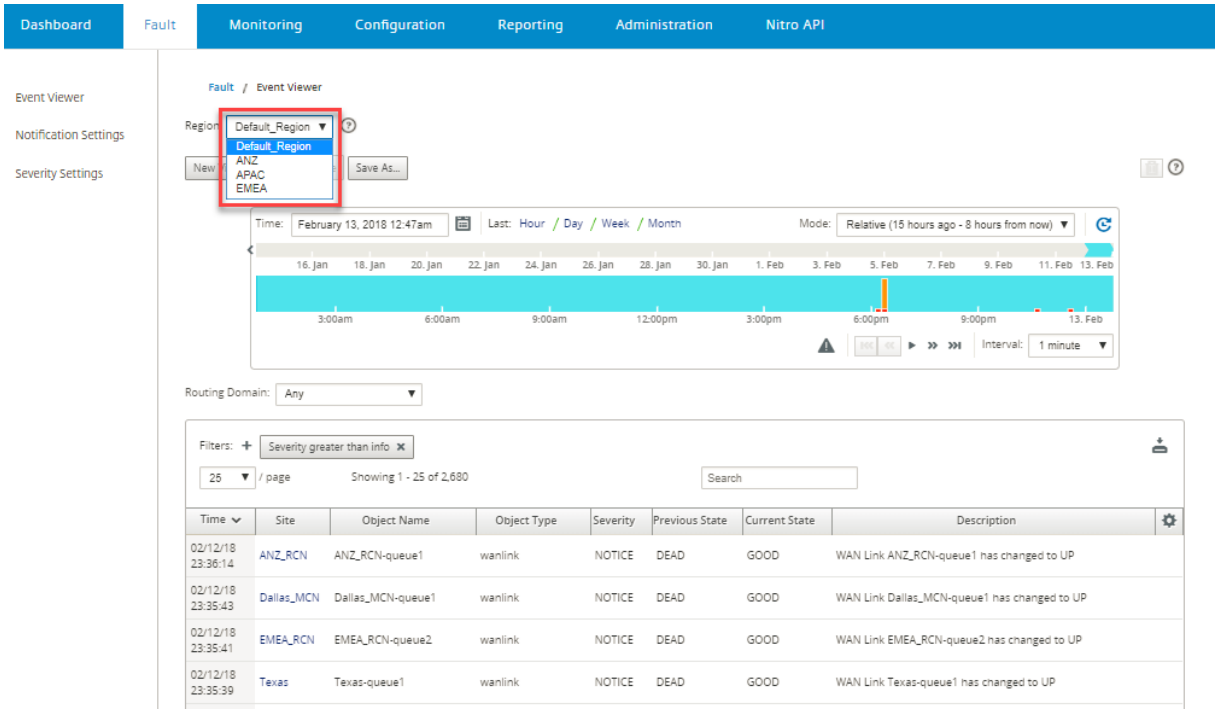
4. Enter the string or value by which to delimit the filter.

> **Note**
>
> This field is case sensitive.

> **Note**
>
> You can create and apply multiple filters.
> For Multi-region network, you can select specific regions to view event.

The events data is fetched from the respective region's collector.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



> **Note**
>
> In single-region network deployment, the **Region** drop-down list is not available.

To download the events table as a CSV file:

Click the Download icon at the upper right corner of the events table.

For more information on event statistics, see Event report.

You can configure Citrix SD-WAN Center to send external event notifications for different event types as email, SNMP traps or syslog messages. For more information, see Event notifications.

Event notifications

March 12, 2021

You can configure Citrix SD-WAN Center to send event notifications for different event types as email, SNMP traps or syslog messages. Once you have configured the email, SNMP and syslog notification settings you can select the severity for different event types and select the mode (email, SNMP, syslog) to send event notifications. Notifications are generated for events equal to or above the specified severity level for the event type.

The available severity levels are as follows, in descending order of severity:

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

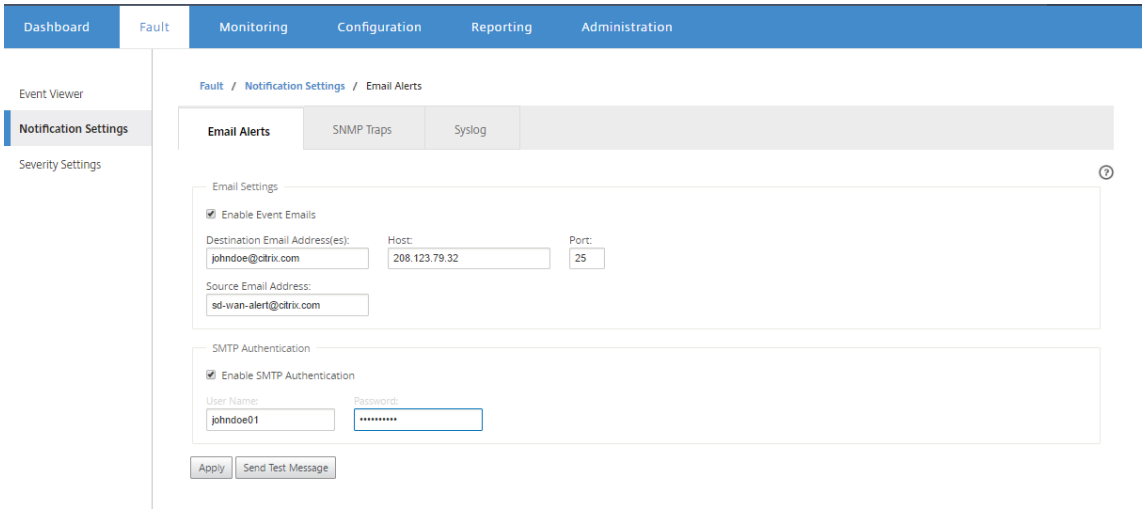
- EMERGENCY
- ALERT
- CRITICAL
- ERROR
- WARNING
- NOTICE
- INFORMATIONAL
- DEBUG

> **Tip**
>
> You can configure notification settings to receive event alerts by email, SNMP traps or Syslog messages on both Citrix SD-WAN Center and the individual Citrix SD-WAN appliances in your network.
>
> However, enabling notifications on Citrix SD-WAN Center allows you to receive event notifications for the entire Citrix SD-WAN network (i.e., MCN and all the sites). While, enabling notifications on the Citrix SD-WAN appliances allows you to receive notifications from the individual appliances only.
>
> It is advised to enable notifications on the Citrix SD-WAN Center only, to avoid redundant notifications from the other Citrix SD-WAN appliances in your network.

Configuring email notification settings

To configure email notification settings:

1. In the Citrix SD-WAN Center web management interface, navigate to **Fault** > **Notification Settings** > **Email Alerts.**



2. Select **Enable Event Emails**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

3. In the **Destination Email Address (es)** field, enter the email address to which alert notifications are to be sent.

   > **Note**
   >
   > You can enter multiple email addresses separated by semicolons.

4. In the **Host** field, enter the IP Address or hostname of an external SMTP server to relay email messages to the internet.
5. In the **Port** field, enter the port number to be used for the SMTP connection. The default port is 25.
6. In the **Source Email Address** field, enter the email address from which email alerts are sent.
7. Select **Enable SMTP Authentication**.
8. In the **User Name** field, enter a user name for the SMTP server used for authentication.
9. In the **Password** field, enter the password associated with the user name for the SMTP server used for authentication.

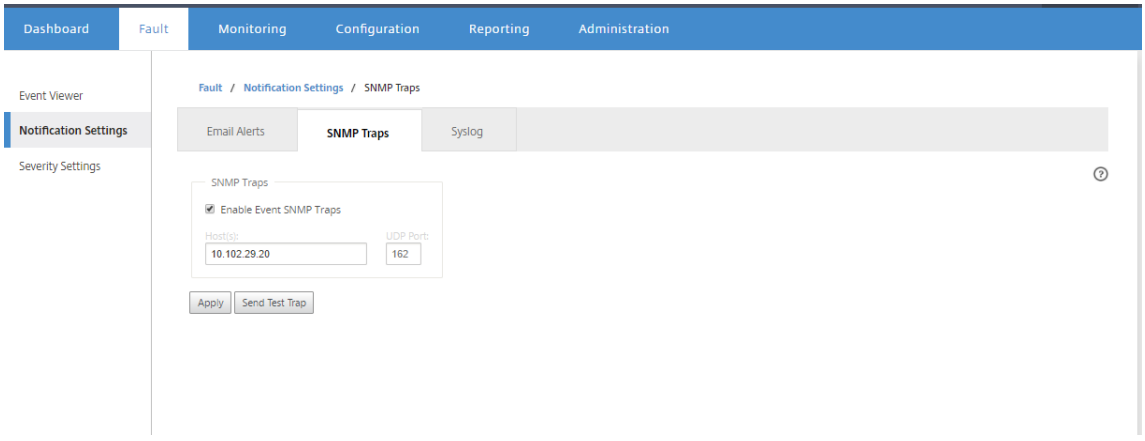
   > **Note**
   >
   > Click **Send Test Message,** to send a sample email alert to the configured recipients.

10. Click **Apply**.

Configuring SNMP trap notification settings

To configure SNMP trap notification settings:

1. In the Citrix SD-WAN Center web management interface, navigate to **Fault** > **Notification Settings** > **SNMP Traps**.
2. Select **Enable Event SNMP Traps.**



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

3. In the **Host(s)** field, enter the IP address or the host name of an external SNMP system. This host will receive the events as SNMP traps.

   > **Note**
   >
   > You can enter multiple IP addresses or hostnames separated by semicolons.

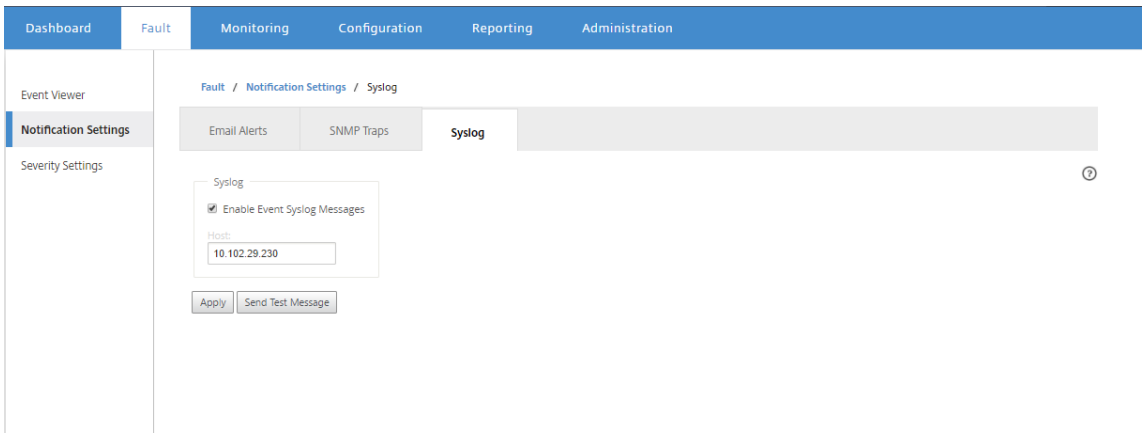
4. In the **UDP Port** field, enter the UDP port to be used to send the SNMP traps. By default, the UDP port is set to 162.
5. Click **Apply** to apply the SNMP traps notification settings.

   > **Note**
   >
   > Alternately, click **Send Test Trap** to verify whether the system is able to send an SNMP trap to the configured destination.

Configuring syslog notification settings

To configure Syslog notification settings:

1. In the Citrix SD-WAN Center web management interface, navigate to **Fault** > **Notification Settings** > **Syslog**.
2. Select **Enable Event Syslog Messages.**



3. In the **Host** field, enter the IP address or the host name of an external syslog server, which will be used to receive events as syslog messages.
4. Click **Apply** to apply the syslog notification settings.

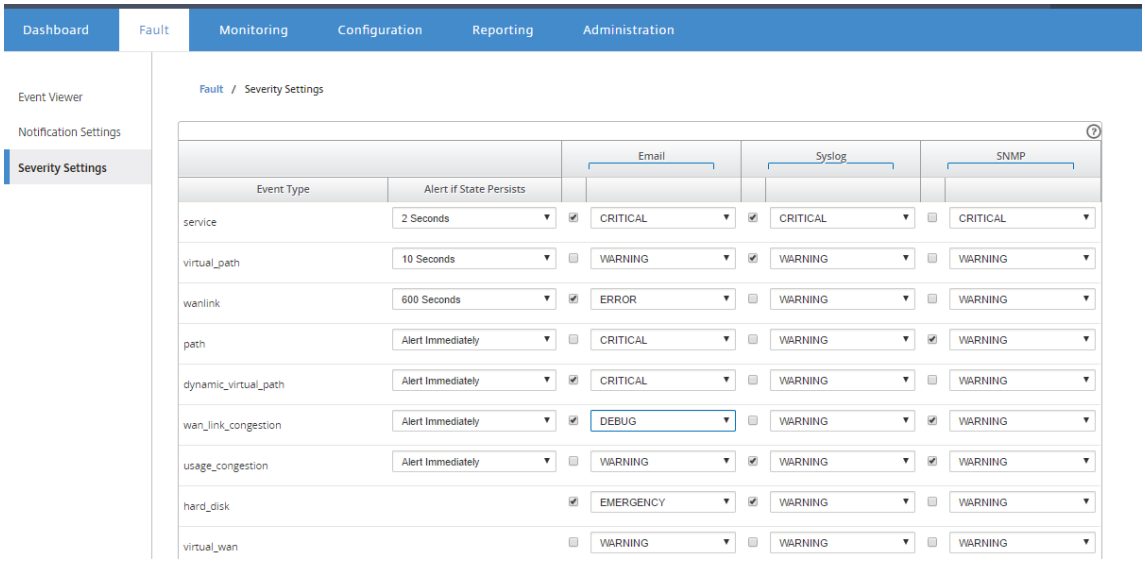
   > **Note**
   >
   > Alternately, click **Send Test Message** to verify whether the system can send a syslog message to the configured host.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Configuring event notifications

To configure event notifications:

1. In the Citrix SD-WAN Center web management interface, navigate to **Fault** > **Severity Settings**.
2. In the **Alert if Sate Persists** field, select the time duration after which if the event still persists a notification will be sent.



3. For each event type select the notification option and select the severity.

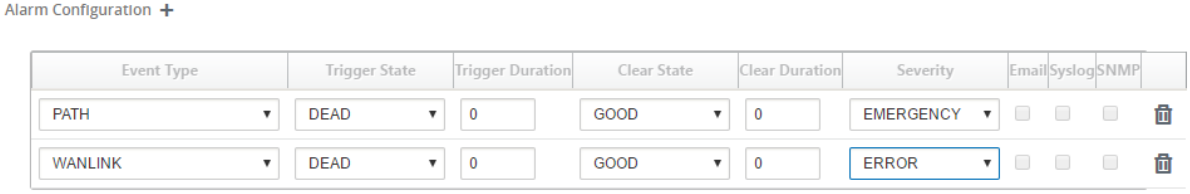
> **Note**
>
> The Email, Syslog and SNMP notification options will be enabled only after configuring the respective notification settings.

4. Click **Apply**.

Configuring alarms

You can also configure alarms in Citrix SD-WAN Center and push it to individual appliances.

To configure alarm in Citrix SD-WAN Center, navigate to **Configuration** > **Appliance Settings** > **Notification Settings** > **Alarm Configuration** and Click **+**.



Select or enter values for the following fields:

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- **Event Type**: The Citrix SD-WAN appliance can trigger alarms for particular subsystems or objects in the network, these are called event types. The available event types are SERVICE, VIRTUAL_PATH, WANLINK, PATH, DYNAMIC_VIRTUAL_PATH, WAN_LINK_CONGESTION, USAGE_CONGESTION, FAN, POWER_SUPPLY, PROXY_ARP, ETHERNET, DISCOVERED_MTU, GRE_TUNNEL, and IPSEC_TUNNEL.
- **Trigger State:** The event state that triggers an alarm for an Event Type. The available Trigger State options depend on the chosen event type.
- **Trigger Duration**: The duration in seconds, this determines how quickly the appliance triggers an alarm. Enter '0'to receive immediate alerts or enter a value between 15-7200 seconds. Alarms are not triggered, if additional events occur on the same object within the Trigger Duration period. Additional alarms are triggered only if an event persists longer than the Trigger Duration period.
- **Clear State**: The event state that clears an alarm for an Event Type after the alarm is triggered. The available Clear State options depend on the chosen Trigger State.
- **Clear Duration:** The duration in seconds, this determines how long to wait before clearing an alarm. Enter '0'to immediately clear the alarm or enter a value between 15-7200 seconds. The alarm is not cleared, if another clear state event occurs on the same object within the specified time.
- **Severity**: A user-defined field that determines how urgent an alarm is. The severity is displayed in the alerts sent when the alarm is triggered or cleared and in the triggered alarm summary.
- **Email**: Alarm trigger and clear alerts for the Event Type is sent via email.
- **Syslog**: Alarm trigger and clear alerts for the Event Type is sent via Syslog.
- **SNMP**: Alarm trigger and clear alerts for the Event Type is sent via SNMP trap.

Memory dumps

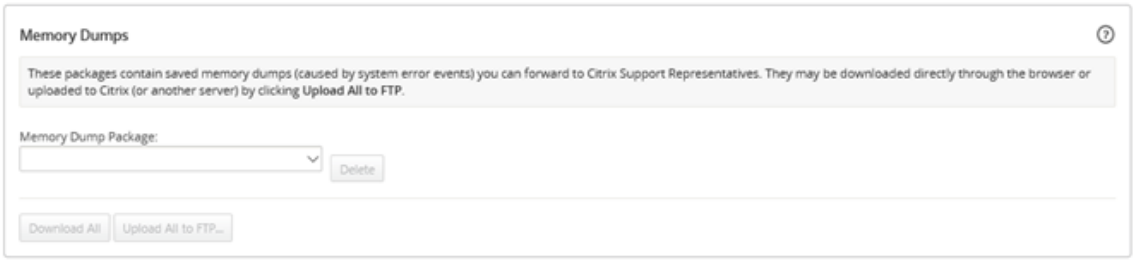
March 12, 2021

A memory dump is generated when a process crashes. All memory dumps currently on the system can be downloaded in one combined package, and uploaded to an FTP server for examination by the Citrix support team. However, you can delete individual memory dumps.

To download memory dumps:

1. In the Citrix SD-WAN Center web interface, click the **Monitoring** tab and then click **Diagnostics**.
2. In the **Memory Dumps** section, from the **Memory Dump Package** drop-down list select a memory dump package.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



3. Click **Download All**. Save the memory dump package on your local computer.

To upload a memory dump package to an FTP server:

1. In the **Memory Dumps** section, from the **Memory Dump Package** drop-down list select a memory dump package.
2. Click **Upload to FTP Server**. This opens the **Upload All to FTP** dialog box for specifying your FTP authentication information and uploading the package to the Citrix Customer Support FTP server, or to another FTP host.

3. In the **Customer Name** field, enter a name to assist Citrix SD-WAN Support in identifying the diagnostic packages.

   A directory with this name will be created on the Citrix FTP server, and your files will be uploaded to that location.
4. In the **FTP Host** field, enter the IP address or host name (if DNS is configured) of the FTP server.
5. In the **Username** field, enter a user name to be used to log onto the FTP server.
6. In the **Password** field, enter the password associated with the user name.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

7. Click **Upload**.

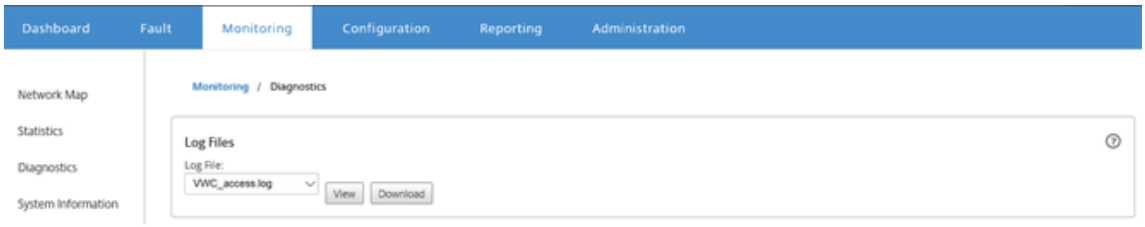
Log files

March 12, 2021

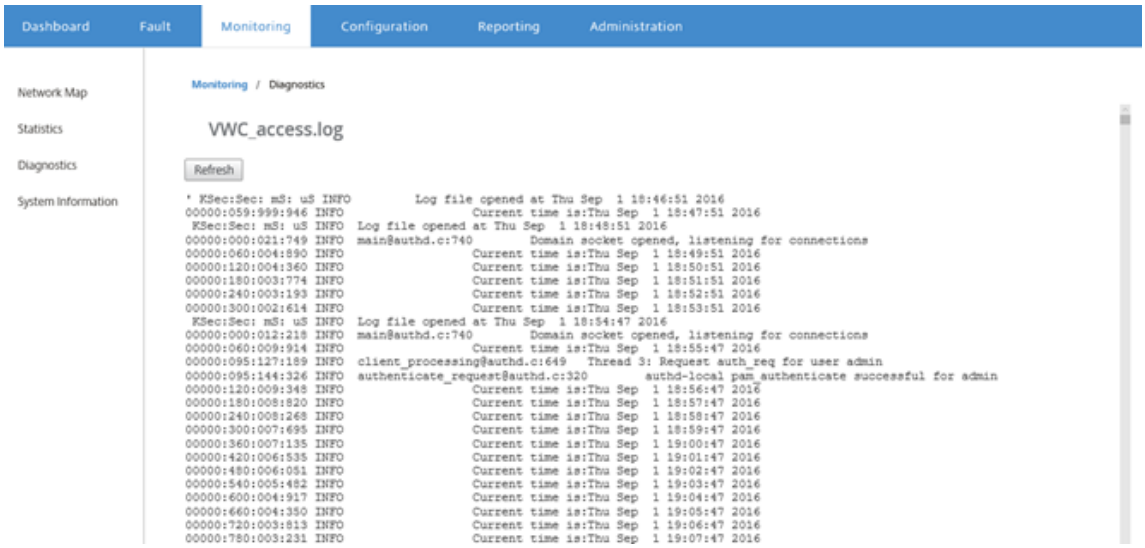
The Log files collect information related to the web console, user interface exceptions, internal crashes and so on. These logs can be used to troubleshoot issues in the Citrix SD-WAN Center.

To view log files:

1. In the Citrix SD-WAN Center web interface, click the **Monitoring** tab.
2. Click **Diagnostics**.
3. From the **Log File** drop-down list, select the log file you want to view.



4. Click **View**. The log file content is displayed.



5. If you want to download the log files to your computer, click **Download**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

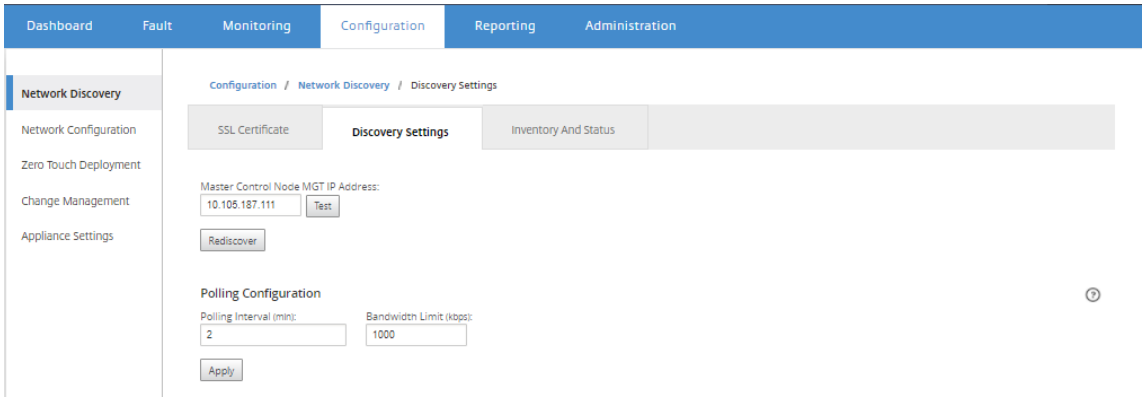
Polling interval

March 12, 2021

Polling refers to the process of collecting statistics from the discovered appliance. You can configure the interval and bandwidth limit for polling operations after discovering the appliances. For information on discovering the appliance, see Single-region network deployment or Multi-region network deployment.

To perform polling configuration:

1. In the Citrix SD-WAN Center web interface, navigate to **Configuration** > **Network Discovery** > **Discovery Settings**.



2. In the **Polling Interval** field, enter the polling frequency in minutes. The range is 2–60 minutes. The default value is 5 minutes.
3. In the **Bandwidth Limit** field, enter the polling bandwidth limit in kbps. The MCN will limit bandwidth to the specified value when transferring polling statistics from the appliance to the Citrix SD-WAN Center. The range is 100 Kbp –1 Gbps . The default value is 1 Mbps.
4. Click **Apply**.

Statistics

March 12, 2021

You can view the statistics collected by Citrix SD-WAN Center as graphs. These graphs are plotted as timeline versus usage, allowing you to understand the usage trends of various network object properties. You can view graphs for network-wide application statistics. For every site in the SD-WAN network, you can view graphs for the following network parameters:

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- Bandwidth
- QoS
- Virtual Path
- Internet Services
- Intranet Services
- Pass-through Services
- WAN Links
- Ethernet Interfaces
- GRE Tunnels
- IPsec Tunnels
- Applications
- Application Families

> **Tip**
>
> You can create views as per your requirement, save it and open existing views.

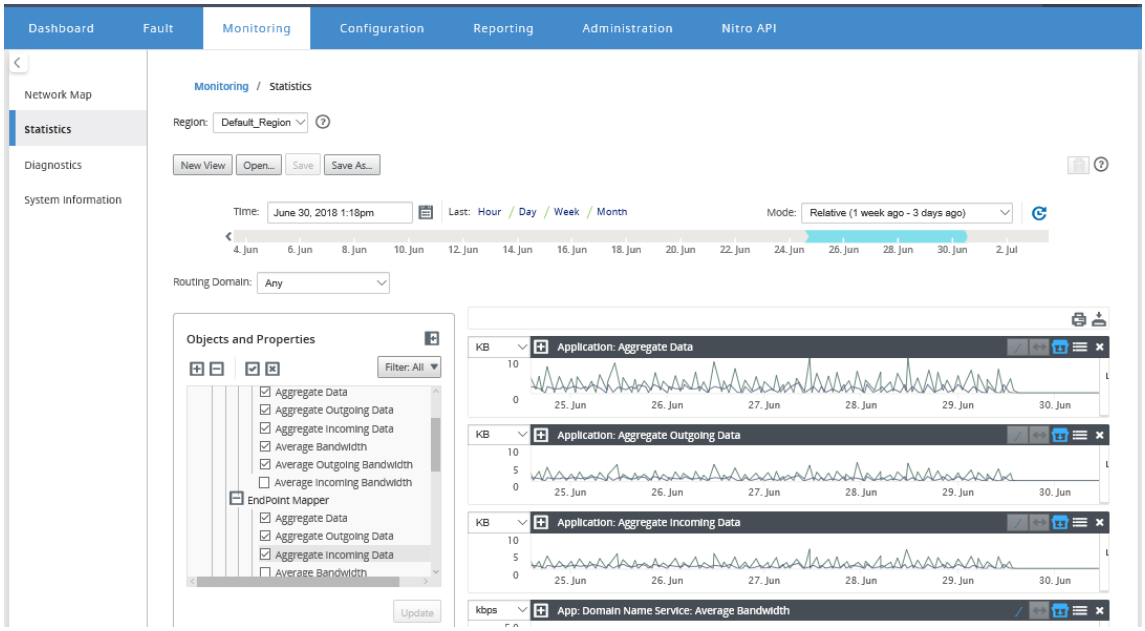
To view statistical graphs:

1. In Citrix SD-WAN Center web UI, navigate to **Monitoring** > **Statistics**.
2. Select a region and a routing domain.
3. From the **Objects and Properties** hierarchical tree, find and select the properties of interest.

   > **Tip**
   >
   > You can also use the **Filter** drop-down menu and **Presets Menu** to simplify the process of finding and selecting properties.

4. Click **Update** to display graphs for the selected properties.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



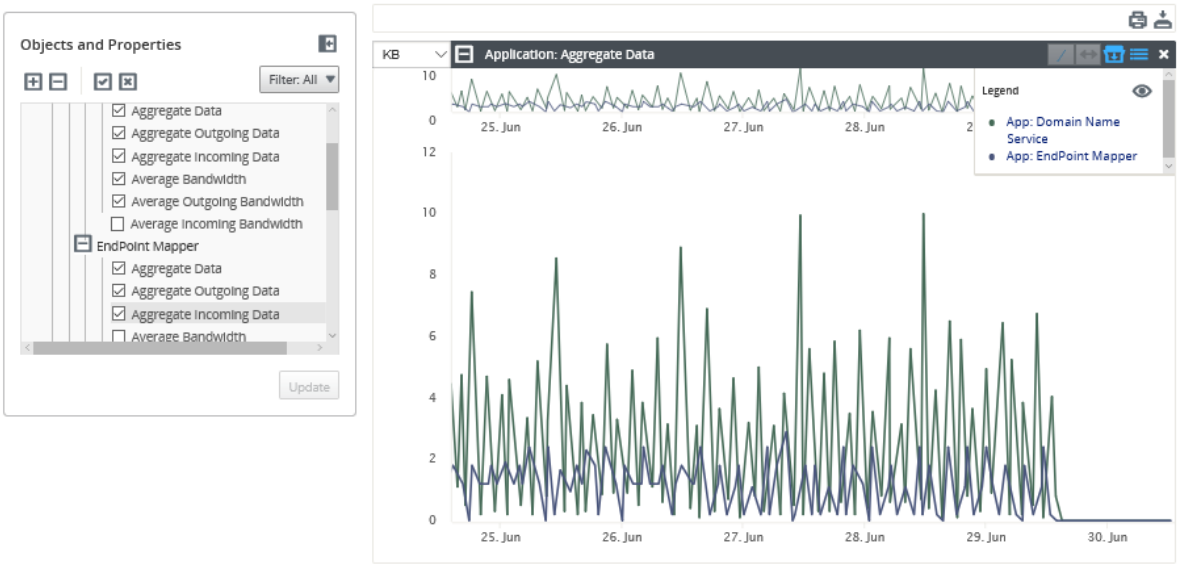
> **Tip**
>
> Deselect a property and click **Update** to remove the graph for that property from the Graphs Display area.

5. Select a period for the current view. For more information, see Timeline Controls

   The graphs are displayed based on the selected properties.

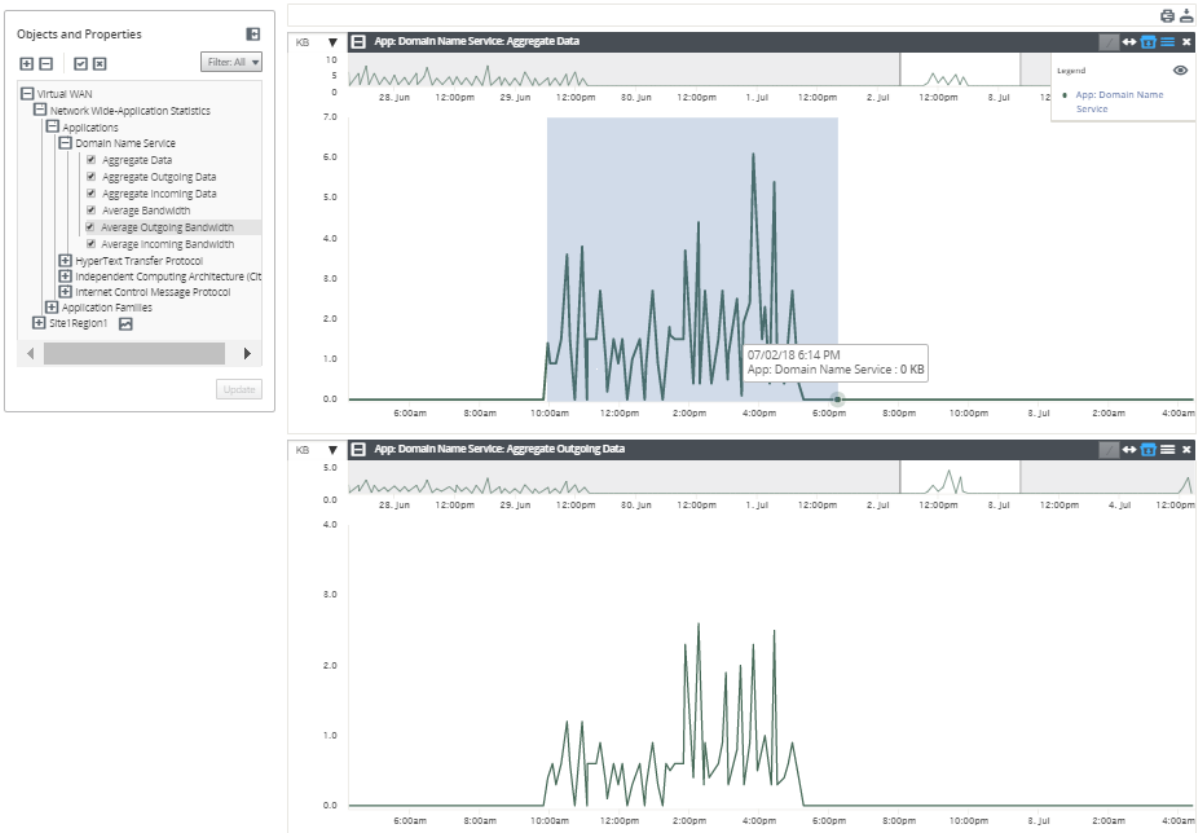
> **Tip**
>
> If you select more than one property, the graphs display in **Trend View** mode to save vertical space. Click on a graph heading to show and hide the fully expanded graph. You can also show and hide the trend view and legends on the graphs.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



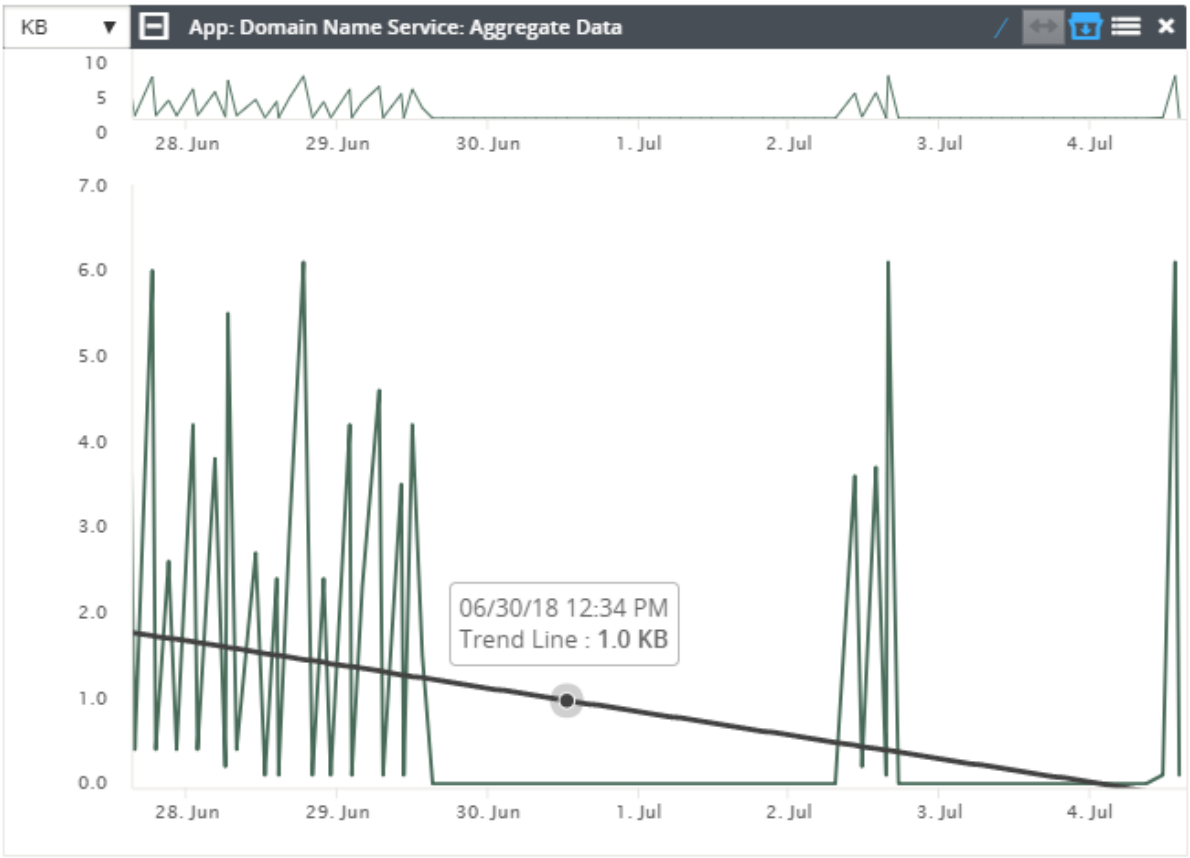
Tip

To zoom a graph, click and drag the graph plot area. Zooming on one graph zooms all graphs, to the selected time, to maintain a consistent view. Click the reset icon (↔) to reset the zoom.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> **Tip**
>
> You can show and hide the trend line by clicking the (/) icon.



> **Note**
>
> You could print the graphs, or download the graph set as a CSV file.

System information

March 12, 2021

The following information is displayed on the system information page:

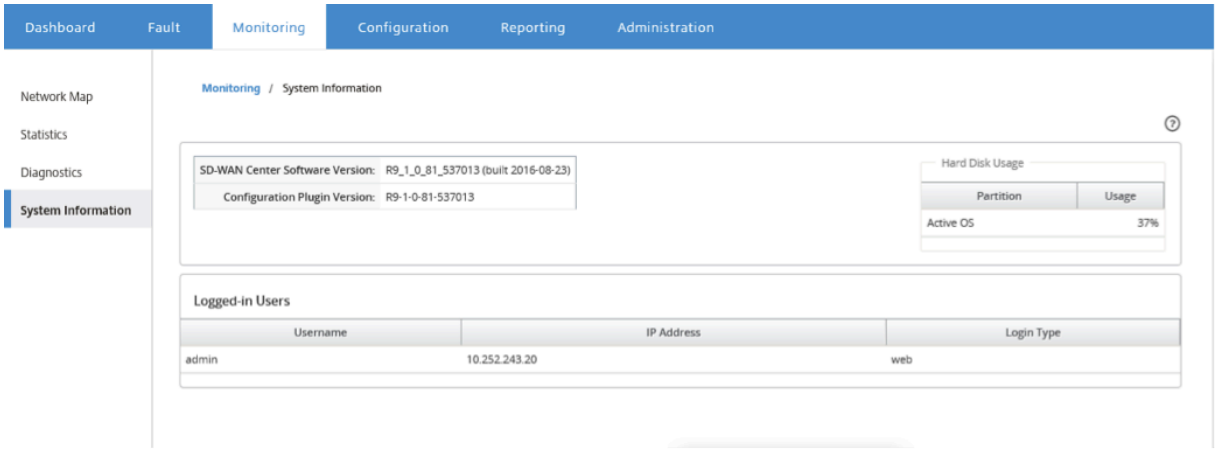
- **Citrix SD-WAN Center Software Version**: The Citrix SD-WAN Center software version currently installed and running on this virtual machine.
- **Configuration Plugin Version**: The version of the Configuration Editor Plugin currently installed and running in this Citrix SD-WAN Center virtual machine.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- **Hard Disk Usage**: The amount of hard disk space used by the operating system and data partitions.
- **Logged-in Users**: The user name, IP Address, and logon type for each user currently logged into this Citrix SD-WAN Center virtual machine.

To display the system information:

In the Citrix SD-WAN Center web interface, click the **Monitoring** tab and then click **System Information**.



Reporting

March 12, 2021

Citrix SD-WAN Center provides the following reports:

- **Applications:** Displays details about incoming traffic, outgoing traffic and total traffic of the top applications, sites, and application families.
- **HDX**: Displays detailed HDX data for every site.
- **Sites:** Displays site level statistics for every site in the Virtual WAN. Sites rows expand to show the **Services** table filtered for the Site.
- **Service:** Displays summary statistics by service type (Virtual Path, Internet, Intranet and Pass-through) for every site in the Virtual WAN. Services rows expand to show the individual Services for the Service type.
- **Virtual Paths:** Displays Virtual Path level statistics for every Virtual Path in the SD-WAN. Virtual Paths rows expand to show the Paths contained within the Virtual Path.

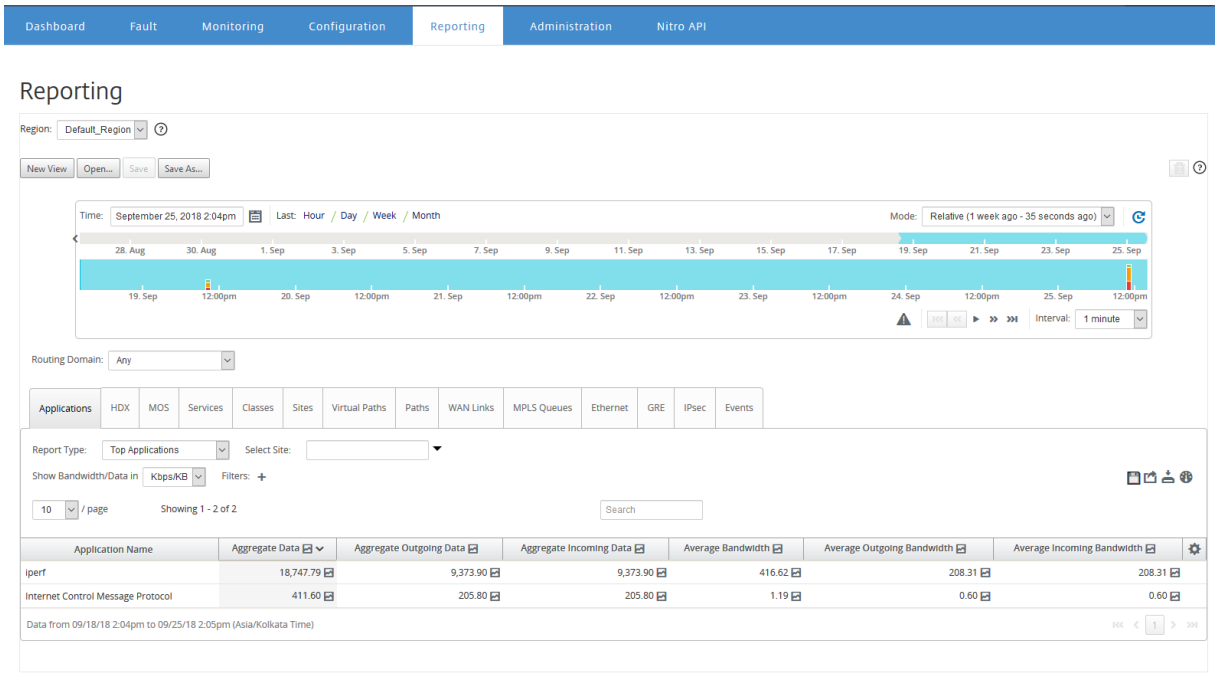
> **Note**
>
> Virtual Path data is recorded from the perspective of both endpoints, as such, each Virtual Path

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

> may have two rows identified by the Site that recorded the statistics.

- **Paths:** Displays Path level statistics for every Path in the Virtual WAN.
- **WAN Links:** Displays WAN Link level statistics for every WAN Link at each Site in the Virtual WAN. WAN Links rows expand to show a Usage Summary for each Service type for that WAN Link. Each Service type row will then expand to show usages for each Service of that type. If the WAN Link is a Private MPLS link, a second table will be shown showing the MPLS Queues for the WAN Link.
- **MPLS Queues:** The MPLS Queues rows expand to show a usage summary for each Service type for that Queue. Each Service type row will then expand to show usages for each Service of that type.
- **Classes:** Displays Class level statistics for every Class for each Virtual Path in the Virtual WAN.
- **MOS Score**: The mean opinion score (MOS) provides a numerical measure of the quality of the experience that an application delivers to end users.
- **Ethernet Interfaces:** Displays Ethernet Interface level statistics for every Interface at each Site in the Virtual WAN.
- **GRE Tunnels:** Displays statistics of every LAN GRE tunnel at each site in the WAN.
- **IPsec Tunnels:** Displays statistics of every IP security tunnel at each site in the WAN.
- **Events:** Displays summary counts of events occurring at each Site in the Virtual WAN. **Events** rows expand to show summary counts by Object Type for that Site. Each Object Type will then expand to show summary counts for each Object of that type.

On the **Reporting** tab of the Citrix SD-WAN Center web interface, you can view all reports or selected reports. You can also download reports.



You can select and view reports of a particular time frame by using the timeline controls. For more

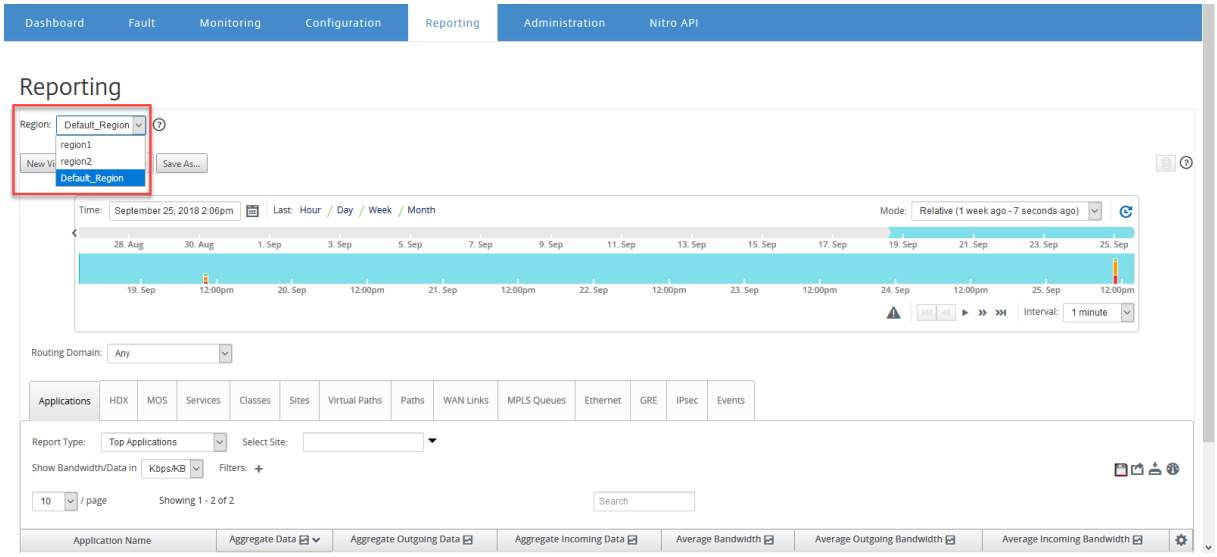
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.

For Multi-region network, you can select specific regions to view statistic reports.

The reports data is fetched from the respective region's collector.



> **Note**
>
> In single-region network deployment, the **Region** drop-down list is not available.

For more details on viewing different reports, see the following topics:

Application report

Bandwidth report

Class report

Ethernet interface report

Event report

GRE tunnel report

HDX report

IPsec tunnel report

Link performance report

MOS for applications

MPLS queues report

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Application report

March 12, 2021

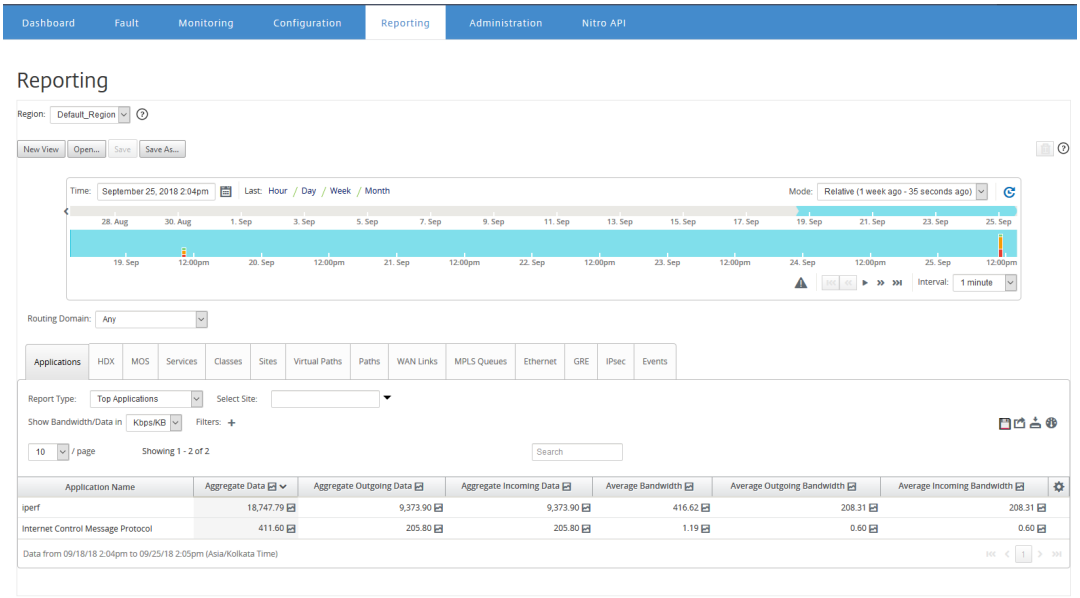
Deep packet inspection (DPI) enables the SD-WAN appliance to parse the traffic passing through it and identify the application and application family types. Citrix SD-WAN appliance records the number of bytes and bandwidth of incoming and outgoing traffic of every application. SD-WAN Center polls the SD-WAN appliance at the defined polling interval, obtains this data, and displays it on the dashboard and as reports.

You can view top applications, top sites, and top application family reports. These reports provide details about the total, incoming, and outgoing data and bandwidth.

To view application reports in Citrix SD-WAN Center:

1. In Citrix SD-WAN Center web UI, navigate to **Reporting** > **Applications**.
2. In the time-line control, select the time interval. For more information, see Timeline controls.
3. Select the unit to display the data. You can choose to view report data in units of Kbps, Mbps, or Gbps.
4. From the **Report Type** drop-down list, select one of the following report types:
    - **Top Applications**: The top applications used in the network for the selected time interval. You can filter top application by site name. By default, the top applications for all the sites are displayed.
    - **Top Application Families**: Top application families used in the network. You can filter top application families by site name. By default, the top application families for all the sites is displayed.
    - **Top Sites**: Traffic at the top sites for the selected time interval. You can filter top sites by application or application family name.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



For each report type, you can view the following data:

- **Aggregated Incoming Data**: Application data coming into the site from the WAN.
- **Aggregated Outgoing Data**: Application data sent from the site to the WAN.
- **Aggregated Data**: Sum of incoming and outgoing traffic.
- **Average Incoming Bandwidth**: Bandwidth of incoming application traffic.
- **Average Outgoing Bandwidth**: Bandwidth of outgoing application traffic.
- **Average Bandwidth**: Total bandwidth consumed by incoming and outgoing application traffic.

> **Tip**
>
> For every value, you can hover the mouse cursor over the graph icon to view a mini-graph, or click to open graph view in another window. For more information, see Statistics.

Application QoE report

March 12, 2021

Application QoE is a measure of Quality of Experience for an application. The Application QoE score range is 0–10, where 10 represents excellent quality and 0 represents poor quality. For more information, see **Application QoE** section.

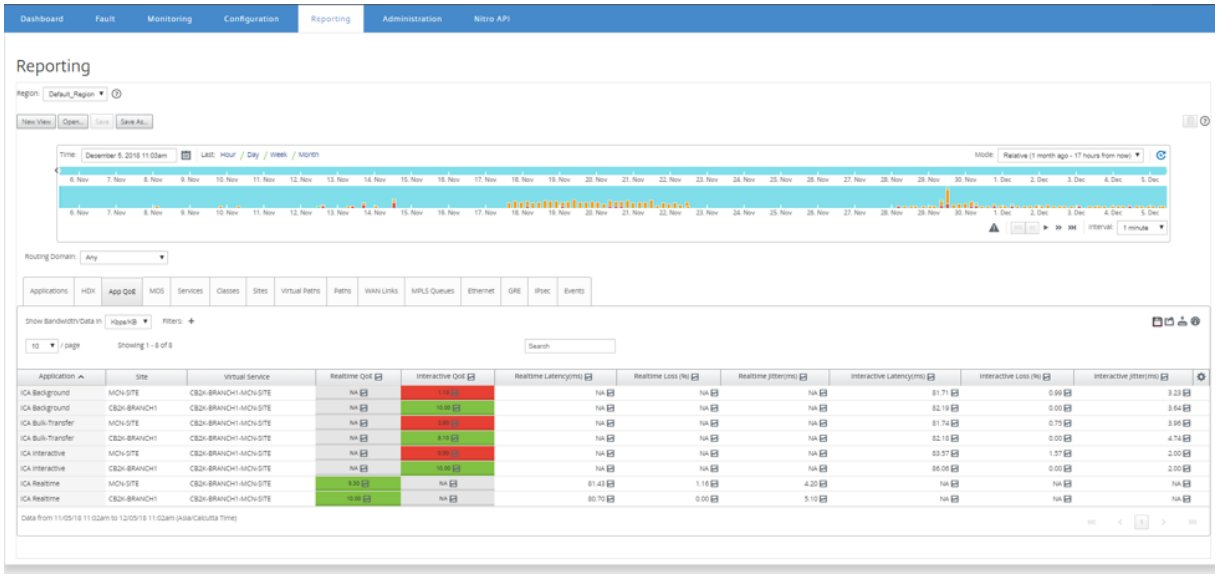
To view Application QoE report:

In Citrix SD-WAN Center, navigate to **Reporting > App QoE**, and in the timeline control select a time period.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

You can select and view reports of a particular period by using the timeline controls. For more information, see, Timeline controls.

You can also create, save, and open report views. For more information, see, Manage views.



You can view the following metrics:

- **Application**: The application or application object name.
- **Site**: The name of the site.
- **Virtual Service**: The virtual path service used.
- **Real-time QoE**: The QoE score for real-time traffic.
- **Interactive QoE**: The QoE score for interactive traffic.
- **Real-time Latency**: The latency in milliseconds for real time traffic.
- **Real-time Loss**: The loss percentage for real-time traffic.
- **Real-time Jitter**: The jitter observed in milliseconds for real time traffic.
- **Interactive Latency**: The latency in milliseconds for interactive traffic.
- **Interactive Loss**: The loss percentage for interactive traffic.
- **Interactive Jitter**: The jitter observed in milliseconds for interactive traffic.

> **Tip**
>
> For every value, you can hover the mouse cursor over the graph icon to view a mini-graph, or click to open graph view in another window.

For more information, see Statistics.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Bandwidth report

March 12, 2021

Citrix SD-WAN Center provides a central view of bandwidth statistics data polled from different sites in your SD-WAN network.

In the Citrix SD-WAN configuration, traffic flowing through the virtual paths is classified as belonging to realtime, interactive, or bulk class types. The classes are predefined, but you can customize these classes and apply rules to them. For more information, see Customizing Classe and Rules by IP Addess and Port Number.

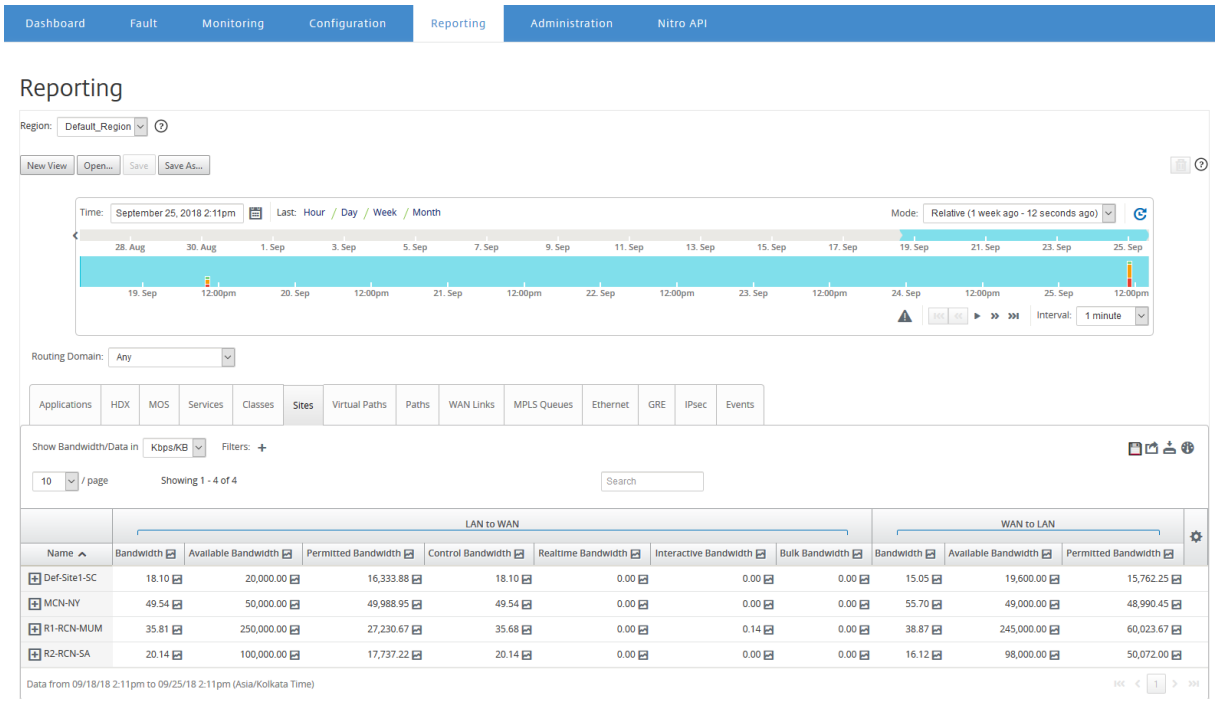
Using Citrix SD-WAN Center, you can view, along with the basic bandwidth statistics, the bandwidth consumed by applications belonging to these class types at each site, path or WAN link level.

To view bandwidth statistics:

In Citrix SD-WAN Center, navigate to **Reporting** > **Sites**, and in the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.



You can view the following metrics:

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- **Bandwidth**: Total bandwidth consumed by all packet types. Bandwidth = Control Bandwidth + Realtime Bandwidth + Interactive Bandwidth + Bulk Bandwidth. For example, in the above screen shot, at SITE2, Bandwidth = 1120.99+166.61+117.21+810.78+26.40
- **Available Bandwidth**: Total bandwidth allocated to all the WAN links of a site.
- **Control Bandwidth**: Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.
- **Permitted Bandwidth**: Bandwidth available for transmitting information.
- **Realtime Bandwidth**: Bandwidth consumed by applications that belong to the realtime class type in the Citrix SD-WAN configuration. The performance of such applications depends to a great extent upon network latency. A delayed packet is worse than a lost packet (for example, VoIP, Skype for Business).
- **Interactive Bandwidth**: Bandwidth consumed by applications that belong to the interactive class type in the Citrix SD-WAN configuration. The performance of such applications depends to a great extent upon network latency, and packet loss (for example, XenDesktop, XenApp).
- **Bulk Bandwidth**: Bandwidth consumed by applications that belong to the bulk class type in the Citrix SD-WAN configuration. These applications involve very little human intervention and are mostly handled by the systems themselves (for example, FTP, backup operations).

Class report

March 12, 2021

The virtual services can be assigned to particular QoS classes, and different bandwidth restraints can be applied to different classes. A class can be one of three basic types:

- **Real-time classes**: Serve traffic flows that demand prompt service up to a certain bandwidth limit. Low latency is preferred over aggregate throughput.
- **Interactive classes**: Serve traffic flows that are sensitive to loss and latency. Interactive classes have lower priority than real-time but have absolute priority over bulk traffic.
- **Bulk classes**: Serve traffic flows that require high bandwidth and are sensitive to loss. Bulk classes have the lowest priority.

Specifying different bandwidth requirements for different classes enables the virtual path scheduler to arbitrate competing bandwidth requests from multiple classes of the same type. The scheduler uses the Hierarchical Fair Service Curve (HFSC) algorithm to achieve fairness among the classes.

For more information about customizing classes, see Customizing Classes.

To view class statistics:

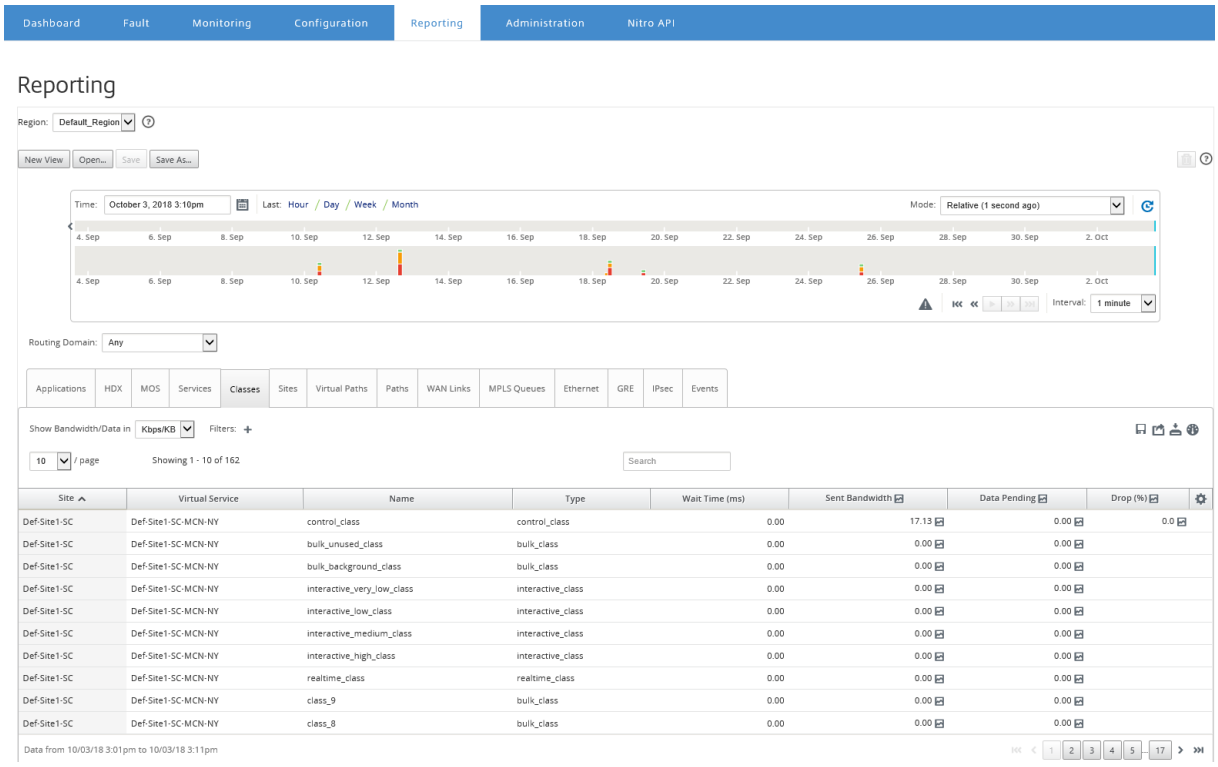
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

In Citrix SD-WAN Center, navigate to **Reports** > **Classes**, and in the timeline control select a time period.

You can select and view reports of a particular period by using the timeline controls. For more information, see, Timeline controls.

> **Note**
>
> You can view the Class data of last 30 days. Any data beyond this period is automatically removed from the SD-WAN Center collector and the respective regional collectors.

You can also create, save and open report views. For more information, see, Manage views.



You can view the following metrics:

- **Name**: Class name
- **Type**: Class Type. Releatime, interactive, or bulk.
- **Wait Time**: The time interval between transmitting packets in milliseconds.
- **Sent Bandwidth**: Transmitted bandwidth
- **Data Sent**: Data sent, in Kbps.
- **Packets Sent**: Number of packets sent.
- **Data Pending**: Data to be sent, in Kbps.
- **Packets Pending**: Number of packets to be sent.
- **Drop**: Percentage of data dropped.
- **Data Dropped**: Data dropped, in Kbps.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- **Packets Dropped**: Number of packets dropped, because of network congestion.
- **Data Coverage**: Percentage of the selected period for which data is available.

> **Note**
>
> Click the settings icon to select the metrics that you want to view.

Ethernet interface report

March 12, 2021

Citrix SD-WAN Center provides a central view of all the Ethernet interfaces on the different Citrix SD-WAN appliances on your SD-WAN network. This helps you during troubleshooting to quickly see whether any of the ports are down. You can also view the transmitted and received bandwidth, or packet details at each port. You can also view the number of errors that occurred on these interfaces during a certain time period.

The Ethernet interfaces are configured on each Citrix SD-WAN appliance during setting up the SD-WAN network.

For information about configuring interface groups for MCN sites, see Configure MCN.

For information about configuring interface groups for branch sites, see Configure Branch Node.

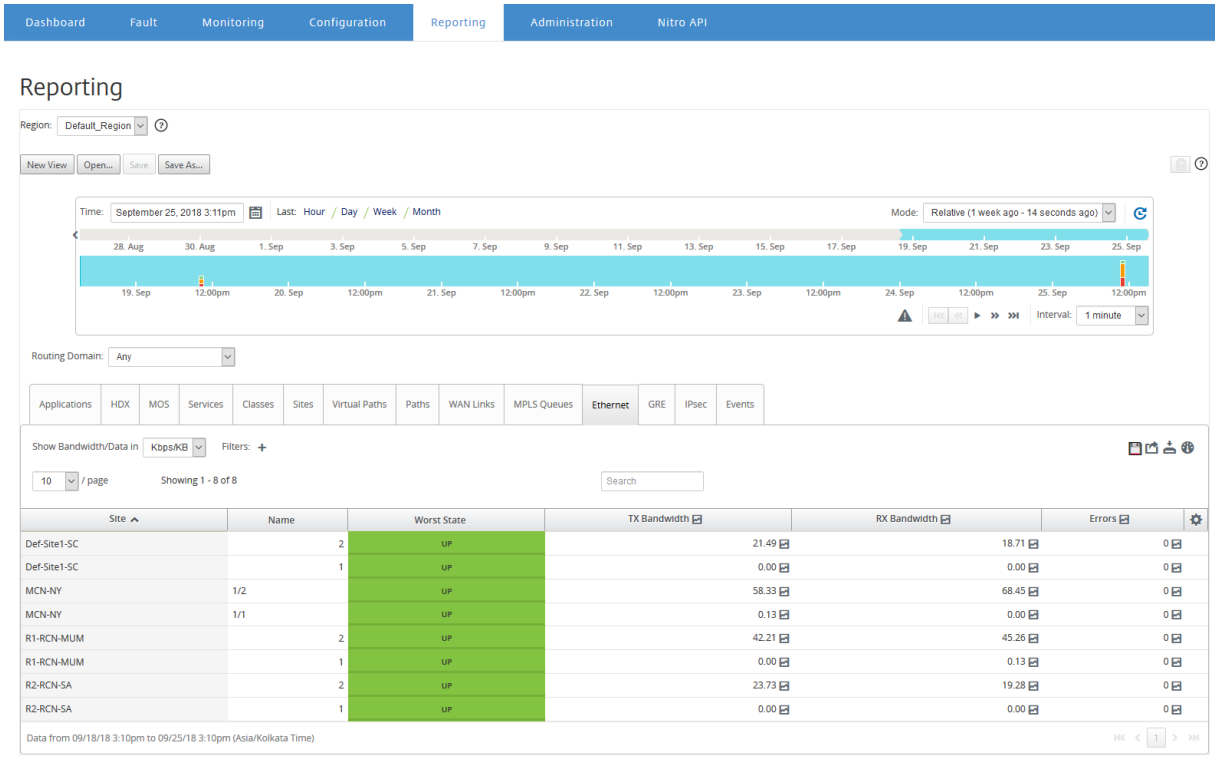
To view Ethernet interface statistics:

In Citrix SD-WAN Center, navigate to **Reports** > **Ethernet**, and in the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



You can view the following metrics:

- **Name**: Name of the Ethernet interface.
- **Worst State**: Worst state observed during the selected time period.
- **TX Bandwidth**: Bandwidth transmitted.
- **RX Bandwidth**: Bandwidth received.
- **TX Packets**: Number of packets transmitted.
- **RX Packets**: Number of packets received.
- **Errors**: Number of errors observed during the selected time period.
- **Data Coverage**: Percentage of the selected time period for which data is available.

> **Note**
>
> Click the settings icon to select the metrics that you want to view.

Event report

March 12, 2021

You can view counts of different events occurring at each site in the SD-WAN network.

For more information about events, see Events.

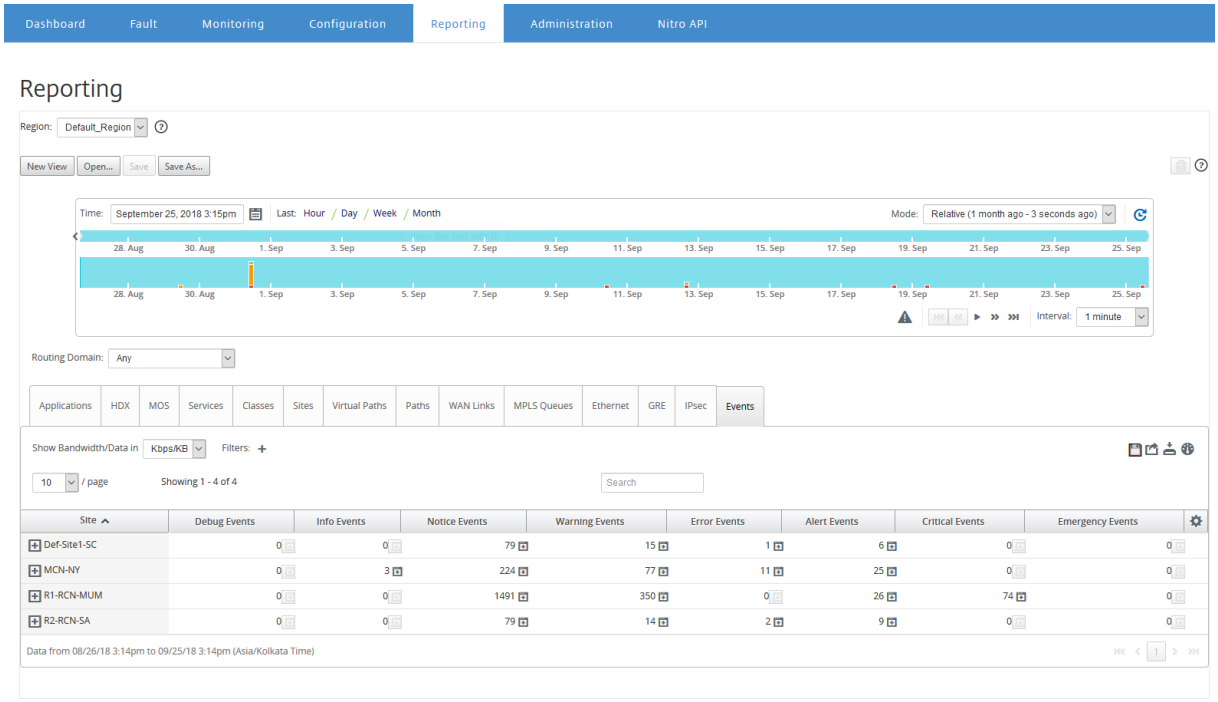
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

To view event statistics:

In Citrix SD-WAN Center, navigate to **Reports** > **Events**, and in the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.



You can view the following metrics:

- **Info Events**: Number of information events that occurred during the selected time period. These are low-level events.
- **Notice Events**: Number of notice events that occurred during the selected time period. These are events that the administrator should know about.
- **Warning Events**: Number of warning events that occurred during the selected time period. These are events that require action in the near future.
- **Error Events**: Number of error events that occurred during the selected time period. These are events that indicate some type of error.
- **Alert Events**: Number of alert events that occurred during the selected time period. These are events that might require action.
- **Critical Events**: Number of critical events that occurred during the selected time period. These are events that indicate an imminent crisis.
- **Emergency Events**: Number of emergency events that occurred during the selected time period. These are events that indicate an immediate crisis (for example, power supply failure, fan

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

failure, hard disk threshold exceeded, service disabled).

- **Debug Events**: Number of debugging events that occurred during the selected time period. Debug events are generated when Test Email or Test Syslog options are used on the Citrix SD-WAN appliances.

> **Note**
>
> Click the settings icon to select the metrics that you want to view.

The following table lists a few examples of the state changes of objects for which events are reported.

Event	Object Type	Previous State	Current State
NOTICE	LAN to WAN path	BAD	GOOD
		GOOD	BAD
	WAN to LAN path	BAD	GOOD
		GOOD	BAD
	Dynamic virtual path	BAD	GOOD
		GOOD	BAD
WARNING	Virtual path	GOOD	BAD
	WAN link congestion	UNCONGESTED	CONGESTED
		CONGESTED	UNCONGESTED
	Usage congestion	UNCONGESTED	CONGESTED
		CONGESTED	UNCONGESTED
	LAN to WAN path	GOOD	DEAD
		BAD	DEAD
	WAN to LAN path	GOOD	DEAD
		BAD	DEAD
ALERT	Virtual path	BAD	DEAD
		DEAD	BAD
ERROR	WAN-link	GOOD	DEAD
	Ethernet	GOOD	UNDEFINED
		UNDEFINED	DEAD
INFO	Proxy-arp	UNDEFINED	ACTIVE
		UNDEFINED	STANDBY

You can configure Citrix SD-WAN Center to send external event notifications for different event types as email, SNMP traps or syslog messages. For more information, see Event notifications.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

GRE tunnel report

March 12, 2021

You can use a tunneling mechanism to transport packets of one protocol within another protocol. The protocol that carries the other protocol is called the transport protocol, and the carried protocol is called the passenger protocol. Generic Routing Encapsulation (GRE) is a tunneling mechanism that uses IP as the transport protocol and can carry many different passenger protocols.

The tunnel source address and destination address are used to identify the two endpoints of the virtual point-to-point links in the tunnel.

For more information about configuring GRE tunnels on Citrix SD-WAN appliances, see GRE Tunnel.

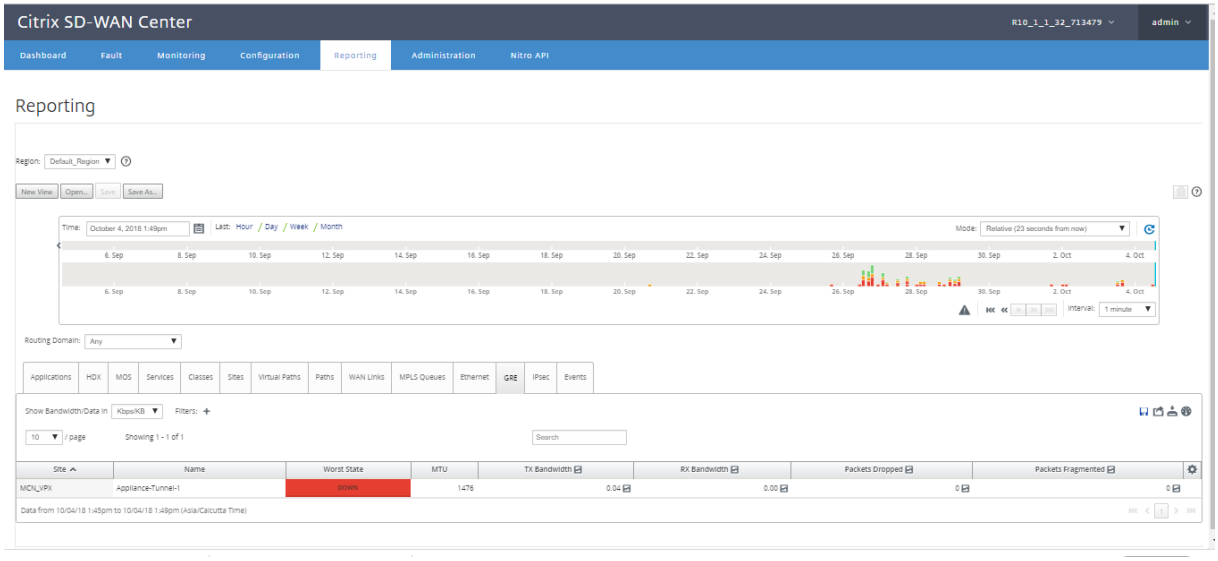
Citrix SD-WAN Center can show you the state of all the GRE tunnels configured in your Citrix SD-WAN network.

To view GRE tunnel statistics:

In Citrix SD-WAN Center, navigating to **Reporting** > **GRE**, and in the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.



You can view the following metrics:

- **Worst State**: Worst state observed during the selected time period.
- **MTU**: Maximum transmission unit — the size of the largest IP datagram that can be transferred through a specific link.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- **TX Bandwidth**: Bandwidth transmitted.
- **RX Bandwidth**: Bandwidth received.
- **TX Packets**: Number of packets transmitted.
- **RX Packets**: Number of packets received.
- **Packets Dropped**: Number of packets dropped, because of network congestion.
- **Packets Fragmented**: Number of packets fragmented. Packets are fragmented to create smaller packets that can pass through a link with an MTU that is smaller than the original datagram. The fragments are reassembled by the receiving host.
- **Data Coverage**: Percentage of the selected time period for which data is available.

> **Note**
>
> Click the settings icon to select the metrics that you want to view.

HDX report

March 12, 2021

Select one of the following report types from the drop-down list:

- HDX Site Stats
- HDX Summary (applicable for both HDX information channel available and unavailable sessions)
- HDX User Sessions (applicable for only HDX information channel available sessions only)
- HDX Apps (applicable for only HDX information channel available sessions only)

HDX site statistics

HDX report provides detailed HDX data per site. The data for each site is shown in two views.

Summary view

The Summary view shows the following data for a site:

- **QoE Index** - The Quality of Experience (QoE) is a numeric value between 0–100. The higher the value the better the user experience.
- **Users** –The number of active users on the site.
- **TCP Flows** - The number of active HDX sessions on the site that use the TCP protocol.
- **UDP Flows** –The number of active HDX sessions on the site that use UDP protocols.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- **Sessions** –The total number of active HDX sessions on the site that includes both Small-Scale Integration (SSI) and Medium-Scale Integration (MSI) sessions.

Detail view

You can click an individual site to view details about all the variables affecting QoE. Each pair of row shows the QoE factors for data calculated at local and remote sides for a given virtual path.

Latency, jitter, and packet drop variables affecting QoE are the effective numbers that the Citrix SD-WAN appliance is measuring. For example, there might be larger percent of packet drop in the network, since Citrix SD-WAN corrects the packet drops through its own protocol, the effective packet loss seen by the application would be much lesser, hence improves the QoE for HDX applications.

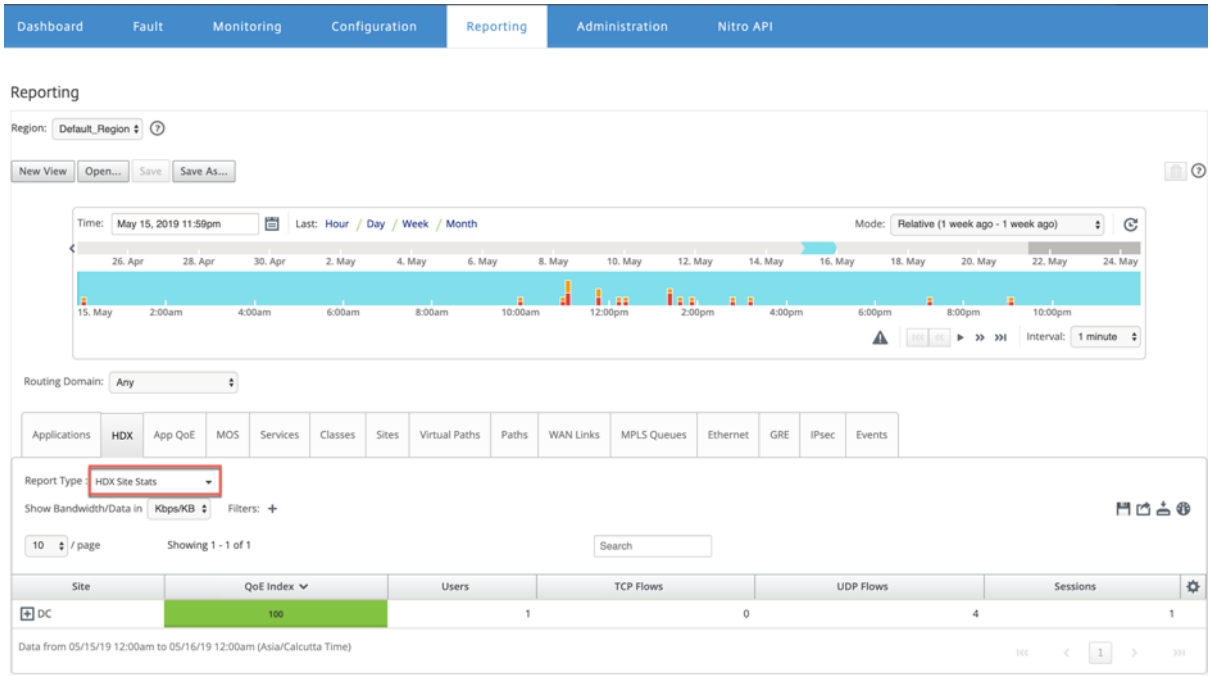
Similarly, latency improvement through packet duplication also improves the QoE for HDX applications. In other words, Citrix SD-WAN improves the QoE for HDX traffic by improving the factors affecting the QoE. For more information see, HDX QoE.

To view HDX Reports:

In the Citrix SD-WAN Center, navigate to **Reporting** > **HDX**, and in the timeline control select a period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

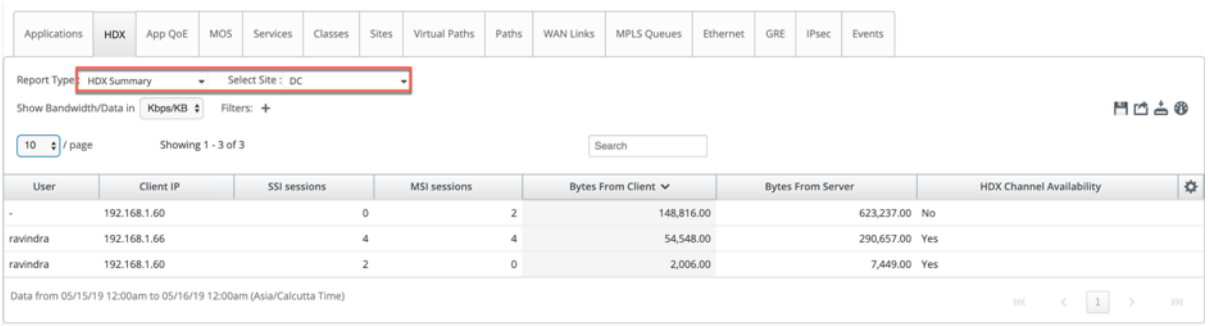
You can also create, save, and open report views. For more information, see, Manage views.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

HDX summary

Select the **HDX Summary** report and the site from the drop-down list. The HDX summary report displays each user's report that has logged in during the selected time period.

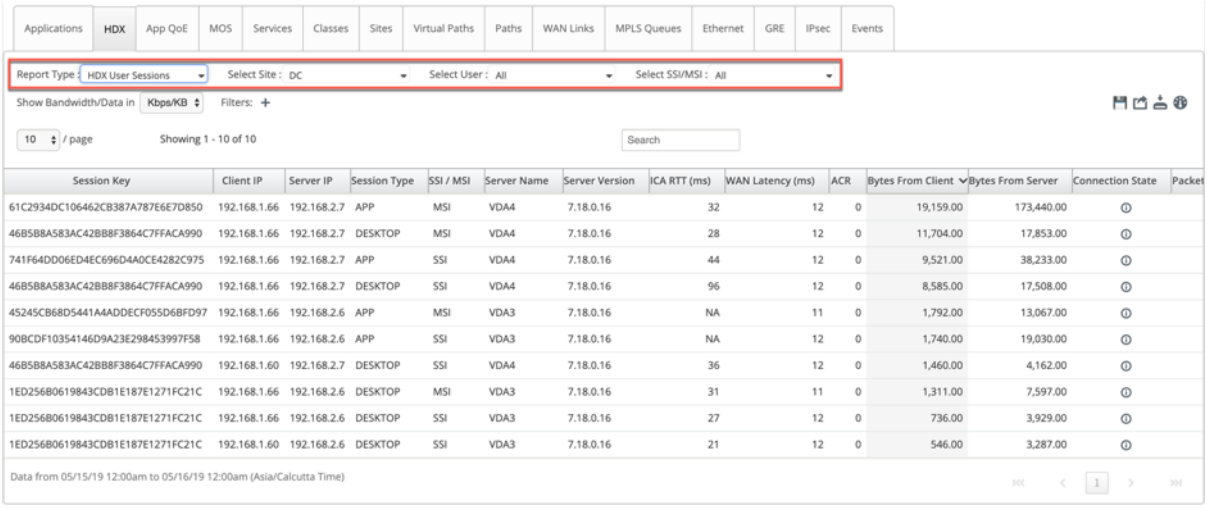


In the HDX summary report, you can view the following parameters:

- **User**: Name of the user.
- **Client IP**: Client IP address.
- **SSI sessions**: Number of active Single Stream ICA (SSI) sessions.
- **MSI sessions**: Number of active Multi Stream ICA (MSI) sessions.
- **Bytes from Client**: Size in bytes from client.
- **Bytes from Server**: Size in bytes from server.
- **HDX Channel Availability**: Provides the HDX information channel availability status as **Yes/No**. If the channel is not available, then the user name shows as a hyphen (-).

HDX user sessions

In the HDX user sessions report, you can see every sessions detail used by each user. Select the site, user, and SSI or MSI from the drop-down list. By default, the **Select User** and **Select SSI/MSI** fields shows **ALL**.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

You can use the **Search** or **Filter:+** options to find out the required session information as per your requirement.

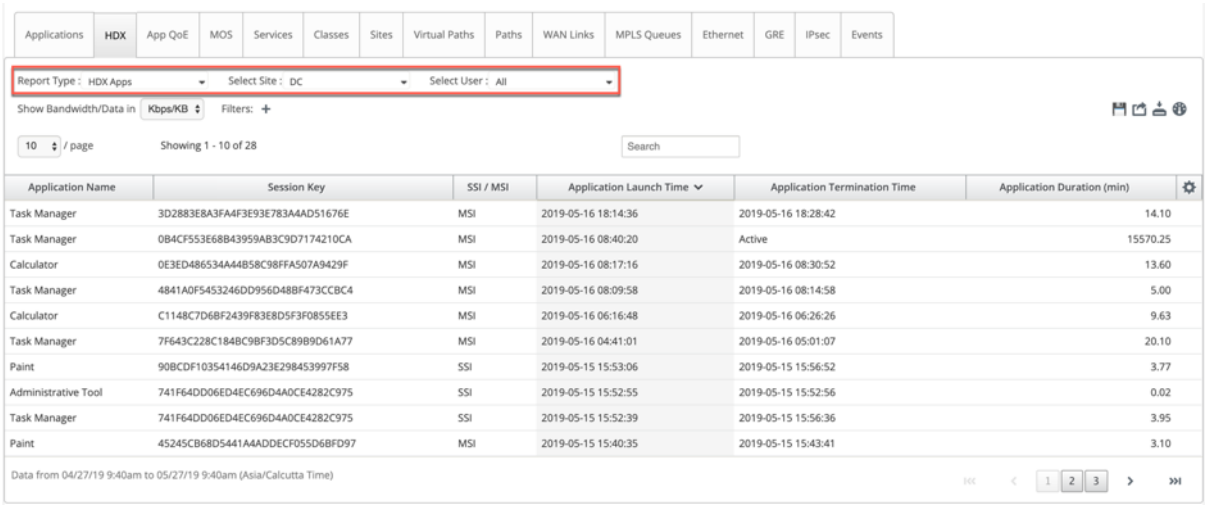
- **Session Key**: The session key represents the unique identity for an ICA session.
- **Client IP**: Client IP address for each session.
- **Server IP**: Server IP address for each session.
- **Session Type**: Type of the sessions (Desktop, App).
- **SSI/MSI**: Shows whether it is an SSI or MSI session.
- **Server Name**: Shows the name of the server.
- **Server Version**: Shows the version of the server.
- **ICA RTT (ms)**: Shows the ICA Round Trip Time (RTT) in milliseconds. This is an end-to-end round trip time between the client and the server.
- **WAN Latency**: Latency over the WAN, that is between the two SD-WANs over the virtual path. This latency doesn't include client-side or server-side network latency.
- **ACR**: Shows the auto client reconnect counts.
- **Bytes from Client**: Size in bytes from client.
- **Bytes from Server**: Size in bytes from server.
- **Connection State**: Hover the mouse to see the connection state.
  - For MSI, there are four connections. These connections are L4 level (TCP/UDP state).
  - For SSI, there is only one connection.

- **Packet from Client**: Number of packets from client.
- **Packet from Server**: Number of packets from server.

HDX apps

You can see all the application used by a specific user or by all users. Select the **Site** and the **User** to view the applications details.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



- **Application Name**: Provides the name of the HDX application.
- **Session Key**: Provides the unique session key which is used for that particular application.
- **SSI/MSI**: Shows whether it is an SSI or MSI session.
- **Application Launch Time**: Provides the application launch time with date.
- **Application Termination Time**: Provides the application termination time with date. If an application is active, it shows active instead of the termination time.
- **Application Duration (min)**: Provides the application time duration in minutes.

> **Note**
>
> - If there is any unintended error such as, if the HDX session information is unavailable on the appliance, then the HDX user-based reports are not shown even if the **HDX User Reporting** is enabled. Some of the fields such as user name, server name, server version, ICA RTT in the reports might be shown as **NA**.
> - Application termination time in **HDX Apps** report is shown only if SD-WAN receives **Application Termination Time** from Xen Application/Xen Desktop Server. Otherwise, some of the applications are reported to be active even if closed.

IPsec tunnel report

March 12, 2021

IP Security (IPsec) protocols provide security services such as encrypting sensitive data, authentication, protection against replay, and data confidentiality for IP packets. Encapsulating Security Payload (ESP), and Authentication Header (AH) are the two IPsec security protocols used to provide these security services.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

In IPsec tunnel mode, the entire original IP packet is protected by IPsec. The original IP packet is wrapped and encrypted, and a new IP header is added before transmitting the packet through the VPN tunnel.

For more information about configuring IPsec tunnels on Citrix SD-WAN appliances, see IPsec Tunnel Termination.

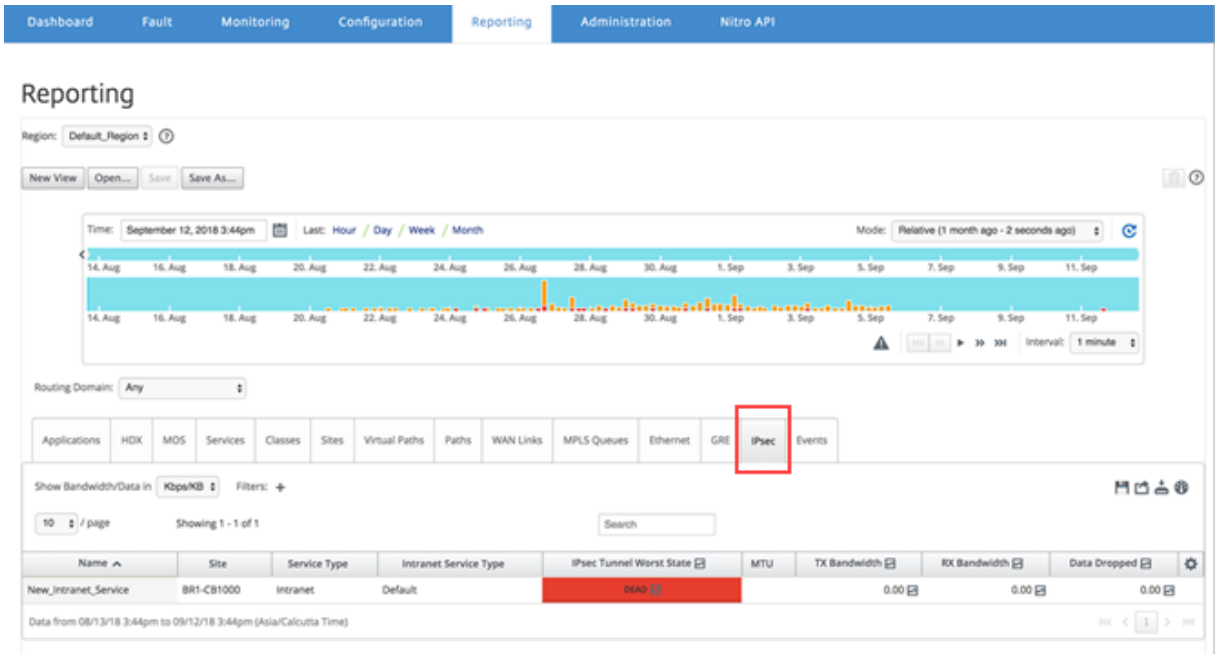
Citrix SD-WAN Center can show you the state of all the IPsec tunnels configured in your Citrix SD-WAN network.

To view IPsec tunnel statistics:

In Citrix SD-WAN Center, navigate to **Reporting** > **IPsec Tunnels**, and in the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save, and open report views. For more information, see, Manage views.



You can view the following metrics:

- **Name**: Application name.
- **Site**: Name of the site.
- **Service Type**: Type of the service.
- **Intranet Service Type**: Type of intranet service associated with the IPsec tunnel. The following are the type of intranet services:
  - Default
  - Microsoft Azure Virtual WAN

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

  - Zscaler
  - Citrix SaaS Gateway

- **IPsec Worst State**: Worst state observed during the selected time period.
- **MTU**: Maximum transmission unit—size of the largest IP datagram that can be transferred through a specific link.
- **TX Bandwidth**: Bandwidth transmitted.
- **RX Bandwidth**: Bandwidth received.
- **TX Packets**: Number of packets transmitted.
- **RX Packets**: Number of packets received.
- **Data Dropped**: Data dropped, in Kbps.
- **Packets Dropped**: Number of packets dropped.

> **Note**
>
> Click the settings icon to select the metrics that you want to view.

Link performance report

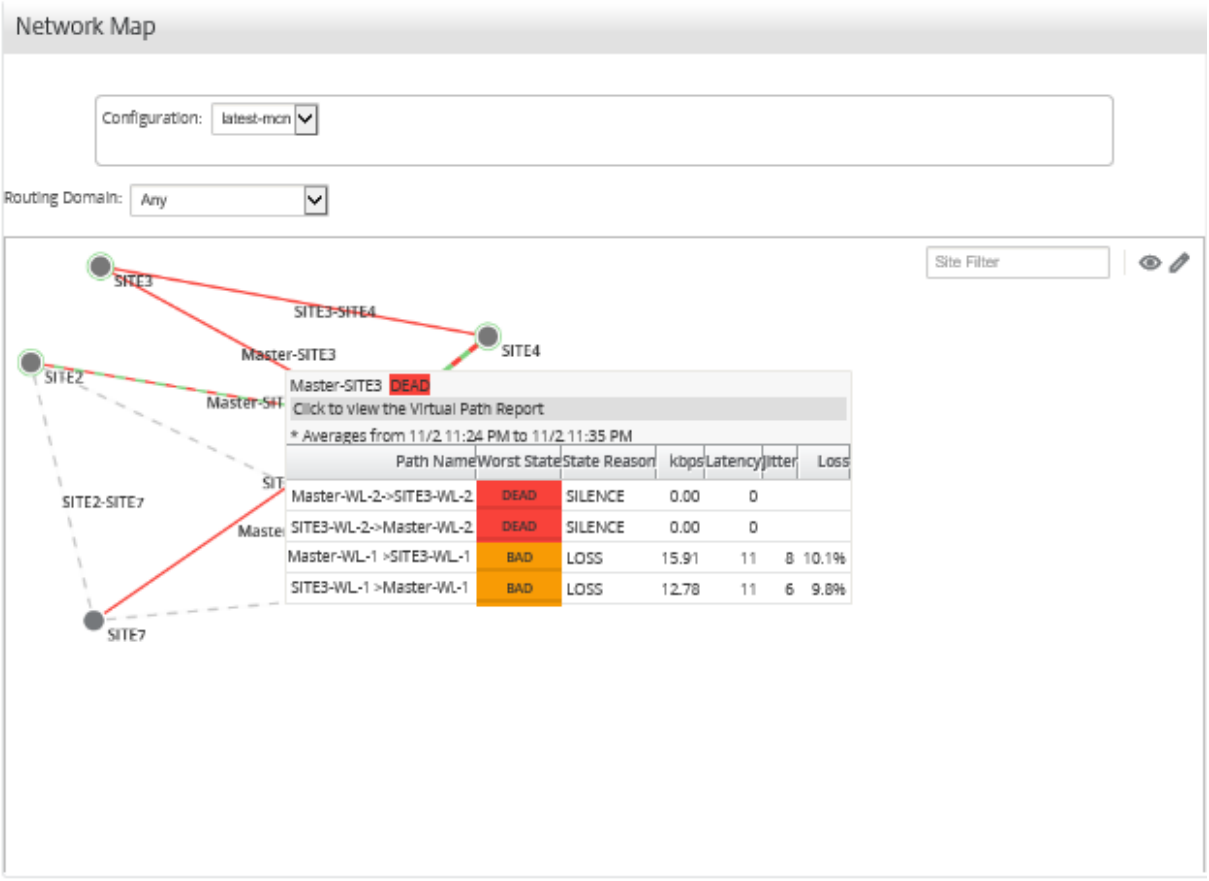
March 12, 2021

Citrix SD-WAN Center can show performance statistics at the site, service, virtual path, or WAN-link level.

Consider a network in which organization ABC has four branch offices. Brownouts have been reported at SITE3. That is, the employees are sometimes unable to view the intranet pages. You suspect that it's because of the performance of the underlying links.

You can get a high-level view of the link statistics by hovering your mouse cursor over the path between a site and the data center on the Network Map on the Dashboard.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



The above screen shot shows that there are two WAN links (WL-1 and WL-2) between SITE 3 and the Master Controller Node (MCN), and displays statistics for the most recent 10 minutes.

The virtual paths Master-WL2->SITE3-WL2 and SITE3-WL2 ->Master-WL2 are not functioning, and alternative paths Master-WL1->SITE3-WL1 and SITE3-WL1 ->Master-WL1 are in poor condition, losing a significant percentage of the transmitted data. That is the probable cause of the brown-out issue at SITE3.

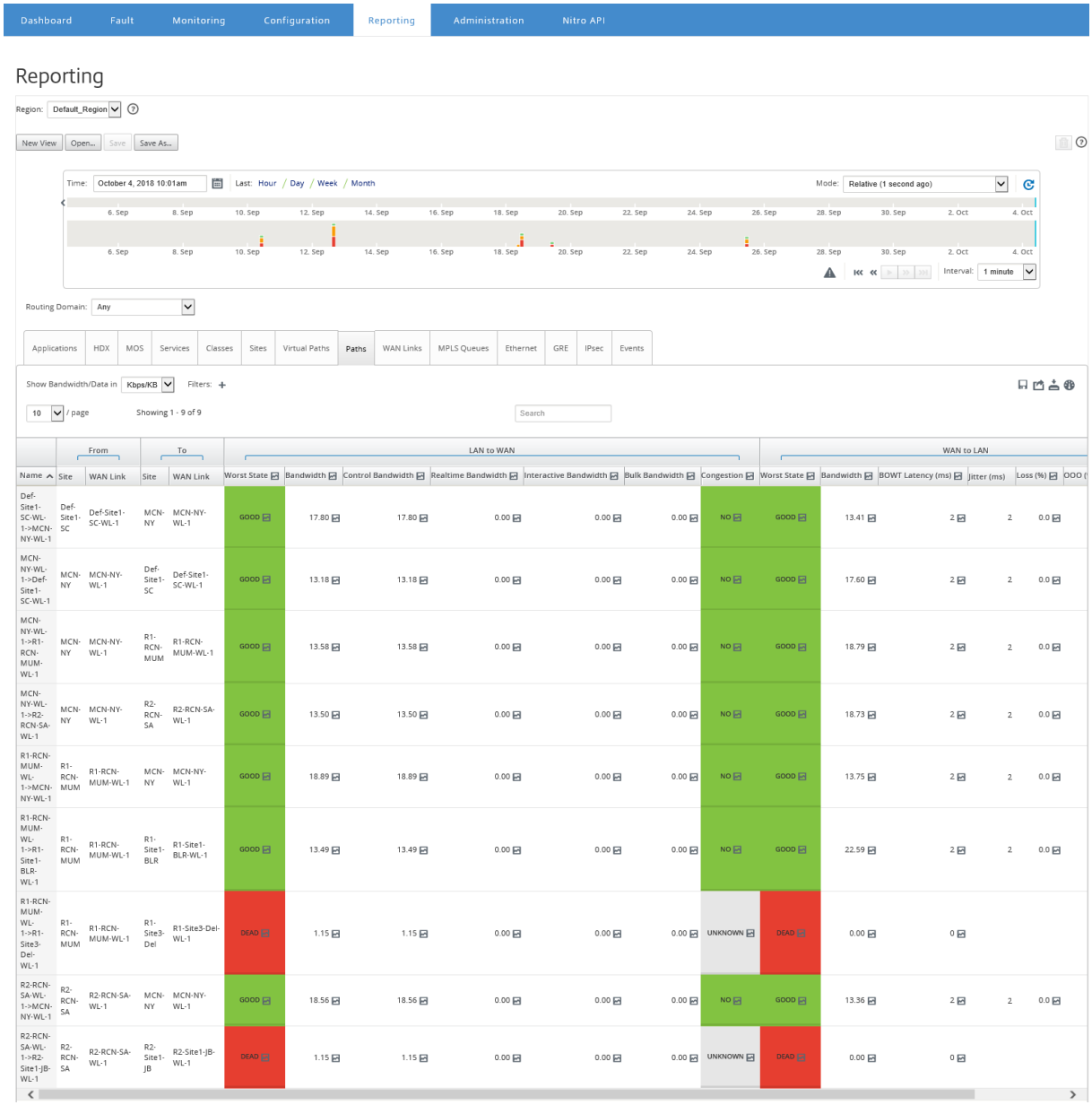
Alternatively, you can view the link statistics by navigating to **Reporting** >**Paths**.

In the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



You can view the following metrics:

- **Name**: The path name.
- **From (Site and WAN Link)**: The source site and WAN link.
- **To (Site and WAN Link)**: The destination site and WAN link.
- **LAN to WAN**
  - **Work State**:
  - **Bandwidth**: Total bandwidth consumed by all packet types. Bandwidth= Control Bandwidth + Real-time Bandwidth + Interactive Bandwidth + Bulk Bandwidth.
  - **Control Bandwidth**: Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

  - **Real-time Bandwidth**: Bandwidth consumed by applications that belong to the real-time class type in the SD-WAN configuration. The performance of such applications depends on a great extent upon network latency. A delayed packet is worse than a lost packet (for example, VoIP, Skype for Business).
  - **Interactive Bandwidth**: Bandwidth consumed by applications that belong to the interactive class type in the SD-WAN configuration. The performance of such applications depends on a great extent upon network latency, and packet loss (for example, XenDesktop, XenApp).
  - **Bulk Bandwidth**: Bandwidth consumed by applications that belong to the bulk class type in the SD-WAN configuration. These applications involve very little human intervention and are mostly handled by the systems themselves (for example, FTP, backup operations).
  - **Congestion**: Congestion due to increased traffic or unexpected delay in packet flow in the WAN.

- **WAN to LAN**:

  - **Worst State**: The worst WAN to LAN state observed during the time period.
  - **Bandwidth**:
  - **BOWT Latency(ms)**: Best one-way time (BOWT) taken for a packet to move from one point to another, in milliseconds.
  - **Jitter (ms)**: Variation in the delay of received packets, in milliseconds.
  - **Loss (%)**: Percentage of packets lost.
  - **OOO (%)**: Percentage of packets that are not in the right order or out of order (OOO).
  - **Congestion**: Congestion due to increased traffic or unexpected delay in packet flow in the WAN.

Click on **Settings** icon and select the parameters that you wants to view on reports.

MOS for applications

March 12, 2021

The mean opinion score (MOS) provides a numerical measure of the quality of the experience that an application delivers to end users. It is primarily used for VoIP applications. In Citrix SD-WAN, MOS is also used to assess the quality of non-VoIP applications by judging the traffic as if it were a VoIP call.

Citrix SD-WAN Center calculates and displays MOS for the traffic that passes through the virtual path. Enable the **Estimate MOS** option for each application on every Citrix SD-WAN appliance to display the MOS scores of these applications in Citrix SD-WAN Center.

For more information about enabling MOS for applications in Citrix SD-WAN, see Add Rule Groups and Enable MOS.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

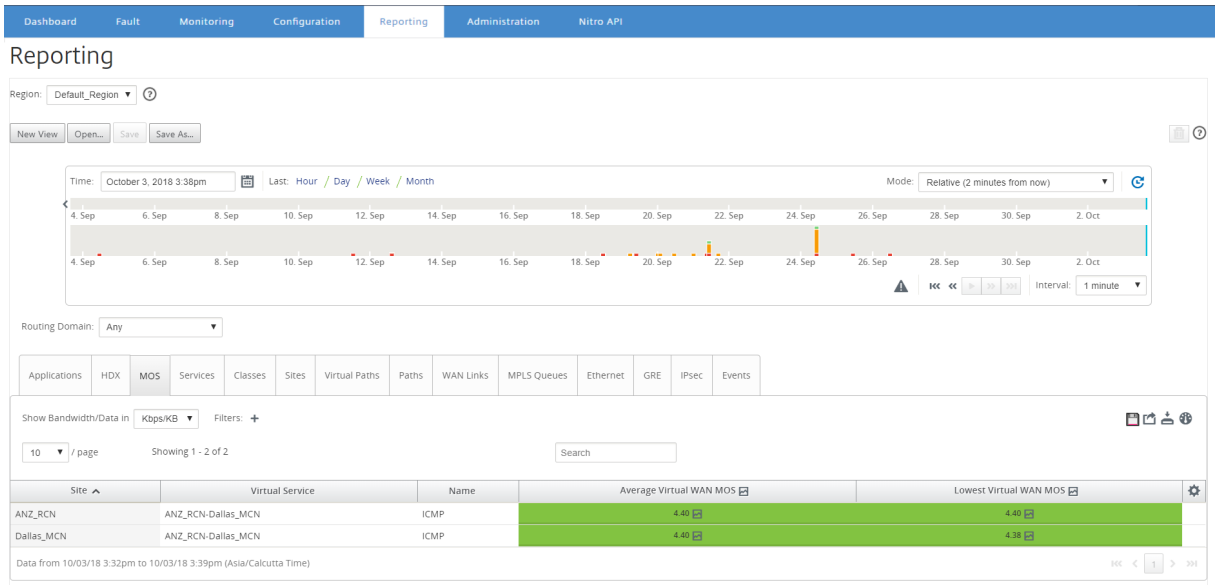
> **Note**
>
> Enable the Track Performance option, under Rules to estimate MOS for applications and display it in Citrix SD-WAN Center. For more information on rules, see Rules by IP address and port number.

To view MOS for applications:

In Citrix SD-WAN Center, navigating to **Reporting** > **Applications**, and in the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.



You can view the following metrics:

- **Name**: Name of the application.
- **Average Virtual WAN MOS**: Average quality score calculated over the selected time period.
- **Lowest Virtual WAN MOS**: Lowest quality score calculated within the selected time period.

The scores are graded as follows:

- 5 –Users are very satisfied.
- 4 –Users are satisfied.
- 3 –Users are dissatisfied.
- 2 –Users are very dissatisfied.
- 1 –Not recommended.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

MPLS queues report

March 12, 2021

MPLS Queues provide service queues controlled by standard Differentiated Services Code Point (DSCP) tags. The tags control the quality of service between two sites on the Virtual WAN.

MPLS Queues allow MPLS providers to identify traffic on the basis of DSCP markings, so that class of service can be applied by the provider.

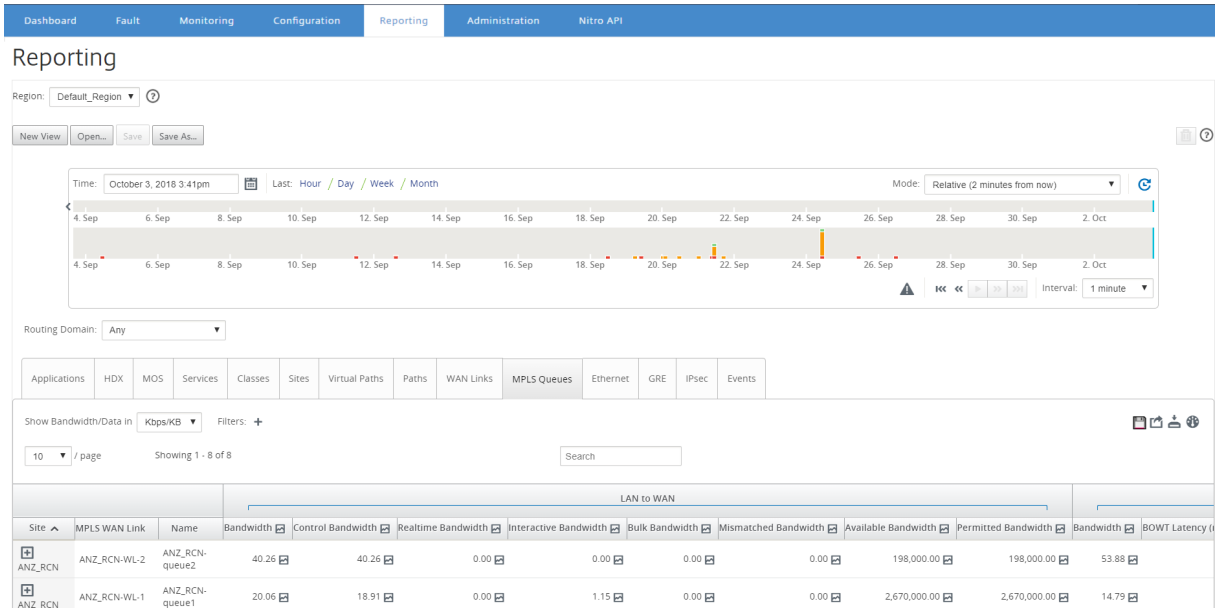
For more information about configuring private MPLS WAN links on Citrix SD-WAN appliances, see MPLS Queues.

To view MPLS queue statistics:

In Citrix SD-WAN Center, navigate to **Reports** > **MPLS Queues**, and in the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.



You can view the following metrics:

- **MPLS WAN Link**: Name of the MPLS WAN link that the MPLS queue is a member of.
- **Name**: The DSCP tag name.
- **Bandwidth**: Total bandwidth consumed by all packet types. Bandwidth = Control Bandwidth + Realtime Bandwidth + Interactive Bandwidth + Bulk Bandwidth.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- **Control Bandwidth**: Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.
- **Realtime Bandwidth**: Bandwidth consumed by applications that belong to the realtime class type in the Citrix SD-WAN configuration. The performance of such applications depends to a great extent upon network latency. A delayed packet is worse than a lost packet (for example- VoIP, Skype for Business).
- **Interactive Bandwidth**: Bandwidth consumed by applications that belong to the interactive class type in the Citrix SD-WAN configuration. The performance of such applications depends to a great extent upon network latency, and packet loss (for example, XenDesktop, XenApp).
- **Bulk Bandwidth**: Bandwidth consumed by applications that belong to the bulk class type in the Citrix SD-WAN configuration. These applications involve very little human intervention and are mostly handled by the systems themselves (for example, FTP, backup operations).
- **Mismatched Bandwidth**: Frames that do not match the defined DSCP tags are mapped to a default queue designated for mismatched bandwidth.
- **Available Bandwidth**: The sum of bandwidth allocated to all the WAN links of a site.
- **Permitted Bandwidth**: Bandwidth available for transmitting information.
- **BOWT Latency**: Best one-way time taken for a packet to move from one point to another, in milliseconds.
- **Jitter**: Variation in the delay of received packets, in milliseconds.
- **Packets Lost**: Number of packets lost.
- **Loss**: Percentage of packets lost.
- **OOO**: Percentage of packets that are not in the right order.
- **Congestion**: Congestion due to increased traffic or unexpected delay in packet flow in the WAN.

> **Note**
>
> Click the settings icon to select the metrics that you want to view.

Administration

March 12, 2021

You can manage and maintain your Citrix SD-WAN Center VPX using the following administrative options.

Configure date and time

HTTPS certificates

Import MCN configuration

Manage database

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Mangae views

Software upgrade

Timeline controls

User accounts

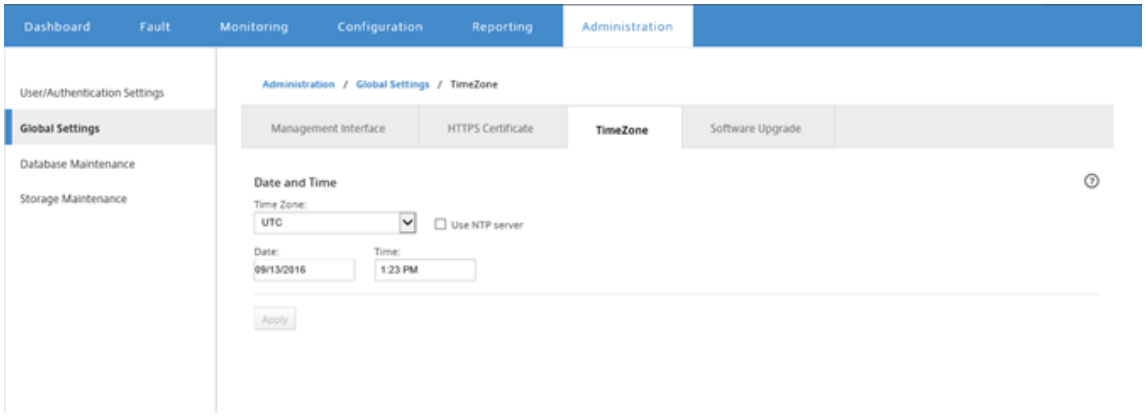
Configure date and time

March 12, 2021

You can change the date and time of the Citrix SD-WAN Center management system either manually or by using an NTP server. If you select the **Use NTP server** option, then you cannot manually enter a current date and time.

To manually set the date and time:

1. In the Citrix SD-WAN Center web interface, click the **Administration** tab.
2. Click **Global Settings**, and then click **Timezone**.



3. In the **Time Zone** field, select a **city** in your current time zone. Alternatively, enter the current date and time for your time zone.
4. Click **Apply**.

You can synchronize the Citrix SD-WAN Center clock with an external NTP server.

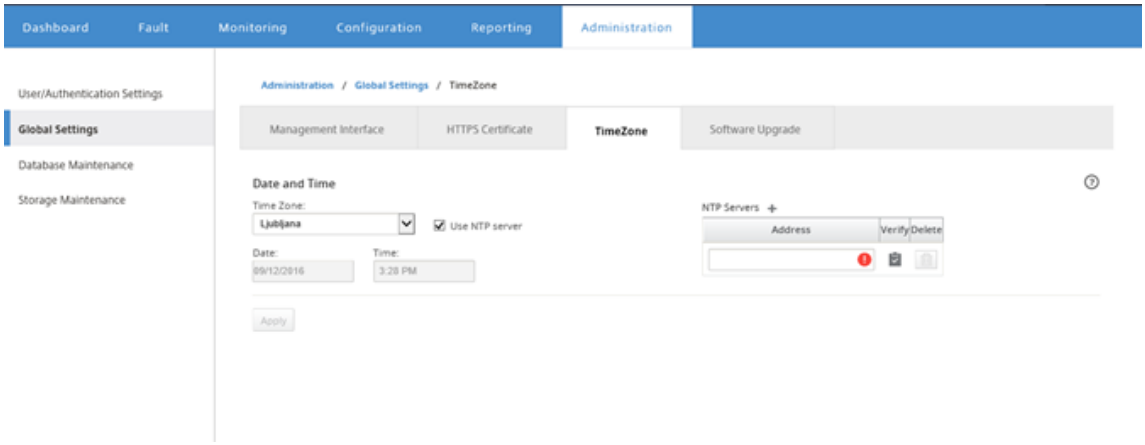
To set the date and time by using an NTP Server:

1. In the Citrix SD-WAN Center web interface, click the **Administration** tab.
2. Click **Global Settings** and then click **TimeZone**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

3. Select **Use NTP Server**.

   This disables the Date and Time fields, and displays the NTP Servers table.



4. To add a new NTP server, click the **+** icon next to NTP Server .
5. In the **Address** field, enter the **IP Address** for the NTP Server.

   You can specify up to three NTP servers, but you must specify at least one. These act as backup NTP servers, if one server is down the Citrix SD-WAN Center automatically synchronizes with the other NTP server.

   If you specify a domain name for an NTP server, you must also configure a DNS server unless you have already done so. To remove a server entry from the table, click the **Delete** icon in the Delete column of the entry.

6. Click **Verify** to verify that the server is reachable, before applying your settings.
7. Click **Apply**.

HTTPS certificates

March 12, 2021

HTTPS certificate is required for establishing secured management HTTPS connection to Citrix SD-WAN Center.

View installed HTTPS certificate details

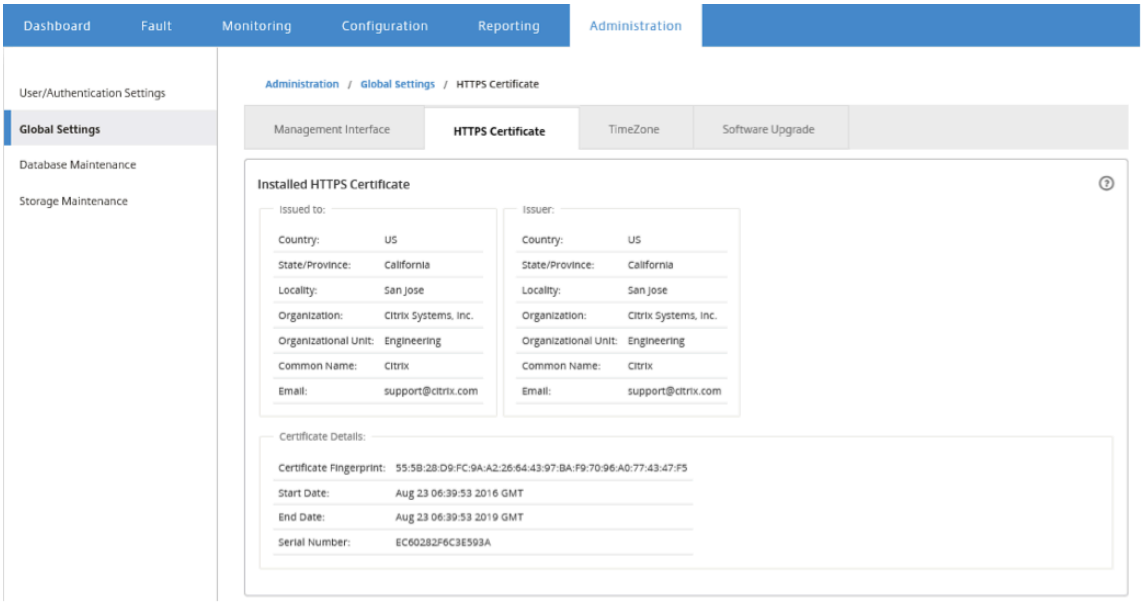
CitrixTo evaluate the current certificate, you can display the certificate details.

To display the details of HTTPS certificate already installed on Citrix SD-WAN Center:

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

1. In the Citrix SD-WAN Center web interface, click the **Administration** tab.
2. Click **Global Settings** and then click **HTTPS Certificate**.

   The HTTPS certificate details appear in the **Installed HTTPS Certificate** section.



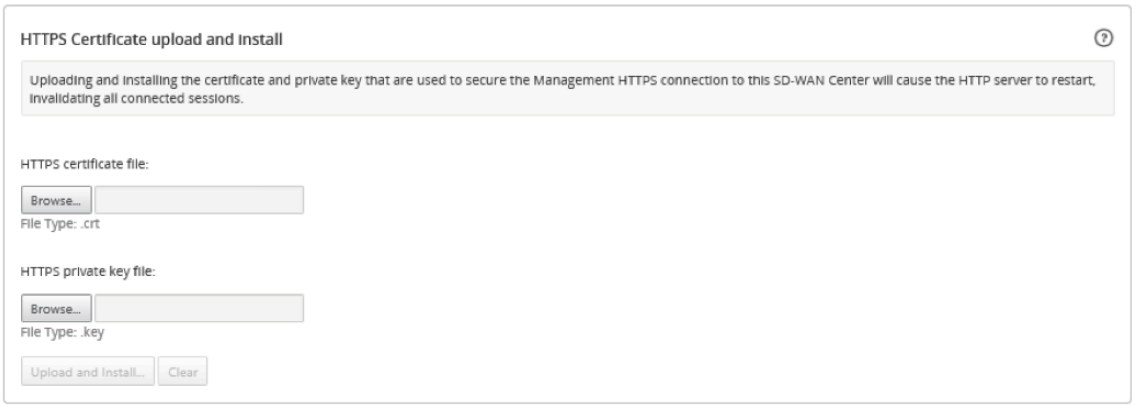
Upload and install an HTTPS certificate

Installing an HTTPS Certificate puts Citrix SD-WAN Center into Maintenance Mode until the operation is complete. When the operation is complete, the web server is restarted, invalidating all connected sessions. If the connection to the server is lost when the web server is restarted, the maintenance mode screen automatically reloads the previous page and displays a security notice from the browser. If the screen does not reload, click **Continue** to reload the previous page.

To upload and install the HTTPS certificate:

1. In the Citrix SD-WAN Center web interface, click the **Administration** tab.
2. Click **Global Settings** and then click **HTTPS Certificates**.
3. In the **HTTPS Certificate upload and Install** section, in the **HTTPS certificate file** field, click **Browse** and select a HTTPS certificate.
4. For the field **HTTPS private key file**, click **Browse** and select an HTTPS private key file.
5. Click **Upload and Install**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



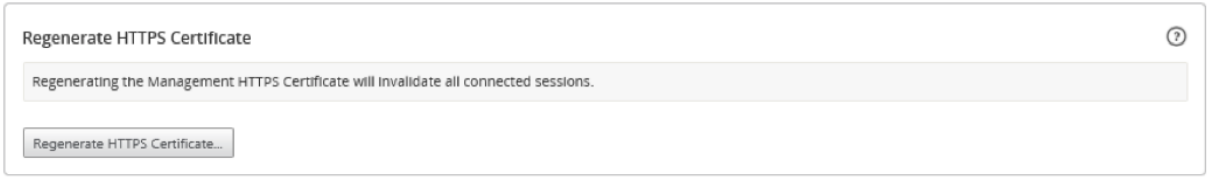
Regenerate the HTTPS certificate

You can regenerate a self-signed certificate that secures the Management HTTPS connection to Citrix SD-WAN Center. Regenerating the HTTPS Certificate puts Citrix SD-WAN Center into Maintenance Mode until the operation is complete. When the operation is complete, the web server is restarted, invalidating all connected sessions.

If the connection to the server is lost when the web server is restarted, the maintenance mode screen automatically reloads the previous page and displays a security notice from the browser. If the screen does not appear, click **Continue** to reload the previous page.

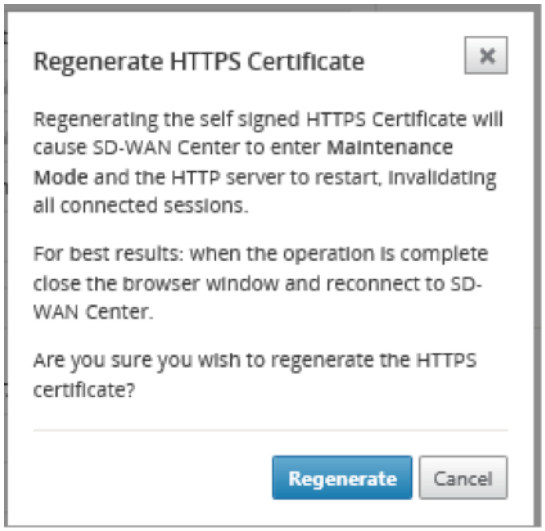
To regenerate the HTTPS certificate:

1. In the Citrix SD-WAN Center web interface, click the **Administration** tab.
2. Click **Global Settings** and then click **HTTPS Certificates**.
3. In the **Regenerate HTTPS Certificate** section, click **Regenerate HTTPS Certificate**.



The Regenerate HTTPS Certificate message appears. Click **Regenerate**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Import MCN configuration

March 12, 2021

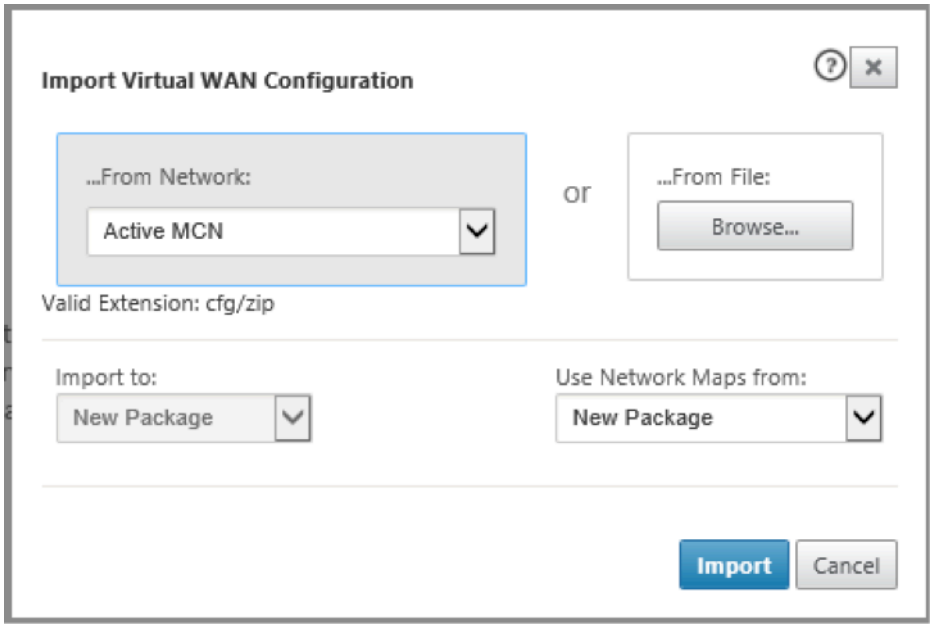
When Citrix SD-WAN Center is set up and a connection is established between the master control node (MCN) and Citrix SD-WAN Center, you can import the MCN configuration to Citrix SD-WAN Center and view the network maps.

The Import function imports a configuration into an open or new Citrix SD-WAN master configuration. If an Citrix SD-WAN master configuration is open when you use the import function, it and its maps are overwritten by the new Citrix SD-WAN master configuration. If no Citrix SD-WAN master configuration is open, an untitled package is created.

To import the MCN configuration to Citrix SD-WAN Center:

1. In the Citrix SD-WAN Center web interface click the **Configuration** tab.
2. Click **Network Configuration** and then click **Import**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



3. In the **From Network** field select one of the following options:

   - **Active MCN**: Connect to the active MCN and download the current Configuration.
   - **Other**: Connect to an IP address of a different MCN and download the current Configuration. You may have to install the security Certificate from this Citrix SD-WAN Center in the MCN before you can Import the Configuration.

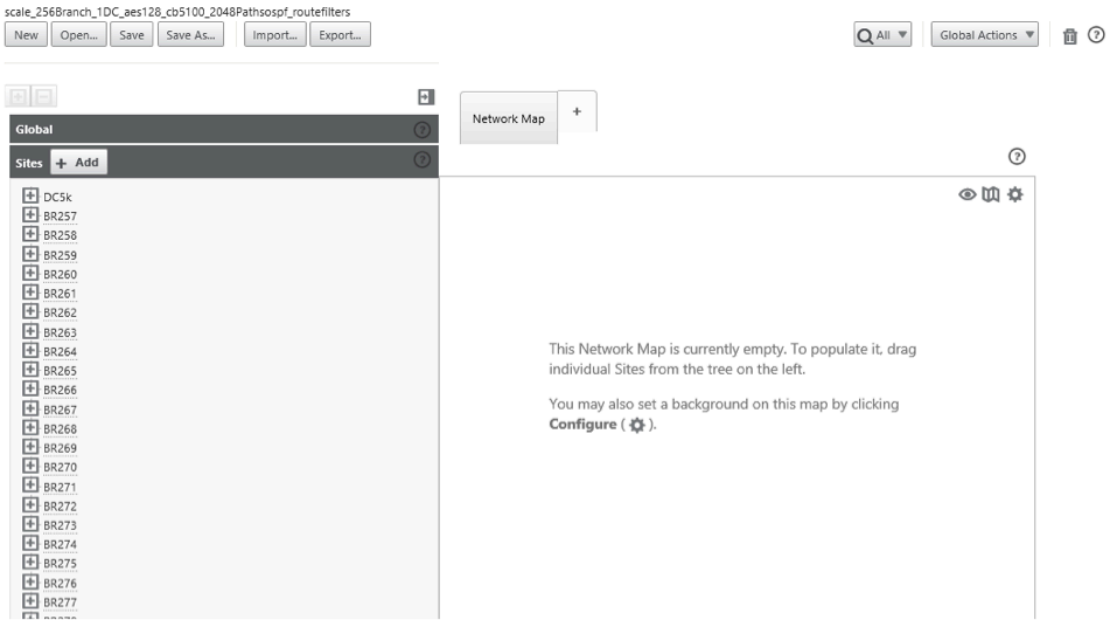
   For more information, see, Install the Citrix SD-WAN Center Certificate.

4. Alternatively, in the **From File** section, click **Browse** and select a Configuration to be uploaded from your computer.
5. In the **Import** to field select **Current Package** to import the contents of the selected file into the current open package.
6. In the **Use Network Maps from**, field select one of the following options.

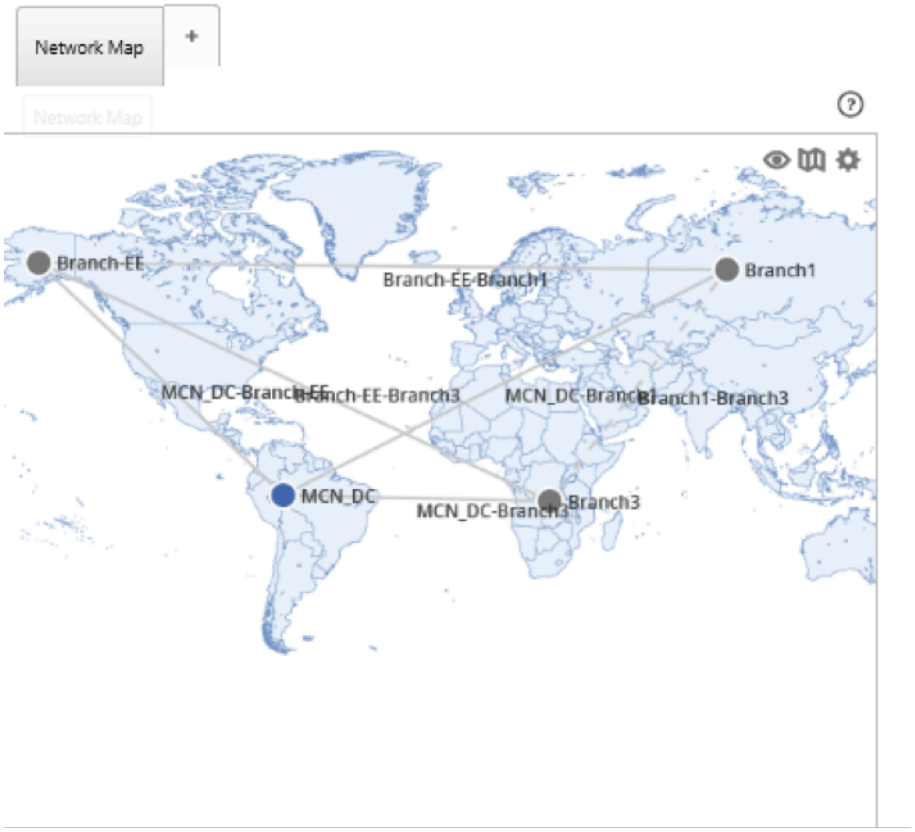
   - **Current Package**: Retain the currently saved set of network maps after the import.
   - **New Package**: Use the network maps from the imported package and discard the current set of maps.
   - **Both Packages**: Use the imported maps in addition to the currently saved maps.

7. Click **Import**. The configuration is imported.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



8. In the **Network Map** section. Click the settings icon and select **Auto populate** to automatically add and arrange each site in the configuration to the map.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Manage database

March 12, 2021

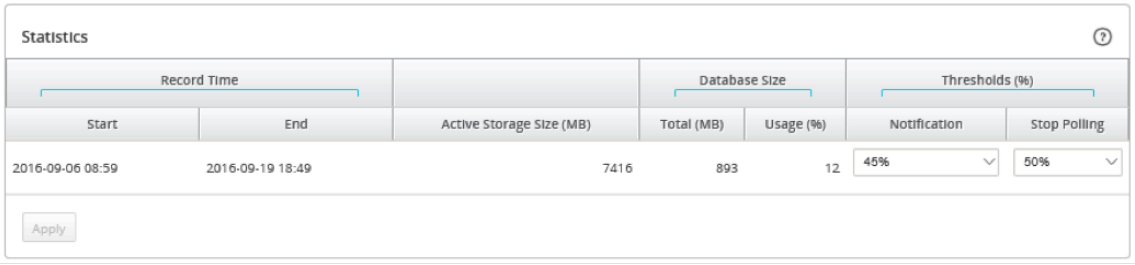
You can monitor and manage the database to ensure that there is enough available disk space to store the polling data from all the discovered appliances on the network.

Viewing database statistics

The **Statistics** table displays the available database statistics, and includes input fields for specifying the database disk usage thresholds for notifications and polling.

To view database statistics:

1. In the Citrix SD-WAN Center Web UI click the **Administration** tab.
2. Click **Database Maintenance**. Under **Statistics** section the following information is displayed.
    - **Record Time:** Displays the date and timestamp for the oldest and most recent records in the database. This column contains the following information:
        - **Start:** Displays the date and timestamp of the oldest record in the database.
        - **End**: Displays the date and timestamp of the most recent record in the database.
    - **Active Storage Size (MB)**: Displays the current active storage's disk space.
    - **Database Size (MB)**: Displays the current database size and use information. This column contains the following information:
        - **Total (MB)**: Displays the total size in MB of the database.
        - **Usage (%)**: Displays the percentage of database disk usage in current active storage's disk space.



To set the notification and polling threshold:

1. In the **Notification** field, enter the percentage of the database size or active storage size to use as a threshold for generating a database usage notification. An email notification will be sent when database use exceeds this threshold.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

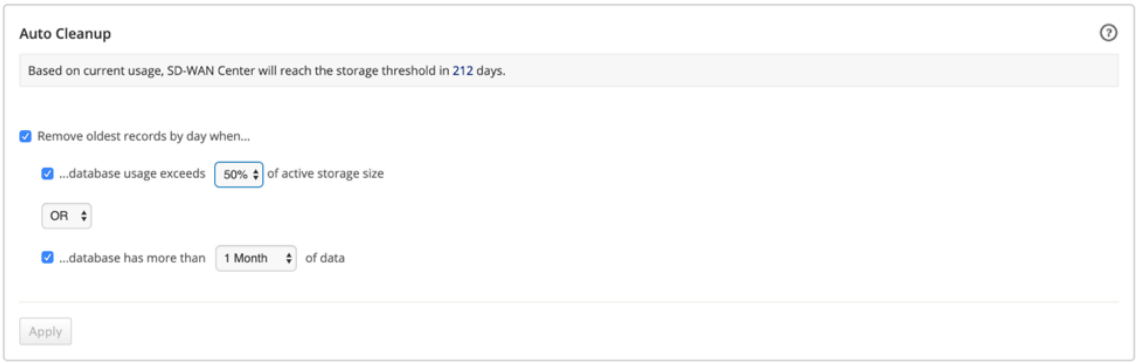
2. In the **Stop Polling** field, enter the database disk usage threshold (percentage) at which to stop statistics polling. Select a value from **10%** to **50%** from the drop-down menu. The default is **50%**.
3. Click **Apply**.

Configuring auto cleanup

To keep database disk usage under control, you can specify thresholds that, when exceeded, trigger the removal of older records from the database.

To enable database cleanup and configure the thresholds:

1. In the Citrix SD-WAN Center Web UI click the **Administration** tab.
2. Click **Database Maintenance**.
3. Under **Auto Cleanup** section, select the **Remove oldest records by day when…** check box to enable database cleanup.



When enabled, the database is automatically checked at 2:00 AM every day. The check initiates a database cleanup if the specified thresholds are met or exceeded. By default, this is not enabled.

Earlier, the default setting for SD-WAN Center database auto clean-up was as following:

- Remove oldest records by day when:
  - …database usage exceeds 50% of active storage size
  - Operator must be select as AND
  - …database has more than 6 months of data

With 11.1.1 release and above, the default setting for SD-WAN Center database auto clean-up has now changed to following:

- Remove oldest records by day when:
  - …database usage exceeds 50% of active storage size

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- Operator must be select as OR
- …database has more than 1 month of data

> **Note**
>
> The change in settings will have no impact for the already provisioned SD-WAN Center systems which are upgraded to 11.1.1 release. It is only applicable to freshly provisioned 11.1.1 release or above SD-WAN Center systems.

4. Select **…database usage exceeds (%) of active storage size** and then select a percentage from the drop-down menu to specify the threshold for a database cleanup. The options are from **10%** to **50%** in increments of **5%**.
5. Select **AND** or **OR**, an operator from the drop-down menu between the "…database usage exceeds…"and "…database has more than…"thresholds to specify an operator how to apply for this rule. The default is **OR** since 11.1.1 release.
6. Select **…database has more than** [# months] **months of data** and then select the number of months from the drop-down menu to specify the time span threshold for a database cleanup for which to keep data in the database. The options are from **1 month** to **12 months** in increments of one month.
7. Click **Apply**.

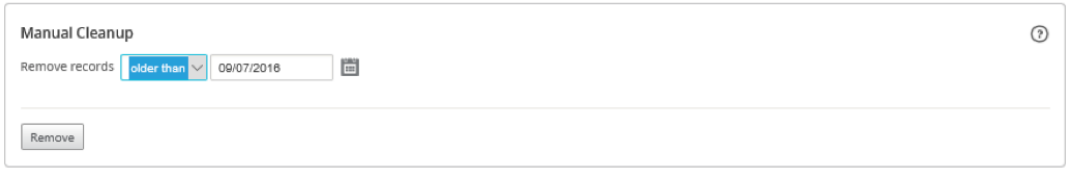
Configuring manual cleanup

You can manually remove statistics and events records from the database, based on specified criteria.

To perform a manual database cleanup:

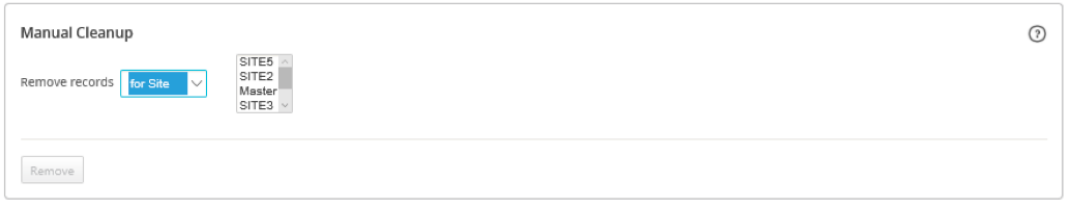
1. In the Citrix SD-WAN Center web interface click the **Administration** tab.
2. Click **Database Maintenance**.
3. Under **Manual Cleanup section** select a filter from the **Remove Records** drop-down menu. The filter options are:

   - **older than:** Remove records collected before a specified date. When you select this filter, a date field and calendar selection button appear. Click the calendar button to select a date. All records older than the specified date will be removed.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- **for Site:** Remove records collected before a specified date. When you select this filter, a date field and calendar selection button appear. Click the calendar button to select a date. All records older than the specified date will be removed.



4. Click **Remove**.

Manage views

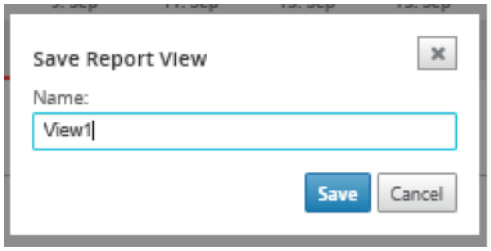
March 12, 2021

The Fault, Reporting, Network Map and Statistics page allows you to create, display, modify and delete the respective views.

> **Note**
>
> The screenshots used in the procedure may vary from the actual user interface depending on the type of the view.

To create a new view:

1. Click **New View**, this creates a new, unnamed view and resets the time specification to the current time.
2. Create and apply filters or make the necessary changes.
3. Click **Save As**.
4. In the **Save View** dialog box enter a name for your view.
5. Click **Save**.



To open and modify an existing view:

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

1. Click **Open**.
2. In the **Open View** dialog box, select a report view from the drop-down list.
3. Click **Open**. The event view opens.
4. Make the necessary modification as required.
5. Click **Save**.

To delete a view, open the view and click the delete icon.

Software upgrade

March 12, 2021

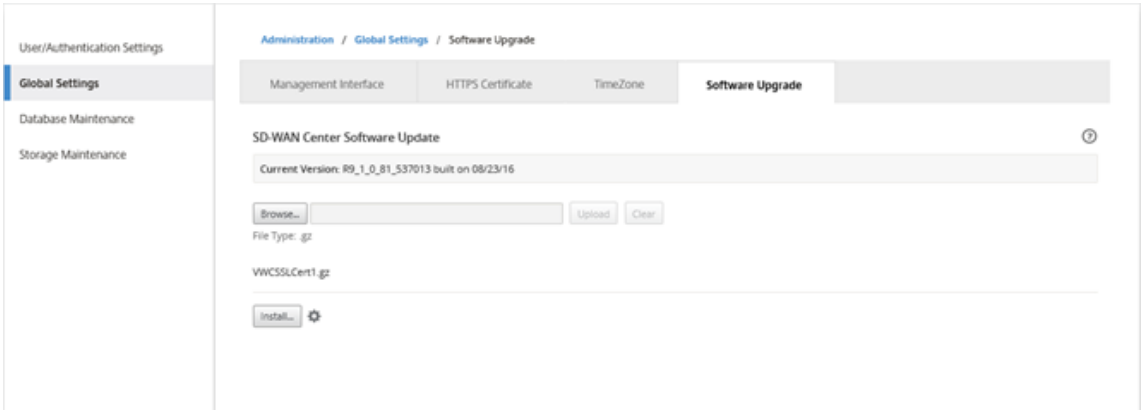
You can use the Software Upgrade option to upgrade your Citrix SD-WAN Center software to the latest version. The software upgrade process places Citrix SD-WAN Center into maintenance mode. If a database migration is required, this process can take several hours. During this time, no statistics data will be collected from the Virtual WAN, and all Citrix SD-WAN Center functionality will be unavailable.

> **Important**
>
> Running the upgrade during maintenance hours is recommended.
>
> **Note**
>
> Download the appropriate Citrix SD-WAN Center software package to your local computer. You can download this package from Downloads page.

To upload and install a new version of the Citrix SD-WAN Center software

1. In the Citrix SD-WAN Center web interface, click the **Administration** tab.
2. Click **Global Settings** and then click **Software Upgrade**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



3. Click **Browse** to open a file browser, and select the software package you want to upload.
4. Click **Upload** to upload the selected software package to the current Citrix SD-WAN Center virtual machine.
5. After the upload completes, click **Install**.
6. When prompted to confirm, click **Install**.
7. In the dialog box that appears, select the **I accept the End User License Agreement** checkbox, and then click **Install**.

Timeline controls

March 12, 2021

The Timeline at the top of the Fault, Reporting, Network Map and Statistics page provides controls for restricting the time frame of the current View. You can view a time frame of up to 30 days of data from the current database.

> **Note**
>
> Based on selected time period, you can view the historic data irrespective of the current Citrix SD-WAN network configuration.

Time

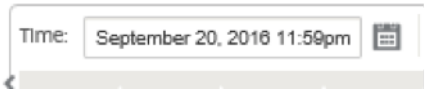
You can use the following elements for specifying a time frame for the current View:

- **Time** - Enter a date and time in the **Time** field to narrow the graph results to a specific date and time. The format can be any of the following:
  - ***Month Day, Year Hour:Minutes*** [**am** / **pm**] For example: September 7, 2015 2:00pm.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

  - ***MM/DD/YYYY HH:MM*** [**am** / **pm**] For example: 09/07/2015 8:36am.
  - ***M/D/YY H:MM*** [**am** / **pm**] For example: 9/7/15 10:14pm

- **Calendar** - (Calendar icon) Click the calendar icon to the right of the Time field and select a date to restrict the view results to that date.



- **Time line** - Click and drag to another point on a timeline to select a time frame of at least 30 minutes.

- **Last: Hour / Day / Week / Month** - Click an option (**Hour**, **Day**, **Week**, or **Month**) to restrict the view results to that time frame.

Mode

The Timeline mode determines how the timeline interprets time frame selections, and how automatic updates are reflected in the current view and on the Dashboard. There are two mode options, **Relative** (*selected time frame*)and **Absolute** (*selected time frame*), where selected time frame is the time frame specified in the **Time** field.

To change the Timeline mode, select either **Relative** or **Absolute** from the **Mode** drop-down menu at the top far right corner of the Timeline.

Relative Mode

If you select **Relative** mode, the Timeline treats the time frame specified for **Time** as a time relative to now. If you save the view and open it later, the information represented in the view will be relative to the time that the view was opened. If you have enabled automatic updates and a statistics update is detected, the view is updated relative to the latest time recorded in the database.

The currently specified time frame is shown in parenthesis as part of the **Relative** menu option. For example, if you selected **Last: Day** as the time frame, the **Relative** option displays as Relative (1 day ago - 1 minute from now).

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

Absolute Mode

If you select **Absolute** mode, the Timeline treats the time frame specified for **Time**: as absolute (static) points in time. The view will always represent the selected time, even if you save the view and open it at a later time, or if you enable automatic updates. The currently specified time frame is shown in parenthesis as part of the **Absolute** menu option, using the following format:

Absolute (*start_date start_time-end_date end_time*)

For example, if you selected **Last: Day** as the time frame, and the current date and time are 9/7 4:43 PM, the **Absolute** option displays as **Absolute (9/6 4:43 PM - 9/7 4:43 PM)**.

User accounts

March 12, 2021

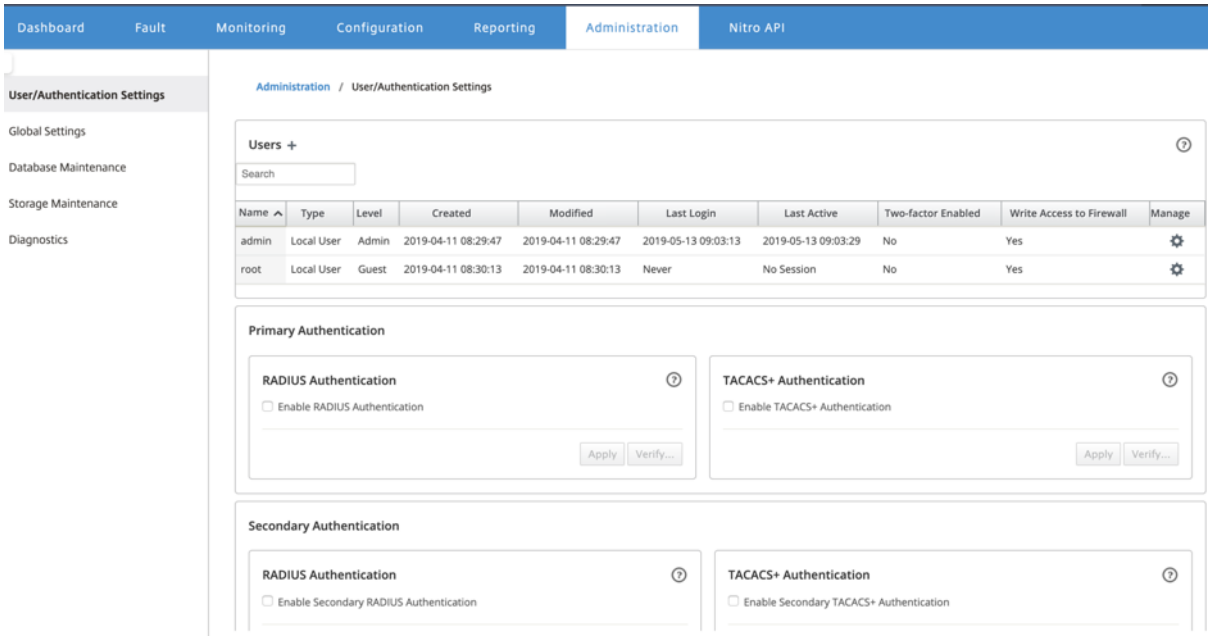
You can view a list of all local and remote user accounts that have logged into Citrix SD-WAN Center virtual machine at least once. Remote user accounts are authenticated through RADIUS or TACACS+ authentication servers. You can also add a new local user account to Citrix SD-WAN Center.

> **Note**
>
> If a user-account is available on a remote authentication server but is never used to log on to Citrix SD-WAN Center, it is not displayed in the **Users** list.

To view user accounts in the SD-WAN Center web interface, navigate to **Administration > User/Authentication Settings**.

A list of user accounts appears in the **Users** section.

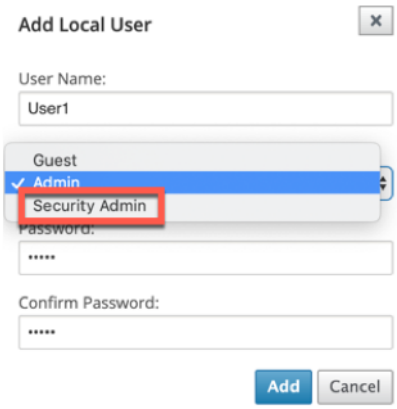
© 1999–2025 Cloud Software Group, Inc. All rights reserved.



The following information is displayed:

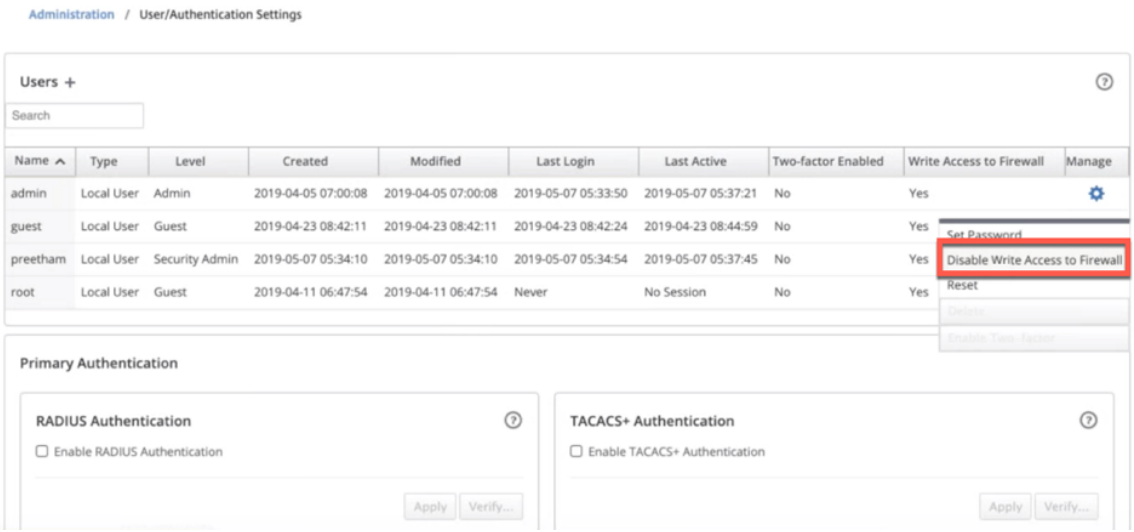
- **Name:** The user name.
- **Type**: The type of user account, it can be one of the following:
  - **Local:** User accounts created and managed locally using the SD-WAN Center interface.
  - **RADIUS**: Remote user accounts authenticated by the RADIUS server.
  - **TACACS+**: Remote user accounts authenticated by the TACACS+ server.
- **Level:** The following are three levels of account privilege:
  - **Admin**: Admin account has administrative privileges. It has read-write access to all the sections.
  - **Guest**: Guest account is a read-only account with access to **Dashboard**, **Reporting**, and **Monitoring** page.
  - **Security Admin**: A **Security Administrator** has the read-write access only for the Firewall and security related settings in **Config Editor**, while having read-only access to the remaining sections.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



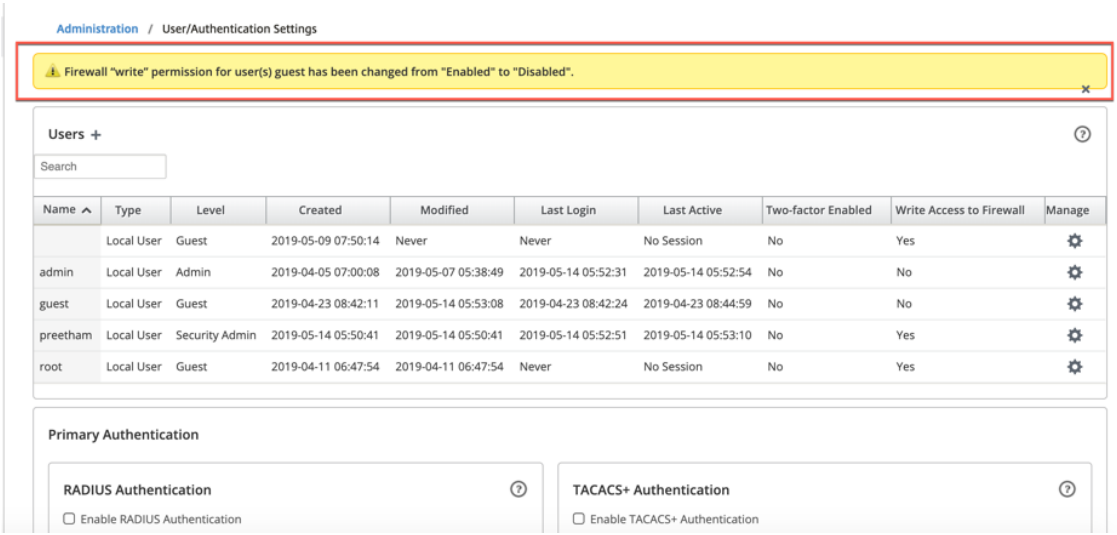
NOTE

* Only the administrator and security administrator can change or modify the security feature configuration.
* Security administrator can enable or disable the write access to the firewall for all user accounts except the super administrator.

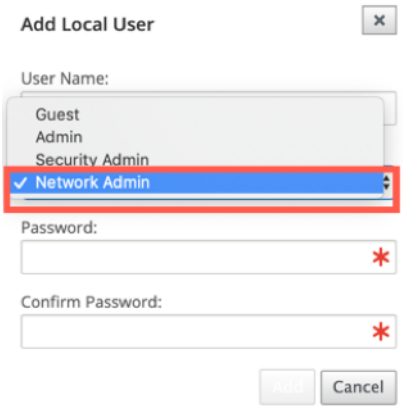


A notification bar appears to all the users after the security administrator changes the firewall write permission for any specific user. This notification is shown per user and hence each logged in user must acknowledge the warning for it to removed.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



- **Network Admin**: A **Network Administrator** has read-write permissions to all the sections and can fully provision a branch except for the firewall and security related settings in the Configuration Editor.



The hosted firewall node is not available for the network administrator. In this case, the network administrator must import a new configuration. Both network and security related settings are maintained by the super administrator (Admin).

The network administrator and security administrator can make changes to the configuration and also deploy it on the network.

> **NOTE**
>
> The network administrator and security administrator cannot add or delete user accounts. They can only edit their own account passwords.

- **Created**: For local user accounts, the date the user account was created. For a remote user account, the date of the first login session.
- **Modified**: For local user accounts, the date the password was last changed. For remote users, the date of the first login session.

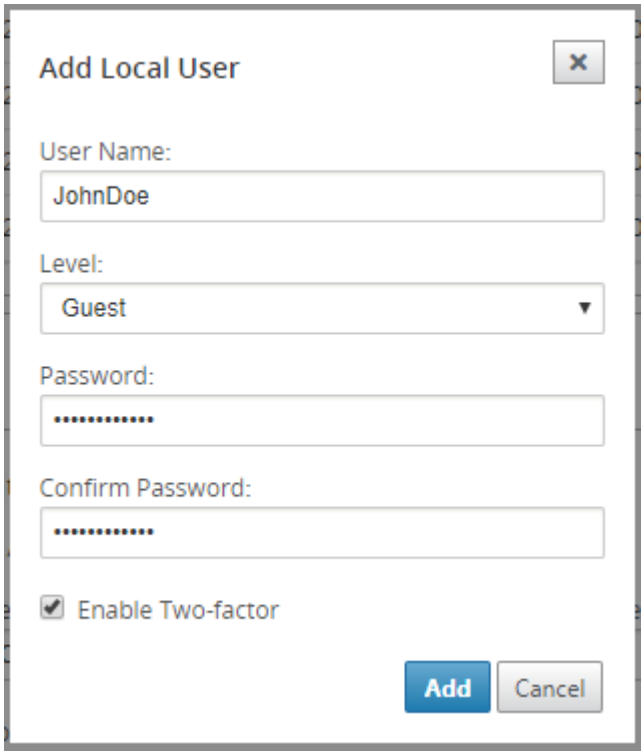
© 1999–2025 Cloud Software Group, Inc. All rights reserved.

- **Last Login**: The date the user last successfully logged in. A tooltip displays the IP Address of the device used to log in.
- **Last Active**: The date the last request was made to the server. A tooltip displays the IP Address of the device used to log in.
- **Manage:** Click the gear icon to view a menu containing the following options:
  - **Set Password**: Change Password for the local user account. The current root password is required to change the root password. You cannot change passwords of remote user accounts.
  - **Reset**: Remove the workspaces and preferences for this user account.
  - **Delete**: Delete the local user account, workspaces, and preferences from SD-WAN Center. You cannot delete remote and admin accounts.
  - **Two-factor Enabled:** Enable two-factor authentication for the local and remote user account. For more information, see two-factor authentication.
- **Write Access to Firewall**: Shows the Write Access to Firewall is enabled or disabled.

To add a new local user account to the Citrix SD-WAN Center:

> **Note**
>
> The user accounts created locally on Citrix SD-WAN Center do not have the privilege to edit and export the network configuration package to the MCN.

1. Click the add icon + next to **Users**. **The Add Local User** dialog box appears.



© 1999–2025 Cloud Software Group, Inc. All rights reserved.

2. Enter values for the following parameters:

   - **User Name**: The user name for the local user account.
   - **Level**: The account privilege. A guest user account is a read-only account limited to viewing dashboard, reports, and statistics. The guest user account does not have the privilege to edit and export the network configuration package to the MCN.
   - **Password**: The password for the user account.
   - **Confirm Password**: Reenter the password for confirmation.

3. Select **Enable Two-factor** to enable two-factor authentication for the local user account.

   > **Note**
   >
   > The **Enable Two-factor** option appears only when the secondary authentication server is configured.
   >
   > Configure a secondary authentication server, either RADIUS, or TACAS+ authentication. Ensure that the user account is configured on the secondary authentication server. For more information, see Secondary authentication.

4. Click **Add**. The new user account is created and the account information is added to the **Users** table.

> **Note**
>
> Citrix SD-WAN Center can have up to 600 local users.

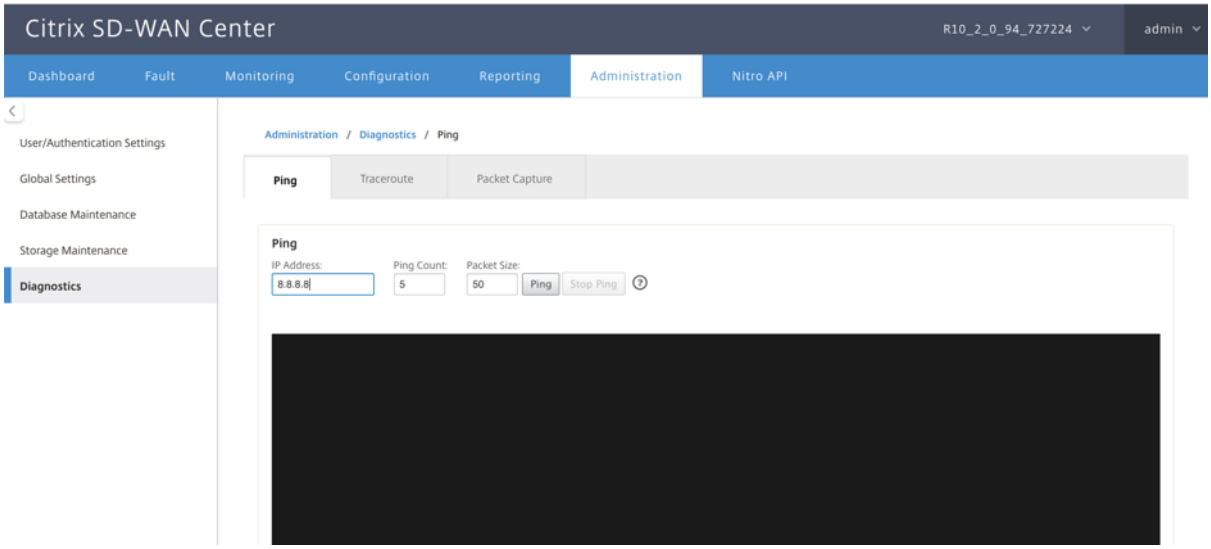
Diagnostics

March 12, 2021

Citrix SD-WAN Center Diagnostics utilities provide Ping, Traceroute, and Packet Capture feature to test and investigate connectivity issues on Citrix SD-WAN Center appliance. The diagnostic options in the **Citrix SD-WAN Center dashboard control data** collection.

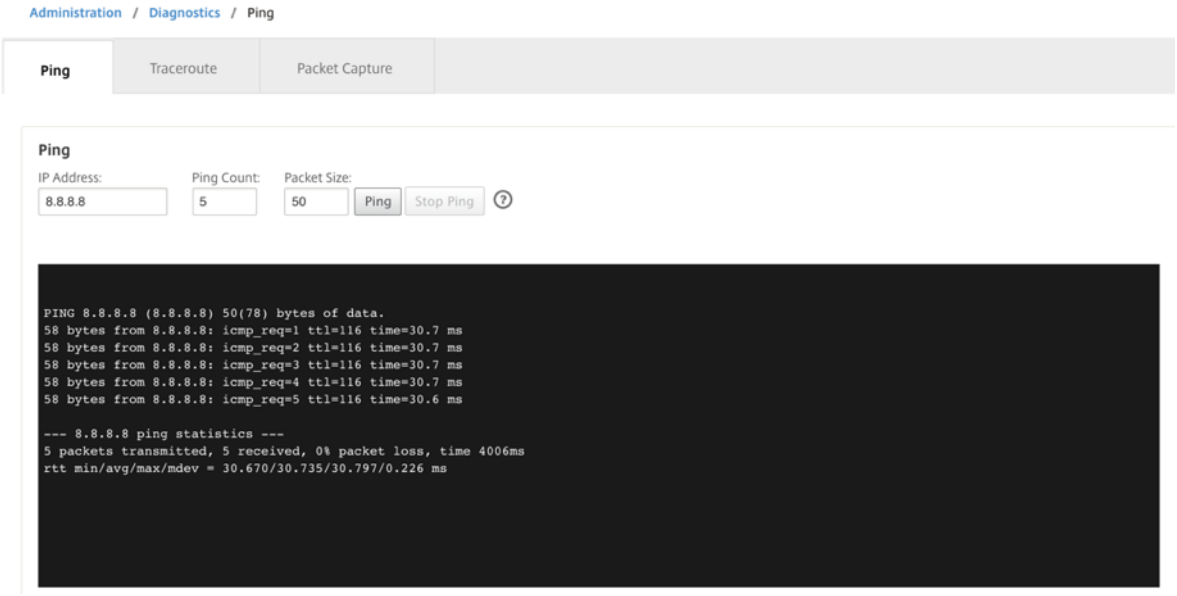
To use the Diagnostics tool, navigate to **Administration > Diagnostics**.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Ping

You can ping any management IP address in the SD-WAN Center network using the **Ping** option.

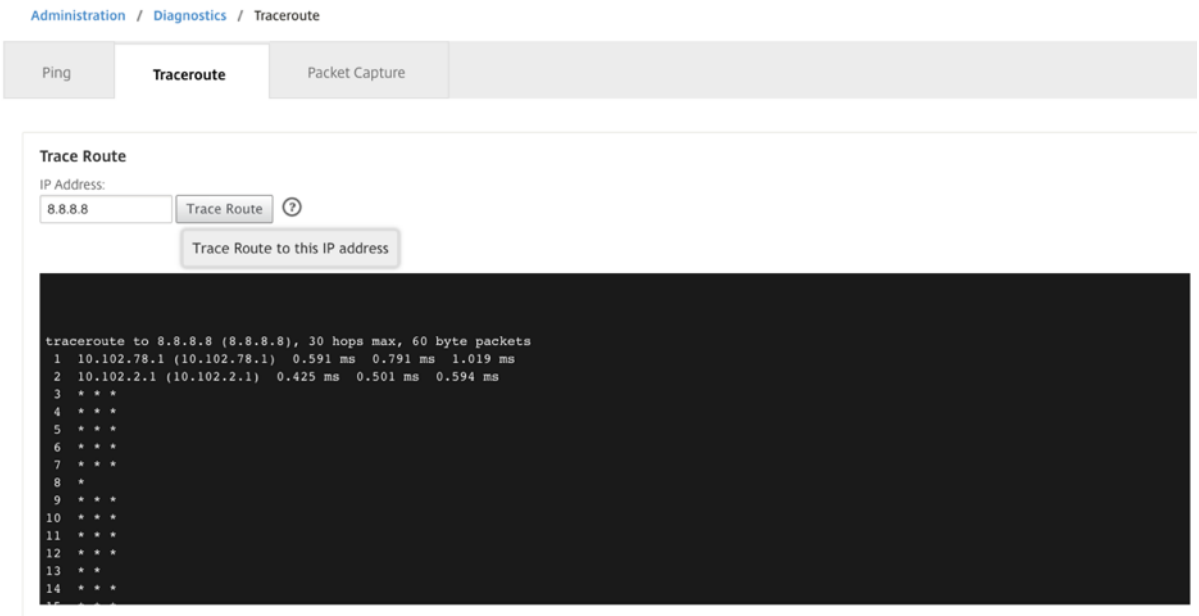


Provide a valid IP address along with the number of ping counts (amount of times to send the ping request) and packet size (number of data bytes). Click **Stop Ping** to stop an ongoing ping search.

Traceroute

Use the **Traceroute** option to ensure that the IP addresses are reachable. You can traceroute any management IP address in the network by displaying the route and measuring transit delays of packets.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



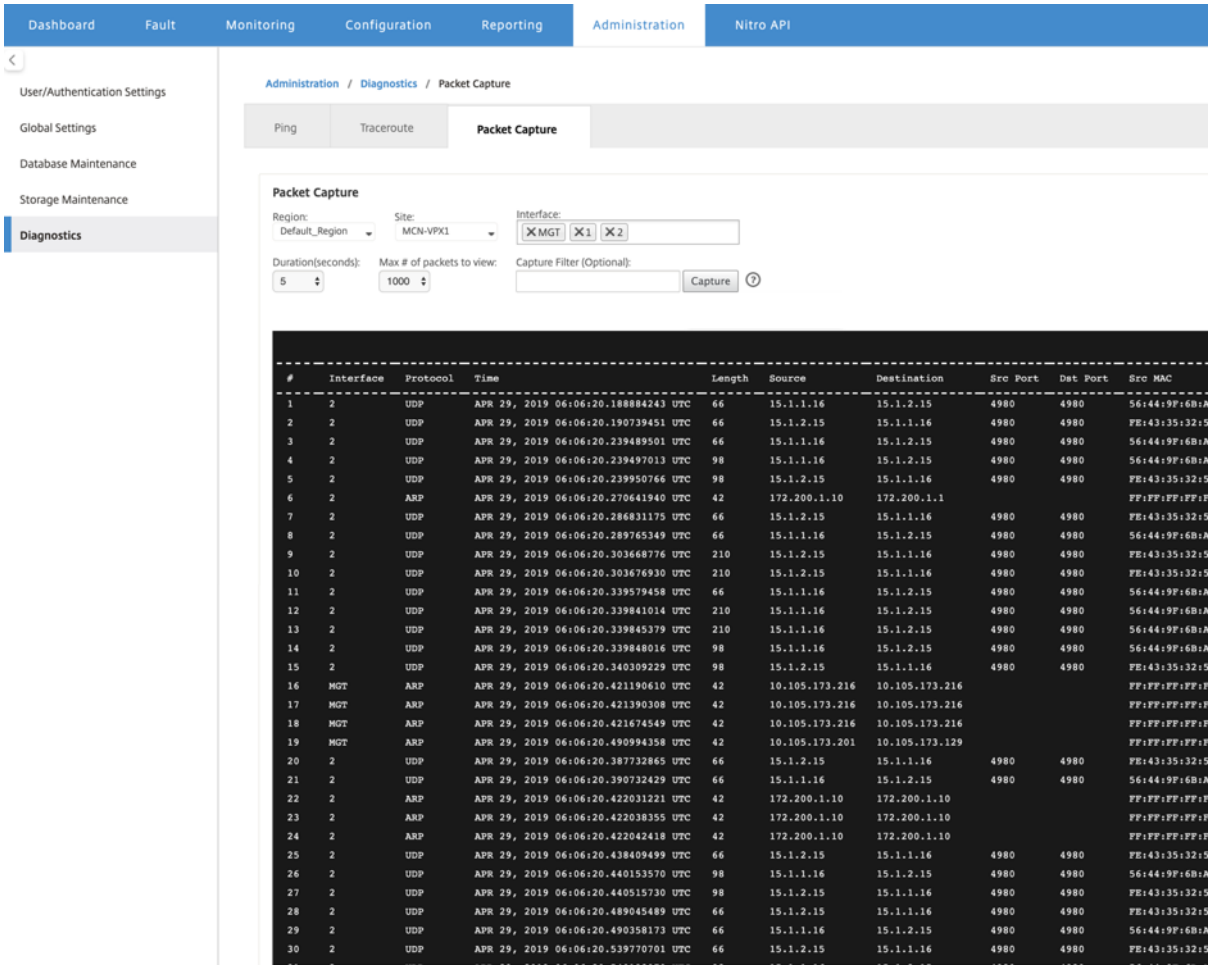
Enter a valid management IP address to trace route. Click **Trace Route**.

> **NOTE:**
>
> The traceroute result display maximum 30 hops.

Packet capture

Use the **Packet Capture** option to intercept the data packet that is traversing over the selected active interface present in the selected site.

© 1999–2025 Cloud Software Group, Inc. All rights reserved.



Provide the following inputs for packet capture operation:

- **Region** - Select a region that is managed by the SD-WAN Center from the drop-down list.
- **Site** - Available sites in the selected region. Select a site from the drop-down list.
- **Interface** - Active interfaces are available for packet capture in the selected site. Select an interface or add interfaces from the drop-down list. At least select one interface to trigger a packet capture.

  > **NOTE:**
  >
  > The ability to run packet capture across all the interfaces at once helps to speed up the troubleshooting task.

- **Duration(seconds)** –Duration (in seconds) for how long the data have to be captured.
- **Max # of packets to view** - Maximum limit of packets to view in the packet capture result.
- **Capture Filter (Optional)** - The optional **Capture Filter** field accepts a filter string that is used to determine which packets are captured. Packets are compared to the filter string and if the

© 1999–2025 Cloud Software Group, Inc. All rights reserved.

comparison result is true, then the packet is captured. If the filter is empty, then all packets are captured. For more information, see Capture Filters.

Following are some examples of this capture filter:

- **Ether proto\ARP** - Captures only ARP packets
- **Ether proto\IP** - Captures only IPv4 packets
- **VLAN 100** - Captures only packets with a VLAN of 100\
- **Host 10.40.10.20** - Captures only IPv4 packets to or from the host with the address 10.40.10.20
- **Net 10.40.10.0 Mask 255.255.255.0** - Captures only IPv4 packets in the 10.40.10.0/24 sub-net
- **IP proto \ TCP** - Captures only IPv4/TCP packets
- **Port 80** - Captures only IP packets to or from port 80
- **Port range 20–30** - Captures only IP packets to or from ports 20 through 30
- **Host 10.40.10.20 and Port 80 and TCP** - Captures only IP packets to or from TCP port 80 on the host 10.40.10.20

> **Note:**
>
> The maximum capture file size limit is up to 575 MB. Once the packet capture file reaches this size, packet capturing is stopped.

Click **Capture** to view the packet capture result.

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.