NetScaler SD-WAN Center 10
Contents

System requirements and installation 3
Install and configure NetScaler SD-WAN Center on ESXi Server 7
Install and configure NetScaler SD-WAN Center on XenServer 21
Single-Region Network Deployment 28
Multi-Region Network Deployment 31
Configuration 37
Configure the management interface settings 37
Install the NetScaler SD-WAN Center certificate 38
Switch the active storage to new data storage 39
Deploy NetScaler SD-WAN appliance 41
Configure NetScaler SD-WAN appliances 41
Configuration Editor 41
Change Management Wizard 43
Appliance settings 45
NetScaler SD-WAN Center as a license server 47
Zero Touch Deployment 50
On-prem zero touch 71
AWS 71
Azure 82
Proxy Server Settings for zero touch deployment 102
Monitoring 104
SD-WAN Center Dashboard 104
Diagnostic packages 116

© 1999-2020 Citrix Systems, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Events</td>
<td>119</td>
</tr>
<tr>
<td>Event notifications</td>
<td>122</td>
</tr>
<tr>
<td>Memory dumps</td>
<td>127</td>
</tr>
<tr>
<td>Log files</td>
<td>128</td>
</tr>
<tr>
<td>Polling interval</td>
<td>129</td>
</tr>
<tr>
<td>Statistics</td>
<td>130</td>
</tr>
<tr>
<td>System information</td>
<td>132</td>
</tr>
<tr>
<td>Reporting</td>
<td>133</td>
</tr>
<tr>
<td>Application report</td>
<td>136</td>
</tr>
<tr>
<td>Bandwidth report</td>
<td>137</td>
</tr>
<tr>
<td>Class report</td>
<td>138</td>
</tr>
<tr>
<td>Ethernet interface report</td>
<td>140</td>
</tr>
<tr>
<td>Event report</td>
<td>141</td>
</tr>
<tr>
<td>GRE tunnel report</td>
<td>143</td>
</tr>
<tr>
<td>HDX report</td>
<td>145</td>
</tr>
<tr>
<td>IPsec tunnel report</td>
<td>146</td>
</tr>
<tr>
<td>Link performance report</td>
<td>148</td>
</tr>
<tr>
<td>MOS for applications</td>
<td>150</td>
</tr>
<tr>
<td>MPLS queues report</td>
<td>151</td>
</tr>
<tr>
<td>Administration</td>
<td>153</td>
</tr>
<tr>
<td>Configure date and time</td>
<td>154</td>
</tr>
<tr>
<td>Configure RADIUS Authentication</td>
<td>155</td>
</tr>
<tr>
<td>Configure TACACS+ Authentication</td>
<td>157</td>
</tr>
<tr>
<td>HTTPS certificates</td>
<td>159</td>
</tr>
<tr>
<td>Feature</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------</td>
<td>------</td>
</tr>
<tr>
<td>Import MCN configuration</td>
<td>161</td>
</tr>
<tr>
<td>Manage database</td>
<td>164</td>
</tr>
<tr>
<td>Manage views</td>
<td>166</td>
</tr>
<tr>
<td>Software upgrade</td>
<td>167</td>
</tr>
<tr>
<td>Timeline controls</td>
<td>168</td>
</tr>
<tr>
<td>User accounts</td>
<td>170</td>
</tr>
</tbody>
</table>
System requirements and installation

June 10, 2019

Before you install NetScaler 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 mutli-region network.

Hardware requirements

NetScaler 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 NetScaler SD-WAN Center data storage. Use direct access storage.

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

**Network bandwidth**

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

Estimated network bandwidth requirements
## Client Sites

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

## Software

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

Hypervisor
NetScaler SD-WAN Center 10

- VMware ESXi server, version 5.5.0 or higher.
- NetScaler XenServer 6.5 or higher.
- Microsoft Hyper-V 2012 R2 or higher.

Cloud Platform

- Microsoft Azure

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

The NetScaler 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 NetScaler SD-WAN Center:

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

Note

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

Download NetScaler SD-WAN Center software

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

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

cctx-sdwc-version_number-platform.extension

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

<table>
<thead>
<tr>
<th>Platform</th>
<th>File extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler XenServer</td>
<td>.xva</td>
</tr>
</tbody>
</table>
Gather the NetScaler SD-WAN Center installation and configuration information

This section provides a checklist of the information you will need to complete your NetScaler 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 NetScaler SD-WAN Center Virtual Machine (VM).
- A unique name to assign to the NetScaler SD-WAN Center VM.
- The amount of memory to allocate for the NetScaler SD-WAN Center VM.
- The amount of disk capacity to allocate for the virtual disk for the VM.
- The Gateway IP Address the NetScaler SD-WAN Center will use to communicate with external networks.
- The subnet mask for the network in which the NetScaler SD-WAN Center VM will be installed.

Install and configure NetScaler SD-WAN Center on ESXi Server

September 24, 2018

Install the VMware vSphere client

Following are basic instructions for downloading and installing the VMware vSphere client that you will use to create and deploy the NetScaler 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 will host your vSphere Client and NetScaler SD-WAN Center Virtual Machine (VM) instance.
   
   The VMware ESXi Welcome page appears.
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 just 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 will host your NetScaler 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 NetScaler SD-WAN Center VM using OVF template

After installing the VMware vSphere client, create the NetScaler SD-WAN Center virtual machine.

1. If you have not already done so, download the NetScaler 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 NetScaler 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.

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*. 
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 could 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 NetScaler 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, do the following:

   1. On the vSphere client Inventory page, select the new NetScaler SD-WAN Center VM in the Inventory tree (left pane).
2. On the NetScaler 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 NetScaler SD-WAN Center VM are as follows:

   - Login: admin
   - Password: password
6. Record the NetScaler 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 completed.

If the DHCP server is not configured in the SD-WAN network, you have to manually enter a static IP
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 NetScaler 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 NetScaler 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 NetScaler SD-WAN Center VM host server.
3. In the left pane, click + next to the IP Address for the server hosting the NetScaler SD-WAN Center VM you just created.
4. Open the new NetScaler SD-WAN Center VM for editing.
5. In the **Inventory** tree, right-click on the name of the NetScaler SD-WAN Center VM you just created and select **Edit Setting** from the drop-down menu.
6. In the Memory Size field, enter the amount of memory to allocate for 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.
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
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**.
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**.
Install and configure NetScaler SD-WAN Center on XenServer

September 24, 2018

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

To install the NetScaler XenServer server on which you will deploy the NetScaler 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 NetScaler SD-WAN Center VM instance.
   - **Username**: 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.
Create the NetScaler SD-WAN Center VM using the XVA file

The NetScaler 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 NetScaler 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.
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.
more information see Add and configure the Datastore on XenServer

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

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

**View and record the management IP address on XenServer**

The management IP address is the IP address of the NetScaler SD-WAN Center VM, use this IP address to log into the NetScaler 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 NetScaler SD-WAN Center VM and select **Start**.

2. When the VM is started, click the **Console** tab.
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 NetScaler SD-WAN Center VM are as follows:

   **Login**: admin
   **Password**: password

   If the DHCP server is not configured in the NetScaler 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 NetScaler 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 NetScaler SD-WAN center.

To add and configure the data storage:

1. In XenCenter, shut down the NetScaler SD-WAN Center VM.

2. On the **Storage** tab, click **Add**.
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**.

**Single-Region Network Deployment**

February 20, 2019

If your organization has a small network spanning a single administrative (or geographical) boundary, you can use 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 SD-WAN Center for centralized management. The region associated with and controlled by the MCN is referred to as the default region. The SD-WAN Center polls the MCN and all the branch appliances in the default region.
To deploy SD-WAN Center for single-region:

1. Download the NetScaler SD-WAN Center Software. For more information, see System Requirements and Installation.

2. Install the NetScaler SD-WAN Center on ESXi Server or XenServer

3. Configuring the management interface settings. For more information, see Configuring the Management Interface Settings.

4. Install the SD-WAN Center Certificate on the MCN. For more information, see Installing the SD-WAN Center Certificate

5. In the SD-WAN Center GUI navigate to Configuration > Network Discovery > Discover Settings.

Note
Do not select Enable Multi-region mode.
6. 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 SD-WAN Center.

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

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

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

9. 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.
1. Click **Apply**.

   1 > **Tip**
   2 >
   3 > You can increase the storage size of the SD-WAN Center by creating a data store on your virtual machine and switching the data store. For more information see, [Switching the Active Storage to the New Data storage](/en-us/netscaler-sd-wan-center/10/common-configuration/switch-active-storage-to-new-data-storage.html).

**Multi-Region Network Deployment**

February 20, 2019

If your organization has a large network spanning multiple administrative (or geographical) boundaries, you can use 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.

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

The multi-region 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.

To deploy SD-WAN Center for Multi-region:
1. Download the NetScaler SD-WAN Center Software. For more information, see System requirements and Installation.

2. Install the NetScaler SD-WAN Center on ESXi Server or XenServer

3. Configuring the management interface settings. For more information, see Configuring the Management Interface Settings.

4. Log-into the SD-WAN Center interface.

5. Download the SSL Certificate from the SD-WAN Center VM and install it on the MCN appliance. For more information, see Installing the SD-WAN Center Certificate.

6. In the SD-WAN Center GUI navigate to Configuration > Network Discovery > Discover Settings, and select Enable Multi-region mode.

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 SD-WAN Center.

8. Click Discover Regions. A list of all the RCNs connected to the MCN appears in the Collector Configuration section.

**Note**
The 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 SD-WAN Center that you want to configure as a collector for a region.

**Note**

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

13. Select all the RCNs and click Discover.

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.

14. 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 the New Data storage.

For Multi-region deployment, you can select specific regions to view event and statistic reports.

The events and statistic reports data is fetched from the respective region’s collector.
The initial few steps to configure NetScaler 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 NetScaler SD-WAN Center certificates
- Switch the active storage to new data storage.

### Configure the management interface settings

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

The management Interface settings include the following:

- NetScaler SD-WAN Center Management IP Address
- Gateway IP Address
- Subnet Mask
- Primary DNS
- Secondary DNS
To configure the management interface settings:

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

4. Click **Apply**.

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

### Install the NetScaler SD-WAN Center certificate

**September 24, 2018**

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

To download and install the NetScaler SD-WAN certificate:

1. In the NetScaler SD-WAN Center web interface, on the **Configuration** tab, select **Network Discovery**.
2. On the SSL Certificate page, click **Download Certificate**. This opens a file browser on your computer for selecting the download location. Navigate to the desired location and save the certificate.

3. Log into the NetScaler SD-WAN Master Control Node web interface.

4. Click the **Configuration** tab.

5. In the navigation tree (left pane), click the + icon next to the **Virtual WAN** branch.

6. Select **SD-WAN Center Certificates**.

7. On the SD-WAN Center Certificates page, next to the **Install Certificate** field, click **Browse**. This opens a file browser on the local PC for selecting the file you want to upload. Select the certificate file you just downloaded, and click **Open**.

8. Click **Upload and Install**. This uploads the certificate file to the master control node (MCN) and displays a success message when installation is complete.

9. Click **Continue**. This displays the MCN Management Web Interface Dashboard page. At this point, you can log out of the MCN (optional).

**Switch the active storage to new data storage**

September 24, 2018

In NetScaler 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 NetScaler 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 NetScaler SD-WAN Center VM:

1. Log into NetScaler SD-WAN Center VM.
   
   The default login credentials for NetScaler 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.

   This places NetScaler 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 NetScaler SD-WAN appliance

September 24, 2018

You can use NetScaler 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 NetScaler SD-WAN appliances.

You can configure NetScaler 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 NetScaler SD-WAN Center as a license server.

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

Configure NetScaler SD-WAN appliances

September 24, 2018

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 NetScaler SD-WAN Center. For more information see, Change Management Wizard.

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

Configuration Editor

September 24, 2018

The Configuration Editor is available as a component of the NetScaler SD-WAN Center Web Interface, and in the NetScaler 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 NetScaler SD-WAN
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 NetScaler SD-WAN Center appliance and the MCN, to edit the configurations on NetScaler SD-WAN Center and to export and install the configurations on the MCN.

For detailed instructions on using the Configuration Editor to configure your NetScaler SD-WAN, see NetScaler SD-WAN Center 10 documentation.

The Configuration Editor enables you to do the following:

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

To open the Configuration Editor:

1. In the NetScaler 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.

   ![Configuration Editor Menu Bar](image)

   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 drop-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.

## Change Management Wizard

September 24, 2018

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

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

To open the Change Management Wizard:

1. In the NetScaler 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.

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.

- **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

September 24, 2018

You can configure appliance setting on NetScaler SD-WAN Center and export it to a set of managed NetScaler 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.
NetScaler SD-WAN Center 10

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

![Citrix SD-WAN Center](image)

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.
Note

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

6. Click Export.

NetScaler SD-WAN Center as a license server

December 18, 2018

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 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 NetScaler SD-WAN edition that the license supports.
- **Maintenance Expiry**: The expiry date of NetScaler 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 NetScaler SD-WAN appliances and save it on your local computer.

**Note**

For instructions on obtaining a NetScaler SD-WAN software license, contact NetScaler 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 NetScaler SD-WAN Center.

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

---

The following parameters are displayed:

- **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 NetScaler Subscription Advantage.
- **License Expiry**: The expiry date of the license.
Zero Touch Deployment

March 15, 2019

Note

The Zero Touch Deployment service is supported only on select NetScaler SD-WAN appliances:

- 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 2000 Standard 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 NetScaler 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 NetScaler 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 NetScaler SD-WAN appliances.

ZTD High-Level Architecture and Workflow

Data Center Site

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

- Configuration creation using NetScaler SD-WAN Center Network Configuration tool, or import of configuration from the Master Control Node (MCN) SD-WAN appliance
- NetScaler 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 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.netscalernetworkapi.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 NetScaler 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.
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.
- NetScaler 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 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 installs 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 NetScaler 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 pro-
cess, 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 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 NetScaler Workspace Cloud to enable ZTD service. The Zero Touch Deployment menu option is now displayed in the SD-WAN Center web management interface.
- 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.

![Citrix SD-WAN Center interface](image)

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 NetScaler Workspace Cloud** button if a NetScaler Cloud account has already been created.

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

![Citrix Cloud Login Successful](image)

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

- Open a web browser to [https://onboarding.cloud.com](https://onboarding.cloud.com)
- Click on the link for **Wait, I have a NetScaler.com account.**
i) Sign-in with an existing NetScaler 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).

**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 NetScaler SD-WAN Center
• Make sure the web browser is not blocking any pop-up windows during the NetScaler 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.

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 configured sites.

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

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

h) 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.

i) 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.
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 is not required to enter serial number into the activation URL generated with the deploy site command
- If Serial Number field is left blank – 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 temporarily 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.
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 appliance 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
- 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.
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).
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.
i) At this point the SD-WAN Network Administrator can gain web management access to on-site appliance utilizing the SD-WAN overlay network.

Remote GUI access through Virtual Path

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.
k) The appliance configuration can be validated using the **Configuration > Virtual WAN > View Configuration** page.
The appliance license file can be updated to a permanent license using the **Configuration > Appliance Settings > Licensing** page.

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

September 24, 2018

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

AWS

September 24, 2018

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
NetScaler SD-WAN Center 10

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

Cloud Topology with NetScaler SD-WAN

This is an example deployment of a SD-WAN cloud deployed site, the NetScaler 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.
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.

![Sites tile](image)

View: Global  Sites

Filter Sites:

![Site list](image)

- DC
- AWS-SE
- Azure-SE
- Branch
- DavidS410
- ZTDBR1000
- ZTDBR2000
- ZTDBR2100
- ZTDBR410

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.
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
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 NetScaler 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**.
d) A pop-up window will appear, where the NetScaler 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.

![Provision and Deploy](image)

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

![Provision and Deploy AWS](image)

**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 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 temporarily 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.

   ![Email Image]

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

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

![Zero Touch Deployment Service](image)


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.
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).
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.
Azure

September 24, 2018

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,
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 NetScaler 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.
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 build 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.
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.
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.
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 NetScaler 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 NetScaler 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 **Provision and Deploy**.

4. A pop-up window will appear, where the NetScaler SD-WAN Admin can initiate the deployment for Zero Touch. Validate that the site name complies with the requirements on Azure (lower-case 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**.
5. After clicking **Next**, the Provision and Deploy Azure (step 1 of 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**.

![Provision and Deploy](image)

a) On the Azure account, we can identify the required **Subscription ID** by navigating to “More Services” and select **Subscriptions**.
b) To identify the required Application ID, navigate to Azure Active Directory, Application registrations, and click New application registration.
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.
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.
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).
i) Copy and save the secret key (note you will not be able to retrieve this later).

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

k) Copy the Federation Metadata Document, to identify your Tenant ID (note the Tenant
ID 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 NetScaler Zero Touch Deployment Service.

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

September 24, 2018

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

**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**.

**Note**

You can remove the proxy server settings altogether, if the NetScaler 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 NetScaler 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**.

**Monitoring**

September 26, 2018

The NetScaler 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 NetScaler SD-WAN Center.

Monitoring related articles:

- Diagnostic Packages
- Event Notifications
- Log Files
- Memory Dumps
- Polling Interval
- Statistics
- System Information

**SD-WAN Center Dashboard**

October 25, 2018
The SD-WAN Center Dashboard displays a subset of the common statistics at a glance. The application and site specific statistics are obtained from the MCN that is discovered in the SD-WAN Center. The following widgets are available on the Dashboard:

- Network Map
- Top Application and Top Application Families
- Network HDX: Quality Summary
- Network HDX: Users and Sessions
- Network HDX: Bottom 5 Sites
- Site HDX: Users
- Site HDX: Sessions
- Site HDX: QoE
- Network Health: Virtual Path Report
- Current Events
- Inventory Manager
- SD-WAN Center: Alarm Summary
- SD-WAN Center: Database Usage
- SD-WAN Center: Active OS Usage

All the widgets are displayed on the dashboard by default. You can customize the dashboard by closing the widgets that you do not want to view and by arranging the widgets as per your requirement. To view all the widgets as per the default settings, click **Reset Dashboard**.

The SD-WAN Center Dashboard is refreshed based on the configured polling interval. The default polling interval is 5 minutes. For more information see, How to Configure Polling Interval.

If SD-WAN Center is deployed in multi-region mode, you can select the region for which you want to view the dashboard. In the **Region** drop-down list, select All to view the multi-region summary dashboard. This provides an overview of the network health at the various regions.
NetScaler SD-WAN Center 10

Click a region card to view a detailed dashboard of the region

Note
In single-region network deployment, the Region drop-down list is not available.

Network Map
You can view the network maps in either the tile view or the schematic view.

Tile View
The tile view provides the following information:

- The total number of sites in a region.
- The number of sites in Poor state. A site is in Poor state if at least one virtual path is DOWN.
- The number of sites in Fair state. A site is in Fair state if 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 Good state. A site is in Good state if all the virtual paths and the associated member paths are UP.
- The number of sites in Unknown state. A site is in Unknown state if polling is in progress.

To view a graphical representation of a path between two sites, select the path and click Visualize.
Hover the mouse cursor over the sites or the path to view more details. Click the sites to view 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. In order to view a network map here, you must import the network configuration and Network maps from the Master Controller Node (MCN). For more information, see How to Import Network Configuration from MCN to SD-WAN Center.

Hover the mouse cursor over the sites or the path to view more details. Click the sites to view report options.
Top Applications and Top Application Families

Deep packet inspection (DPI) allows the SD-WAN appliance to parse the traffic passing through it and identify the application and application family types. The top results of the parsed traffic is displayed in this widget.

The SD-WAN Center dashboard displays the top applications and top application families. You can select the site and time interval as last 24 hours, last 1 hour, or last 5 minutes.

Network HDX: Quality Summary

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 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 Application QoE.

The HDX traffic is classified into the following three quality categories:

<table>
<thead>
<tr>
<th>Quality</th>
<th>QoE Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good</td>
<td>80-100</td>
</tr>
<tr>
<td>Fair</td>
<td>50-80</td>
</tr>
<tr>
<td>Poor</td>
<td>0-50</td>
</tr>
<tr>
<td>No HDX Traffic</td>
<td>N/A</td>
</tr>
</tbody>
</table>

You can click on the chart to view HDX reports per site. For more information, see How to View HDX Reports.

Note

Sometimes, the HDX dashboard data and HDX reports from different sites may not seem to be in sync because each site statistics are polled independently. The out of sync could happen when some sites stats are polled and refreshed but other sites are not polled yet.

On HDX dashboard widgets, you may see a site with no HDX traffic, but there may be a non-zero number of HDX sessions and users. This could happen when the HDX sessions remain idle for that polling period, and still stay in open state.
**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.

**Network HDX: Bottom 5 Sites**

This widget provides a list of the bottom 5 sites that have the least scoring QoE to help 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.

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.

Current Events

The Current Events section of the dashboard displays the events from all the discovered appliances in the network, that occurred in the last one hour. The output of events can be filtered using the Routing Domain drop-down menu. The information displayed in this section is gathered from the Fault tab. For more information, see Events.
Inventory Manager

Once every 30 minutes, the Inventory Manager gathers the hardware information collected from all the SD-WAN appliances that have been discovered by the SD-WAN Center VM. The Inventory Manager page displays this data in columns that you select and filter. The following columns are available:

- **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. The name is a link to connect to the appliance management 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. The IP address is a link to the appliance management web console.
- **Model**: Hardware model of the appliance
- **Serial Number**: Serial Number of the appliance.
- **BIOS Version**: BIOS version of the appliance.
- **Days Since Memory Dump**: Time since last system-error memory dump. If the appliance dumped its memory in the past 4 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 on the time opens the log page of the SD-WAN.
- **Active OS**: The OS currently running on the appliance.
- **Backup OS**: The OS on the appliance’s backup partition.
- **RAM Size (GB)**: Amount of Random Access Memory 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**

The Inventory Manager displays the sub-model information for the 210-SE platform. The sub-model distinguishes the model of the 210-SE platform configured in the network by displaying either LTE or BASE.
Network Health: Virtual Path Report

The Virtual Path Reports section of the dashboard displays virtual path level statistics for every virtual path in virtual WAN network that was measured as an average over the last 24 hours. The output can be filtered based on the selected routing domain.

For more information, see Reports

SD-WAN Center: Alarm Summary

The Alarm Summary section of the dashboard gives a graphical overview of the type and quantity of events. You can click on 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, Configuring Event Notifications.
The Database Usage section of the dashboard displays a graphical overview of the database-resource usage and the thresholds for sending notifications or halting the collection of data. You can click on 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 Setting 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,
How to Manage Database.
SD-WAN Center: Active OS Usage

The Active OS Usage section of the dashboard gives a graphical overview of the used and available storage space in GB. You can click on the graph to view the details in the Storage Maintenance page.

Diagnostic packages

September 24, 2018

A diagnostic package consists of all of the system log files, system information, and other necessary details that will assist the NetScaler SD-WAN Support team in diagnosing and resolving issues with
After creating the package you can download it to your computer and then mail the diagnostic package to NetScaler Customer Support or you can directly upload it to the NetScaler Customer Support server (or another server).

Note
NetScaler SD-WAN Center can store a maximum of five diagnostic packages at a time.

To create a diagnostic package:

1. In the NetScaler 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.
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 NetScaler Customer Support FTP server, or to another FTP host.

3. In the **Customer Name** field, enter a name to assist NetScaler SD-WAN Support in identifying the diagnostic packages.
   
   A directory with this name will be created on the NetScaler 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.
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**

September 28, 2018

NetScaler 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.

- **ObjectName**: The name of the object generating the event.
- **ObjectType**: 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.

**Viewing events**

You can view the events, filter it and also download it from the Event Viewer page.

**To access the event viewer page.**
In the NetScaler 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 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](#).

**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:
   - 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.

Filter:

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.
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 NetScaler 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

September 24, 2018

You can configure NetScaler 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:

- 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 NetScaler SD-WAN Center and the individual NetScaler SD-WAN appliances in your network.

However, enabling notifications on NetScaler SD-WAN Center allows you to receive event notifications for the entire NetScaler SD-WAN network (i.e., MCN and all the sites). While, enabling notifications on the NetScaler SD-WAN appliances allows you to receive notifications from the individual appliances only.
It is advised to enable notifications on the NetScaler SD-WAN Center only, to avoid redundant notifications from the other NetScaler SD-WAN appliances in your network.

Configuring email notification settings

To configure email notification settings:

1. In the NetScaler SD-WAN Center web management interface, navigate to Fault > Notification Settings > Email Alerts.

2. Select Enable Event Emails.

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.
Configuring SNMP trap notification settings

To configure SNMP trap notification settings:

1. In the NetScaler SD-WAN Center web management interface, navigate to Fault > Notification Settings > SNMP Traps.

2. Select Enable Event SNMP Traps.

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 NetScaler SD-WAN Center web management interface, navigate to **Fault > Notification Settings > Syslog**.

2. Select **Enable Event Syslog Messages**.

![Syslog Notification Settings](image)

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.

**Configuring event notifications**

**To configure event notifications:**

1. In the NetScaler SD-WAN Center web management interface, navigate to **Fault > Severity Settings**.

2. In the **Alert if Sate Persist**s 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 NetScaler SD-WAN Center and push it to individual appliances.

To configure alarm in NetScaler SD-WAN Center, navigate to Configuration > Appliance Settings > Notification Settings > Alarm Configuration and Click +.

Select or enter values for the following fields:

- **Event Type**: The NetScaler 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**

September 24, 2018

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 NetScaler support team. However, you can delete individual memory dumps.

To download memory dumps:

1. In the NetScaler 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.
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 NetScaler Customer Support FTP server, or to another FTP host.

3. In the **Customer Name** field, enter a name to assist NetScaler SD-WAN Support in identifying the diagnostic packages.

   A directory with this name will be created on the NetScaler 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.

7. Click **Upload**.

---

**Log files**

September 24, 2018
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 NetScaler SD-WAN Center.

To view log files:

1. In the NetScaler 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**.

### Polling interval

September 24, 2018

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 NetScaler SD-WAN Center web interface, navigate to **Configuration > Network Discovery > Discovery Settings**.

![NetScaler SD-WAN Center web interface screenshot](image)

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 NetScaler SD-WAN Center. The range is 100 Kbps – 1 Gbps. The default value is 1 Mbps.

4. Click **Apply**.

**Statistics**

September 28, 2018

You can view the statistics collected by NetScaler 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:

- 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 NetScaler 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.

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.

![Graphs and chart](image)

**Note**

You could print the graphs, or download the graph set as a CSV file.

**System information**

September 24, 2018

The following information is displayed on the system information page:

- **NetScaler SD-WAN Center Software Version**: The NetScaler 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 NetScaler SD-WAN Center virtual machine.
- **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 NetScaler SD-WAN Center virtual machine.

To display the system information:
In the NetScaler SD-WAN Center web interface, click the Monitoring tab and then click System Information.

**Reporting**

September 28, 2018

NetScaler 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 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 NetScaler 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
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.

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**
Application report

September 24, 2018

You can view details about incoming traffic, outgoing traffic, and total traffic of the top applications, sites, and application families as reports. This provides a holistic view of your network bandwidth usage.

Deep packet inspection (DPI) enables the SD-WAN appliance to parse the traffic passing through it and identify the application and application family types. The number of bytes of incoming and outgoing traffic of every application is recorded and is stored on the SD-WAN appliance. 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.

To view application reports in SD-WAN Center:

1. In SD-WAN Center, click **Reporting > Applications**.
2. In the time-line control, select the time interval.
3. From the **Report Type** drop-down list, select a report type.

You can view the following reports:
• **Top Applications**: The top applications used in the network for the selected time interval. Can be filtered by site name. By default, the top applications for all the sites is displayed.

• **Top Application Families**: Top application families used in the network. Can be filtered 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. Can be filtered by application or application family name.

For each report, you can view the following details:

• **Incoming Traffic**: Megabytes of application data coming into the site from the WAN.

• **Outgoing Traffic**: Megabytes of application data sent from the site to the WAN.

• **Total Traffic**: Sum of incoming and outgoing traffic.

You can view this data in units of Kbps, Mbps or Gbps.

**Bandwidth report**

September 28, 2018

NetScaler SD-WAN Center provides a central view of bandwidth statistics data polled from different sites in your SD-WAN network.

In the NetScaler 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 Classes and Rules by IP Address and Port Number.

Using NetScaler 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 NetScaler 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:

- **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 NetScaler 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 NetScaler 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 NetScaler 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**

September 28, 2018

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:

- **Realtime 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 realtime 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:

In NetScaler 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 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**: Class name
- **Type**: Class Type. Realtime, 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.
• **Packets Dropped**: Number of packets dropped, because of network congestion.
• **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.

**Ethernet interface report**

September 28, 2018

NetScaler SD-WAN Center provides a central view of all the Ethernet interfaces on the different NetScaler 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 NetScaler 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 NetScaler 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](#).
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**

September 28, 2018

You can view counts of different events occurring at each site in the SD-WAN network.

For more information about events, see **Events**.

**To view event statistics:**
In NetScaler 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 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 NetScaler.
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.

<table>
<thead>
<tr>
<th>Event</th>
<th>Object Type</th>
<th>Previous State</th>
<th>Current State</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTICE</td>
<td>LAN to WAN path</td>
<td>BAD</td>
<td>GOOD</td>
</tr>
<tr>
<td></td>
<td>GOOD</td>
<td>BAD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WAN to LAN path</td>
<td>BAD</td>
<td>GOOD</td>
</tr>
<tr>
<td></td>
<td>GOOD</td>
<td>BAD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Dynamic virtual path</td>
<td>BAD</td>
<td>GOOD</td>
</tr>
<tr>
<td></td>
<td>GOOD</td>
<td>BAD</td>
<td></td>
</tr>
<tr>
<td>WARNING</td>
<td>Virtual path</td>
<td>GOOD</td>
<td>BAD</td>
</tr>
<tr>
<td></td>
<td>WAN link congestion</td>
<td>UNCONGESTED</td>
<td>CONGESTED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CONGESTED</td>
<td>UNCONGESTED</td>
</tr>
<tr>
<td></td>
<td>Usage congestion</td>
<td>UNCONGESTED</td>
<td>CONGESTED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CONGESTED</td>
<td>UNCONGESTED</td>
</tr>
<tr>
<td></td>
<td>LAN to WAN path</td>
<td>GOOD</td>
<td>DEAD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BAD</td>
<td>DEAD</td>
</tr>
<tr>
<td></td>
<td>WAN to LAN path</td>
<td>GOOD</td>
<td>DEAD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BAD</td>
<td>DEAD</td>
</tr>
<tr>
<td>ALERT</td>
<td>Virtual path</td>
<td>BAD</td>
<td>DEAD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DEAD</td>
<td>BAD</td>
</tr>
<tr>
<td>ERROR</td>
<td>WAN-link</td>
<td>GOOD</td>
<td>DEAD</td>
</tr>
<tr>
<td></td>
<td>Ethernet</td>
<td>GOOD</td>
<td>UNDEFINED</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UNDEFINED</td>
<td>DEAD</td>
</tr>
<tr>
<td>INFO</td>
<td>Proxy-arp</td>
<td>UNDEFINED</td>
<td>ACTIVE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UNDEFINED</td>
<td>STANDBY</td>
</tr>
</tbody>
</table>

You can configure NetScaler 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.

**GRE tunnel report**

September 28, 2018

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 NetScaler SD-WAN appliances, see GRE Tunnel.

NetScaler SD-WAN Center can show you the state of all the GRE tunnels configured in your NetScaler SD-WAN network.

To view GRE tunnel statistics:

In NetScaler SD-WAN Center, navigating to Reporting > LAN GRE 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:
• **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.
• **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**

September 28, 2018

HDX report provides detailed HDX data per site. The data for each site is shown in two views.

**Summary view**

This view shows the following data for a site:

• **QoE Index** - The 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 TCP protocol.
• **UDP Flows** – The number of active HDX sessions on the site that use UDP protocols.
• **Sessions** – The total number of active HDX sessions on the site, this includes both SSI and MSI sessions.

**Detail View**

You can click on 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 effective numbers that NetScaler SD-WAN appliance is measuring. For example, there could be larger percent of packet drop in the network, since NetScaler 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, NetScaler SD-WAN improves the QoE for HDX traffic by improving the factors those affect the QoE. For more information see, Application QoE.

To view HDX Reports:
In NetScaler 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.

IPsec tunnel report

September 28, 2018

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.
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 NetScaler SD-WAN appliances, see [IPSec Tunnel Termination](#).

NetScaler SD-WAN Center can show you the state of all the IPsec tunnels configured in your NetScaler SD-WAN network.

**To view IPsec tunnel statistics:**

In NetScaler 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:

- **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.
NetScaler SD-WAN Center 10

- **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**

September 28, 2018

NetScaler 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.
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.
MOS for applications

September 28, 2018

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 NetScaler 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.

NetScaler 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 NetScaler SD-WAN appliance to display the MOS scores of these applications in NetScaler SD-WAN Center.

For more information about enabling MOS for applications in NetScaler SD-WAN, see Add Rule Groups and Enable MOS.

Note

Enable the Track Performance option, under Rules to estimate MOS for applications and display it in NetScaler SD-WAN Center. For more information on rules, see Rules by IP address and port number.

To view MOS for applications:

In NetScaler 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.

**MPLS queues report**

September 28, 2018

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 NetScaler SD-WAN appliances, see MPLS Queues.

To view MPLS queue statistics:

In NetScaler 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.
- **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 NetScaler 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 NetScaler 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 NetScaler 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**

September 28, 2018

You can manage and maintain your NetScaler SD-WAN Center VPX using the following administrative options.

- Configure date and time
- HTTPS certificates
- Import MCN configuration
- Manage database
- Manage views
- Software upgrade
- Timeline controls
- User accounts
Configure date and time

September 28, 2018

You can change the date and time of the NetScaler 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 NetScaler 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 NetScaler SD-WAN Center clock with an external NTP server.

To set the date and time by using an NTP Server:

1. In the NetScaler SD-WAN Center web interface, click the Administration tab.
2. Click Global Settings and then click TimeZone.
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 NetScaler 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.

Configure RADIUS Authentication

March 7, 2019

You can enable Remote Authentication Dial-In User Service (RADIUS) and configure connections to RADIUS authentication servers. RADIUS can then be used to authenticate remote users logging onto SD-WAN Center.

To use RADIUS, 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 will be checked sequentially, starting with the server listed first in the Servers section.

To enable and configure RADIUS authentication

1. In the SD-WAN Center web interface, click the Administration tab.

2. Click User/Authentication Settings. In the RADIUS Authentication section, select the Enable RADIUS Authentication checkbox.
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 10 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.

6. Click the plus icon (+) next to **Servers** to add a new 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 at which this RADIUS server will listen. The default port number is 1812.

9. Click **Apply**.

10. Click **Verify** to verify the connection to the RADIUS server. The Verify RADIUS Server Settings dialog box appears.
11. Enter a valid user name and password for the authentication servers, and click **Verify**.

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

**Configure TACACS+ Authentication**

March 7, 2019

You can enable and configuring connections to Terminal Access Controller Access Control System (TACACS+) authentication servers. TACACS+ can then be used to authenticate users logging onto the appliances.

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 will be checked sequentially, starting with the server listed first in the Servers section.

To enable and configure TACACS+ authentication for the managed appliances:

1. In the SD-WAN Center web interface, click the **Administration** tab.
2. Click **User/Authentication Settings**.
3. In the **TACACS+ Authentication** section, select the **Enable TACACS+ Authentication** checkbox.
   
   **Note**
   
   RADIUS authentication will be disabled if it is currently enabled.
4. 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 10 seconds.
5. In the **Authentication Type** field, enter the encryption method to use to send the user name and password to the TACACS+ server.
6. In the **Server Key** field, enter a secret key to use when connecting to the TACACS+ servers.

7. 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.

8. Click the plus icon (+) next to **Servers** to add a new 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 at which this TACACS+ server will listen. 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.

13. Enter a valid user name and password for the authentication servers, and click **Verify**.
To configure additional servers, repeat the steps 6 through 11.

**HTTPS certificates**

September 28, 2018

HTTPS certificate is required for establishing secured management HTTPS connection to NetScaler SD-WAN Center.

**View installed HTTPS certificate details**

To display the details of HTTPS certificate already installed on NetScaler SD-WAN Center:

1. In the NetScaler 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 NetScaler 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 mainte-
nance 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 NetScaler 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 an HTTPS certificate.
4. For the field **HTTPS private key file**, click **Browse** and select an HTTPS private key file.
5. Click **Upload and Install**.

![HTTPS Certificate upload and install](image)

**Regenerate the HTTPS certificate**

You can regenerate a self-signed certificate that secures the Management HTTPS connection to NetScaler SD-WAN Center. Regenerating the HTTPS Certificate puts NetScaler 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 NetScaler 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**.

---

**Import MCN configuration**

September 28, 2018

When NetScaler SD-WAN Center is set up and a connection is established between the master control node (MCN) and NetScaler SD-WAN Center, you can import the MCN configuration to NetScaler SD-WAN Center and view the network maps.

The Import function imports a configuration into an open or new NetScaler SD-WAN master configuration. If an NetScaler SD-WAN master configuration is open when you use the import function, it and its maps are overwritten by the new NetScaler SD-WAN master configuration. If no NetScaler SD-WAN master configuration is open, an untitled package is created.

To import the MCN configuration to NetScaler SD-WAN Center:

1. In the NetScaler SD-WAN Center web interface click the **Configuration** tab.
2. Click **Network Configuration** and then click **Import**.
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 NetScaler SD-WAN Center in the MCN before you can Import the Configuration.

   For more information, see, Install the NetScaler 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.
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.
Manage database

September 28, 2018

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 NetScaler 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.
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 NetScaler 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...** checkbox 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.

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 thresholds. The default is **AND**.

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 **3 months** 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 NetScaler 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.
   - **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**

September 28, 2018

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:

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

September 28, 2018
You can use the Software Upgrade option to upgrade your NetScaler SD-WAN Center software to the latest version. The software upgrade process places NetScaler 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 NetScaler SD-WAN Center functionality will be unavailable.

**Important**

Running the upgrade during maintenance hours is recommended.

**Note**

Download the appropriate NetScaler 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 NetScaler SD-WAN Center software

1. In the NetScaler SD-WAN Center web interface, click the **Administration** tab.

2. Click **Global Settings** and then click **Software Upgrade**.

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 NetScaler 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**

September 28, 2018
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 NetScaler 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.
  
  - *MM/DD/YYYY HH:MM [am / pm]*  
    
    For example: 09/07/2015 8:36am.
  
  - *M/D/YY HH: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).

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 7, 2019

You can display a list of all locally managed user accounts, and a list of any remote users (users authenticated through RADIUS or TACACS+ servers) who have logged in to the SD-WAN Center virtual machine at least once. You can also add a new local user account to the SD-WAN Center.

**Note**

If a user account is available on a remote authentication server, but has never been used to log onto this SD-WAN Center, that user account is not displayed.

To display user accounts:

1. In the SD-WAN Center web interface, click the **Administration** tab.
2. Click **User/Authentication Settings**. The list of user accounts appears in the **Users** section.
To add a new local user account to the SD-WAN Center:

**Note**
The user accounts created locally on SD-WAN center do not have the privilege to edit and export the network configuration package to the MCN.

3. Click the plus icon (+) next to **Users** at the top left corner of the table heading.

The **Add a new Local User Account** dialog box appears.

4. Enter the username, password, and password confirmation.

5. Click **Add**.

   This creates the new user account and adds the account information to the **Users** table.

**Note**
The SD-WAN Center can have up to eight local users.