



SD-WAN Orchestrator for On-premises 9.6

Contents

Release Notes for SD-WAN Orchestrator for On-premises 9.6 Release	3
Release Notes for SD-WAN Orchestrator for On-premises 1.0 Release	5
System requirements and installation	7
Difference between SD-WAN Orchestrator for On-premises and Citrix SD-WAN Orchestrator service	9
Install and configure SD-WAN Orchestrator for On-premises on ESXi Server	10
Install and configure SD-WAN Orchestrator for On-premises on XenServer	17
SD-WAN Orchestrator for On-premises log-in	25
SD-WAN Orchestrator for On-premises licensing	32
Connectivity with Citrix SD-WAN appliances	36
Network configuration	40
Delivery services	49
Routing	61
Inter-link communication	80
QoS policies	82
HDX QoE	89
Security	104
Site and IP Groups	127
Application and DNS settings	132
Profiles and Templates	149
Site configuration	154
LTE firmware upgrade	181
Address resolution protocol	184

Virtual paths	185
Dynamic routing	190
Network address translation	199
Dynamic host configuration protocol	201
Multicast routing	204
Virtual router redundancy protocol	208
Domain Name System settings	210
Link aggregation groups	214
Appliance settings	216
In-band management	233
Customer/Network dashboard	241
Site dashboard	245
Network Troubleshooting	247
Site troubleshooting	248
Customer/Network reports	250
Site reports	272
Diagnostics	296
User administration	298
Domain name	304
HTTPS certificate	306
Disk space management	308
Replace an affected Citrix SD-WAN appliance	312
API guide for SD-WAN Orchestrator for On-premises	315
Orchestrator administration	318

Orchestrator diagnostics

327

Release Notes for SD-WAN Orchestrator for On-premises 9.6 Release

March 25, 2021

This release notes document describes the enhancements and changes, fixed and known issues that exist for the SD-WAN Orchestrator for On-premises release 9.6.

Note

This release notes document does not include security related fixes. For a list of security related fixes and advisories, see the Citrix security bulletin.

What's New

The enhancements and changes that are available in release 9.6.

Configuration and Management

Dynamic Routing

From Citrix SD-WAN 11.3.1 release onwards, you can configure one router ID for the entire protocol and also one router ID per routing domain. With this enhancement, you can enable stable dynamic routing across multiple instances with different router IDs converging in a stable manner.

[SDW-17097]

Miscellaneous

HTTPS Certificate

HTTPS Certificate is required for establishing secure management HTTPS connection to SD-WAN Orchestrator for On-premises. You can use the default certificate available on SD-WAN Orchestrator for On-premises GUI or upload a custom HTTPS certificate generated from any other framework such as OpenSSL. Custom HTTPS certificate allows you to have control over the security and the other subject parameters related to the certificate.

[SDW-16359]

Interfaces

From Citrix SD-WAN 11.3.1 release onwards, you can enable or disable a virtual interface using the **Enabled** check box.

[SDW-15993]

Fixed Issues

The issues that are addressed in release 9.6.

Configuration and Management

For Citrix SD-WAN 6100 SE appliance, the UI does not display **LAG** page under **Configuration > Advanced Settings**.

[SDWANHELP-1895]

Miscellaneous

SD-WAN Orchestrator for On-premises GUI prompts the users to log in every one hour even when the GUI is in continuous use and not left idle.

[SDWANHELP-1902]

When you create a site by cloning an existing site **Deploy Config/Software > Verify Config** fails.

[SDW-16103]

Known Issues

The issues that exist in release 9.6.

Miscellaneous

If you open SD-WAN Orchestrator for On-premises GUI in a new tab while authentication token refresh is in progress, all existing sessions in the browser get logged out.

[SDW-17719]

If the disk is resized to more than 1.8 TB, resizing of the disk does not happen.

[SDW-16404]

The CLI allows users to create a password out of the allowed 8–128 length range but the GUI login fails if the password length is out of the allowed range.

Workaround: On logging into the GUI, the user is forced to change the length of the password to the allowed range.

[SDW-16068]

When a user tries to log in, a red banner might display at the top of the page for a fraction of a second before displaying the login page.

[SDW-16024]

When the database backup of an appliance is restored on another appliance having the same release of SD-WAN Orchestrator for On-premises, the user details are not restored. On the restored appliance, if you create a user with the same user name as in the backed-up database, the following error is displayed:

User has a role already assigned

Workaround: Create a user with a different user name that did not exist on the backed-up database.

[SDW-15984]

Release Notes for SD-WAN Orchestrator for On-premises 1.0 Release

March 25, 2021

SD-WAN Orchestrator for On-premises is a self-hosted, management service available as separate instance for each customer. It provides a single-pane of glass management platform that enables you to configure, monitor, and analyze all the SD-WAN appliances on your SD-WAN network.

SD-WAN Orchestrator for On-premises is recommended for customers with strong regulatory requirements around data sovereignty and data privacy.

The following are some of the key capabilities:

- **Authentication:** Supports local and RADIUS / TACACS+ authentication.
- **Centralized configuration:** Centralized configuration of SD-WAN networks, with guided workflows, visual aids, and profiles.
- **Zero touch provisioning:** Seamless bring up of the network and connections.
- **Application-centric policies:** Application based traffic steering, Quality of Service (QoS), and Firewall policies, configurable globally or per site.
- **Hierarchical summarization of health:** Ability to centrally monitor the health, usage, quality, and performance of a network as a whole, with the ability to drill down into individual sites and associated connections.
- **Troubleshooting:** Device & Audit Logs, Diagnostic utilities such as Ping, Traceroute, Packet Capture to troubleshoot network connectivity issues.

Prerequisites

- **Appliances:** A minimum of two appliances. Each SD-WAN appliance or virtual instance must have an IP address configured.

- **Citrix SD-WAN Orchestrator service account:** To use Citrix SD-WAN Orchestrator on-premises, you must have an account in the Citrix SD-WAN Orchestrator service. For more information, see [Onboarding Citrix SD-WAN Orchestrator service](#).

SD-WAN Orchestrator for On-premises 1.0.1

Fixed Issues

- **SDW-16456:** Any to any routing domain is not supported in SD-WAN Orchestrator for On-premises.
- **SDW-16063:** At the network level, the Wi-Fi summary reports are unavailable.
- **SDW-16054:** If a customer account is created outside of the US region on Citrix SD-WAN Orchestrator service, then the API token obtained by the Identity and Management (IDAM) page from Citrix Cloud does not work. The customer's login to SD-WAN Orchestrator for On-premises fails with the following error message: "Invalid Customer ID, Client ID, or Client Secret".

You can now select the **POP** in which your cloud account was on-boarded, on booting up the SD-WAN Orchestrator for On-premises for the first time.

Known issues

- **SDW-16068:** The CLI allows users to create a password out of the allowed 8–128 length range but the GUI login fails if the password length is out of the allowed range.
 - **Workaround:** On logging into the GUI, the user is forced to change the length of the password to the allowed range.
- **SDW-16024:** When a user logs in to the UI, a red banner might display at the top of the page for a fraction of a second before displaying the login page.
- **SDW-15984:** When the database backup of an appliance is restored on another appliance having the same release of SD-WAN Orchestrator for On-premises, the user details are not restored. On the restored appliance, if you create a user with the same user name as in the backed-up database, the following error is displayed:

User has a role already assigned

 - **Workaround:** Create a user with a different user name that did not exist on the backed-up database.
- **SDW-16103:** When you create a site by cloning an existing site, **Deploy Config/Software > Verify Config** fails.
 - **Workaround:** Do not create a site by cloning an existing site.
- **SDW-16404:** If the disk is resized to more than 1.8 TB, resizing of the disk does not happen.

System requirements and installation

February 25, 2021

Before you install SD-WAN Orchestrator for On-premises on a Virtual Machine (VM), ensure that you must understand the hardware and software requirements and have met the prerequisites.

Note

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

Hardware requirements

SD-WAN Orchestrator for On-premises has the following hardware requirements.

Processor

- 8 Core, 3 GHz (or equivalent) processor or better for a server managing up to 128 sites.

Memory

- A minimum of 16 GB of RAM is recommended that manages up to 128 Sites.

Disk space requirements

For 128 sites with 2 WAN links per site, 300 GB of storage is required for SD-WAN Orchestrator for On-premises to store data of 1 month.

Software

SD-WAN Orchestrator for On-premises VPX can be configured on the following platforms:

Hypervisor

- VMware ESXi server, version 6.5.
- Citrix XenServer 6.5 or higher.

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

SD-WAN Orchestrator for On-premises 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 SD-WAN Orchestrator for On-premises:

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

Note

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

Download SD-WAN Orchestrator for On-premises software

Download the SD-WAN Orchestrator for On-premises Management Console software installation files, for the required release and platform, from the [Downloads](#) page.

SD-WAN Orchestrator for On-premises installation files use the following naming convention:

- ctx-sdw-onprem-build.extension
- ctx-onprem-build.extension
- ctx-onprem-build.extension

Platform	File extension
Citrix XenServer	.xva
VMware ESXi	-vmware.ova

Installation and configuration checklist

This section provides a checklist of the information you need to complete your SD-WAN Orchestrator for On-premises installation and deployment.

Gather or determine the following information:

- The IP address of the ESXi server and XenServer that hosts the SD-WAN Orchestrator for On-premises Virtual Machine (VM).
- A unique name to assign to the SD-WAN Orchestrator for On-premises VM.
- The amount of memory to allocate for the SD-WAN Orchestrator for On-premises VM.
- The amount of disk capacity to allocate for the virtual disk for the VM.
- The Gateway IP Address the SD-WAN Orchestrator for On-premises use to communicate with external networks.

- The subnet mask for the network in which the SD-WAN Orchestrator for On-premises VM is installed.

Difference between SD-WAN Orchestrator for On-premises and Citrix SD-WAN Orchestrator service

March 12, 2021

Features

Features	Citrix SD-WAN Orchestrator service	SD-WAN Orchestrator for On-premises
Advanced Edition Platform	Yes	No
Premium Edition Platform	Yes	No
Zscaler Service	Yes	No
Cloud Direct Service	Yes	No
Azure Virtual WAN Service	Yes	No
Citrix Secure Internet Access Service	Yes	No
Hosted Firewall	Yes	No
Application Routing	Yes	No
Orchestrator - High Availability	Yes	No

Requirements

Requirements	Citrix SD-WAN Orchestrator service	SD-WAN Orchestrator for On-premises
SD-WAN Factory Image required	All (Factory Shipping release)	Citrix SD-WAN 11.2.2, 11.3.0 and above.*
Appliance Deployed in the Network	All	Citrix SD-WAN 11.2.2, 11.3.0 and above.*
SD-WAN appliance internet connectivity	Required	Not Required

Requirements	Citrix SD-WAN Orchestrator service	SD-WAN Orchestrator for On-premises
Firewall ports to be open	443	443, 22, ICMP
Licensing	Postpaid and Prepaid models	Prepaid model only

- The supported Citrix SD-WAN software version depends on the SD-WAN Orchestrator for On-premises software version.

Install and configure SD-WAN Orchestrator for On-premises on ESXi Server

January 20, 2021

Install the VMware vSphere client

Following are the basic instructions for downloading and installing the VMware vSphere client that you use to create and deploy the SD-WAN Orchestrator for On-premises Virtual Machine (VM).

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

1. Open a browser and navigate to the ESXi server that hosts your vSphere Client and SD-WAN Orchestrator for On-premises virtual machine 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 downloaded, and accept each of the default options when prompted.

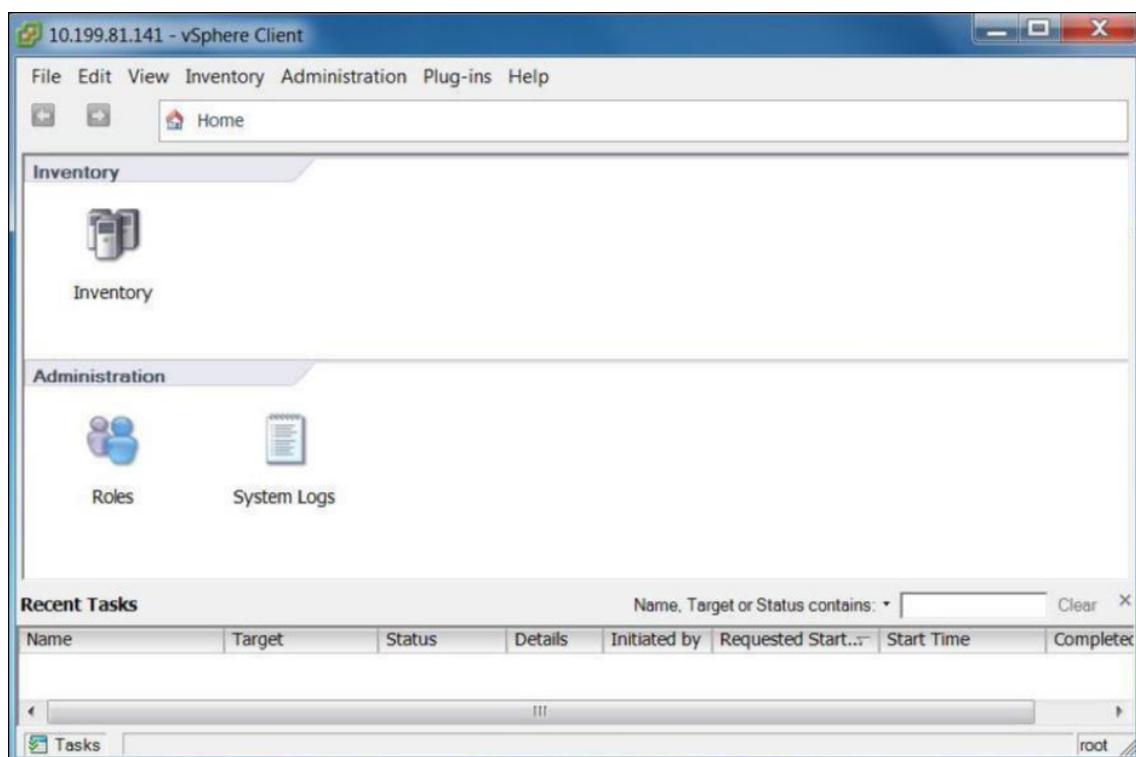
4. After the installation completes, start the vSphere Client program.

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

5. Enter the ESXi server login credentials:
 - **IP address/Name:** Enter the IP Address or Fully Qualified Domain Name (FQDN) for the ESXi server that hosts your SD-WAN Orchestrator for On-premises virtual machine 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.



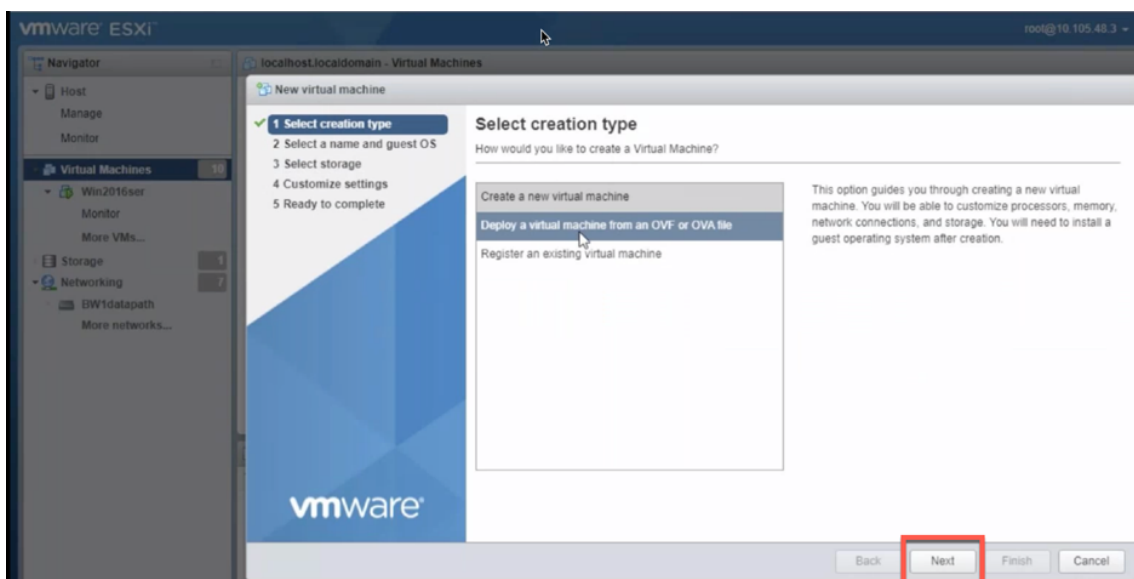
Creating the SD-WAN Orchestrator for On-premises virtual machine using the OVF template

After installing the VMware vSphere client, create the SD-WAN Orchestrator for On-premises virtual machine.

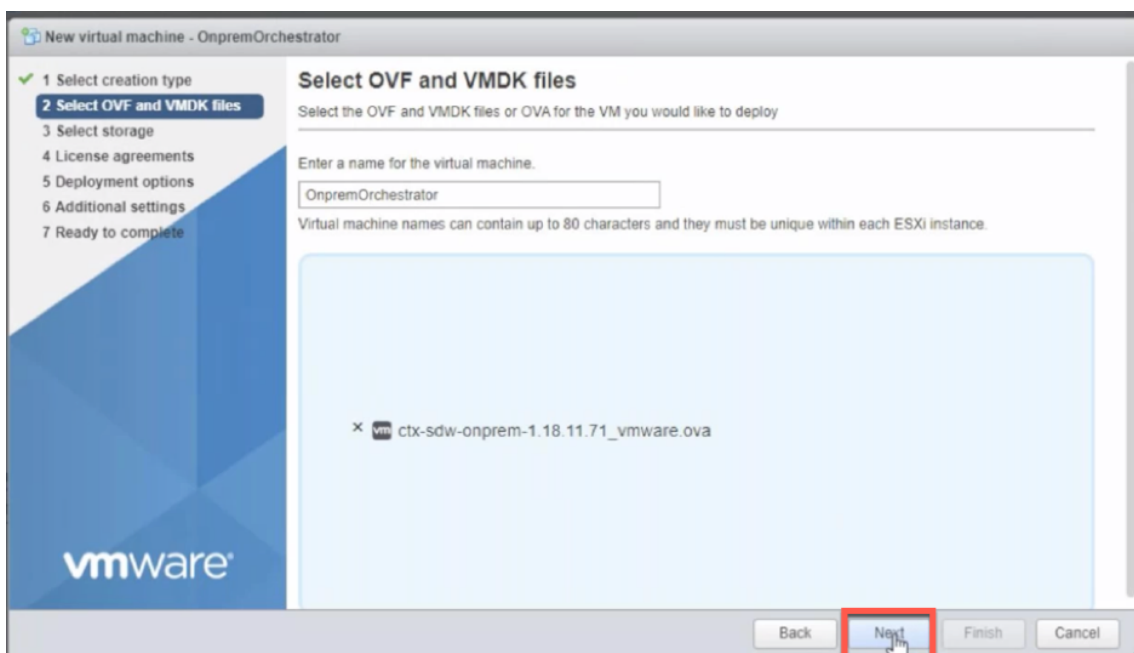
1. If you have not already done so, download the SD-WAN Orchestrator for On-premises OVF template file (.ova file) to the local PC.

For more information, see [System requirements and installation](#).

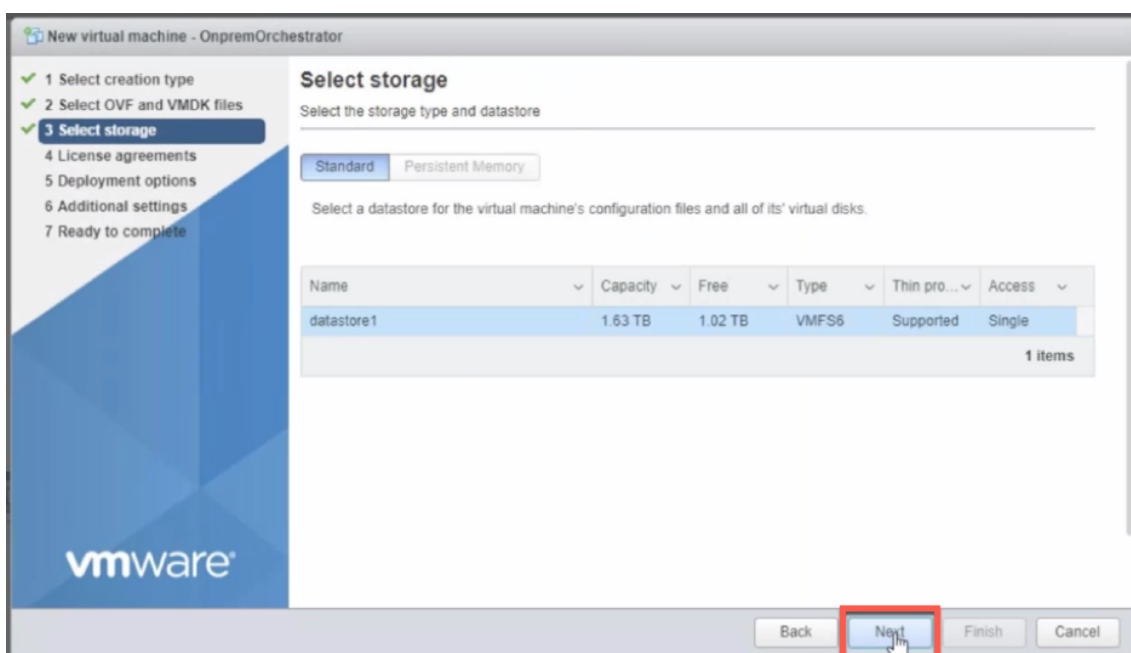
2. In the vSphere Client, click **Create/Register VM**, and then select **Deploy a virtual machine from an OVF or OVA file** from the list. Click **Next**.



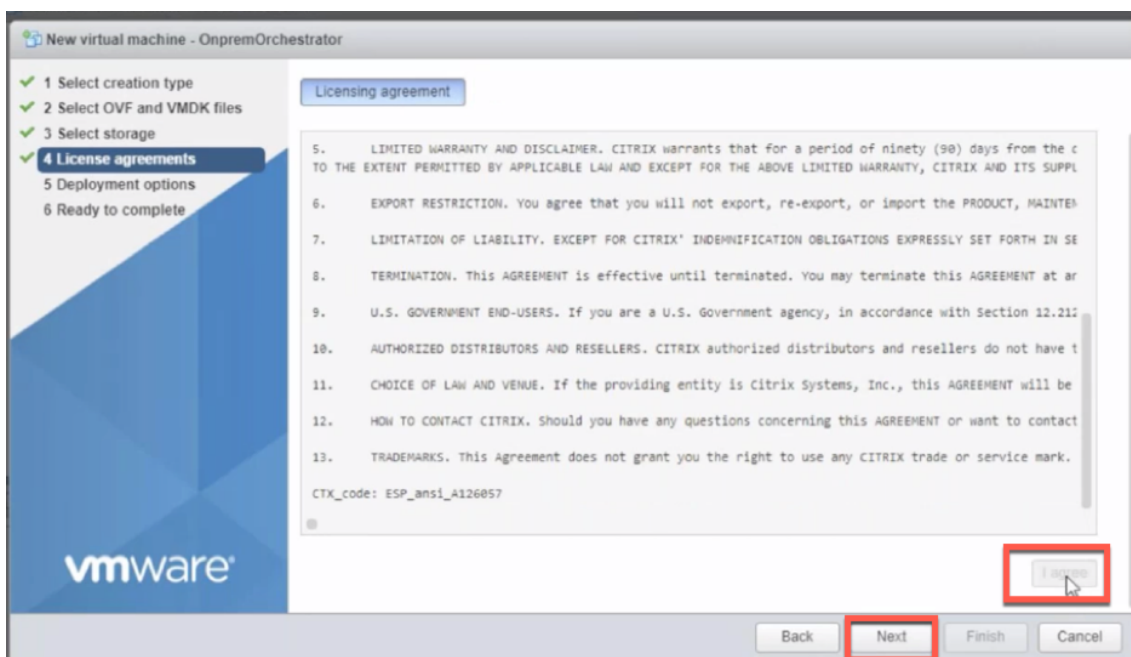
3. Enter a unique name for the new virtual machine.
4. Click inside the box and select the SD-WAN Orchestrator for On-premises OVF template (.ova file) that you want to install or you can drag and drop the file inside the box.
5. Click **Next**.



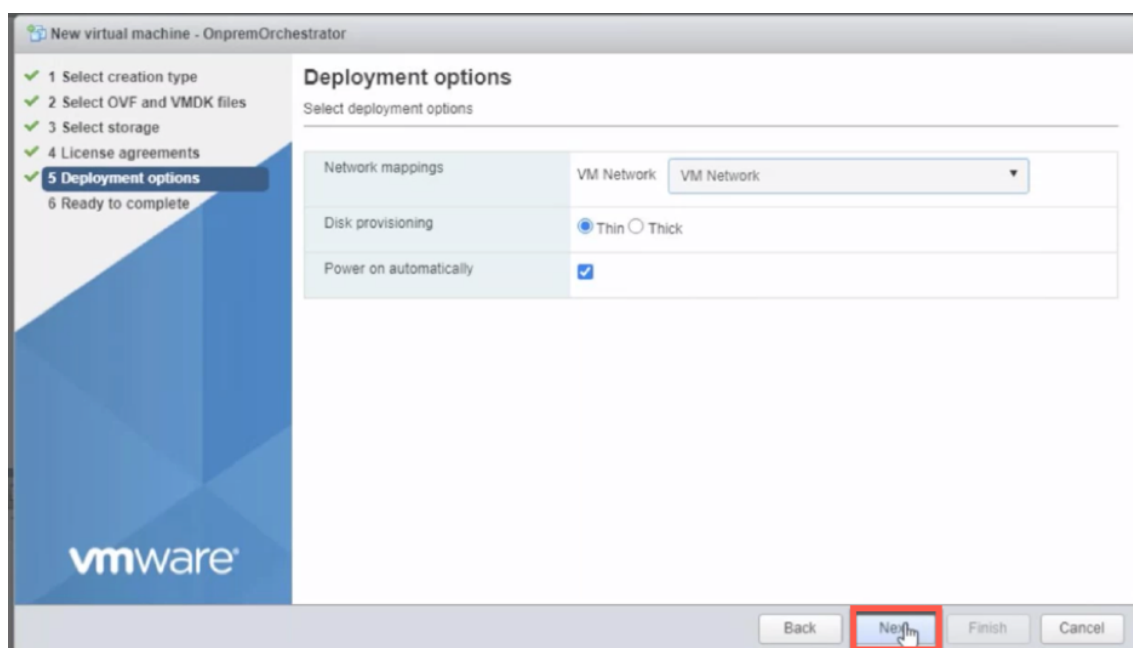
6. Click **Next**.
The Storage page appears.
7. Accept the default storage resource by clicking **Next**.



8. On the End User License Agreement page, click **I Agree**, and click **Next**.



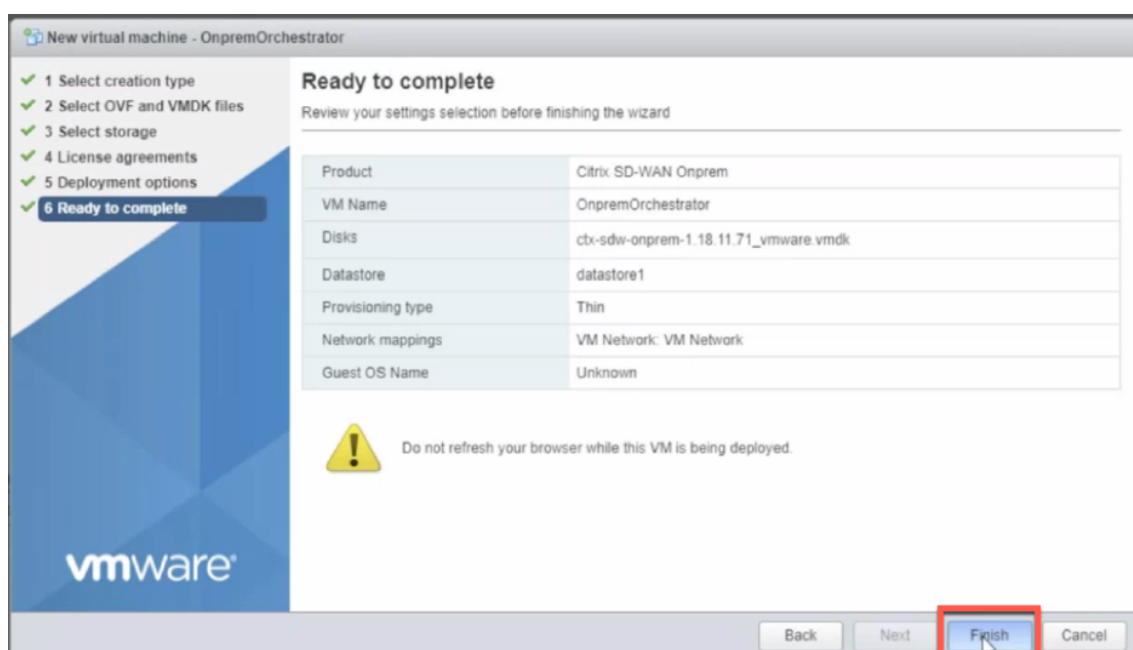
9. On the Deployment option page, select the VM Network from the drop-down list and accept the default settings for other fields. Click **Next**.



10. On the Ready to Complete page, click **Finish** to create the virtual machine.

Note

Decompressing the disk image onto the server can take several minutes.

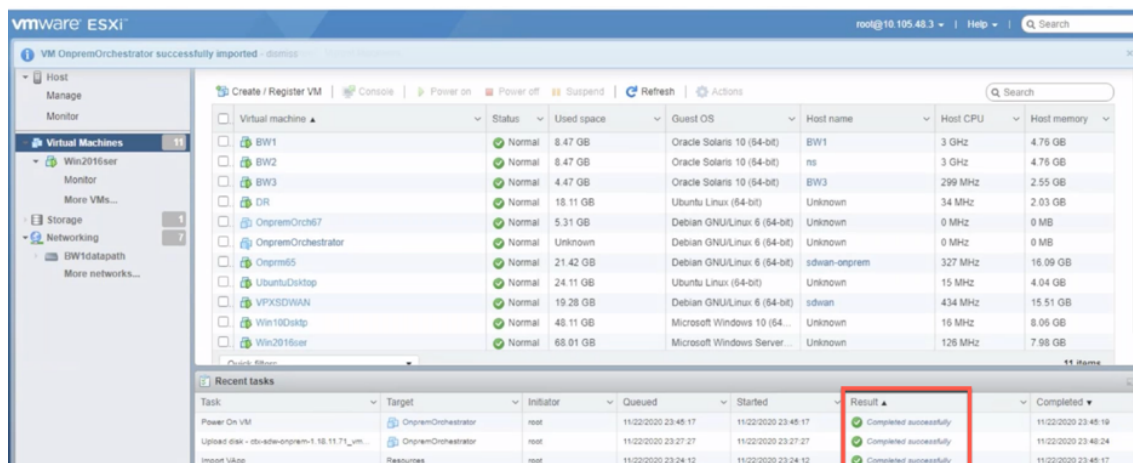


View and record the management IP address on the ESXi server

The management IP address is the IP address of the SD-WAN on-premises Orchestrator virtual machine, use this IP address to log into the SD-WAN Orchestrator for On-premises Web UI.

To display the management IP address, do the following:

1. On the vSphere client Inventory page, select the new SD-WAN Orchestrator for On-premises virtual machine.
2. On the SD-WAN Orchestrator for On-premises page, under Recent Tasks, wait for the result to show completed.

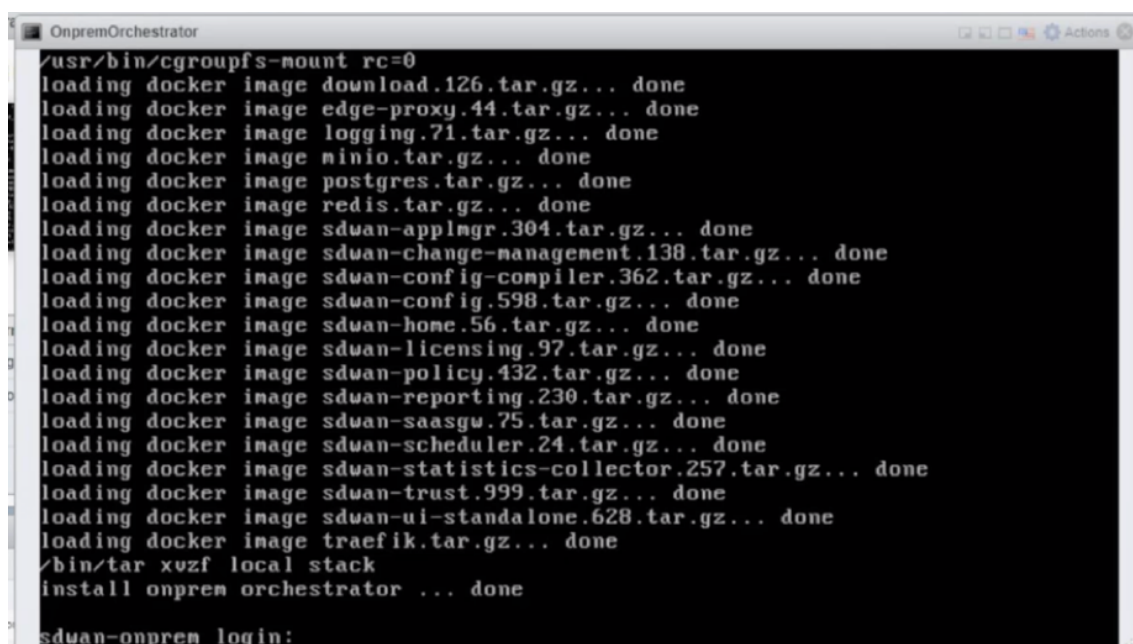


3. Select the **Console** tab, and then click anywhere inside the console area to enter console mode.

Note

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

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



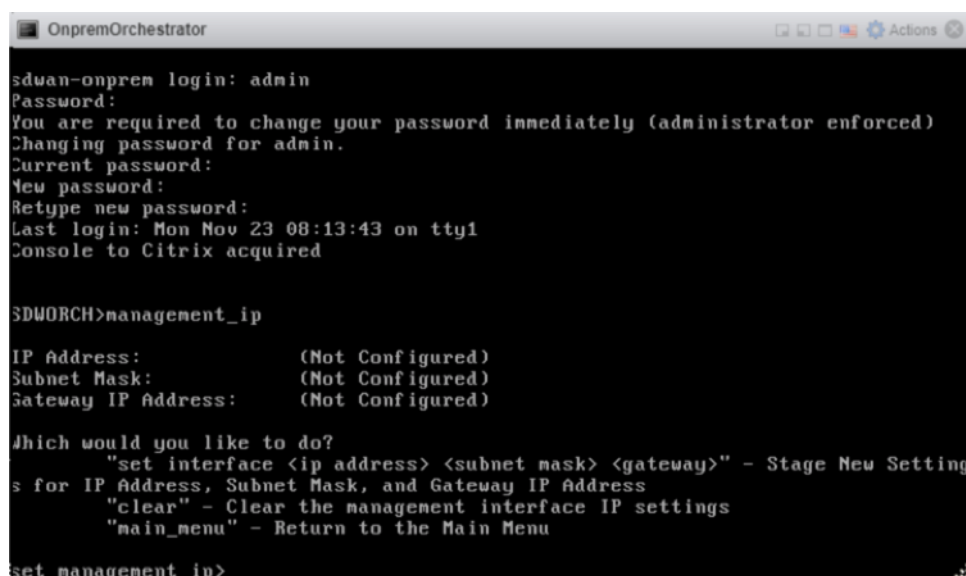
5. Log into the virtual machine console.

The default login credentials for the new SD-WAN Orchestrator for On-premises virtual machine are as follows:

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

Note

It is mandatory to change the default admin user account password on a first time login. This change is enforced using both CLI and UI.



```
OnpremOrchestrator
sdwan-onprem login: admin
Password:
You are required to change your password immediately (administrator enforced)
Changing password for admin.
Current password:
New password:
Retype new password:
Last login: Mon Nov 23 08:13:43 on tty1
Console to Citrix acquired

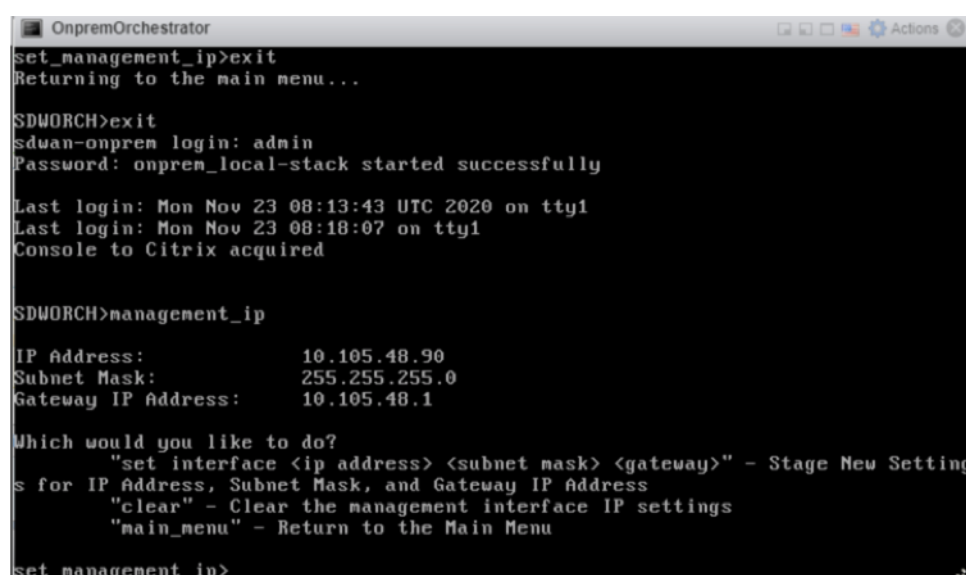
SDWORCH>management_ip

IP Address:          (Not Configured)
Subnet Mask:         (Not Configured)
Gateway IP Address:  (Not Configured)

Which would you like to do?
    "set interface <ip address> <subnet mask> <gateway>" - Stage New Settings for IP Address, Subnet Mask, and Gateway IP Address
    "clear" - Clear the management interface IP settings
    "main_menu" - Return to the Main Menu

set management ip>
```

6. Record the SD-WAN Orchestrator for On-premises virtual machine's management IP address, which is shown as the Host IP address in a welcome message that appears when you log on.



```
OnpremOrchestrator
set_management_ip>exit
Returning to the main menu...

SDWORCH>exit
sdwan-onprem login: admin
Password: onprem_local-stack started successfully

Last login: Mon Nov 23 08:13:43 UTC 2020 on tty1
Last login: Mon Nov 23 08:18:07 on tty1
Console to Citrix acquired

SDWORCH>management_ip

IP Address:          10.105.48.90
Subnet Mask:         255.255.255.0
Gateway IP Address:  10.105.48.1

Which would you like to do?
    "set interface <ip address> <subnet mask> <gateway>" - Stage New Settings for IP Address, Subnet Mask, and Gateway IP Address
    "clear" - Clear the management interface IP settings
    "main_menu" - Return to the Main Menu

set management ip>
```


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 address.

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

1. When the virtual machine is started, click the **Console** tab.
2. Log into the virtual machine. The default login credentials for the new SD-WAN Orchestrator for On-premises virtual machine 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.
5. Are you sure you want to change your Management Interface IP settings?

You may lose connectivity to the appliance. <y/n>?

Press “y” to change the IP and access the new management IP configured after nearly 6–7 minutes.

Install and configure SD-WAN Orchestrator for On-premises on XenServer

January 20, 2021

Before installing the SD-WAN Orchestrator for On-premises virtual machine on a XenServer server, gather the necessary information as described in [Installation and configuration checklist](#).

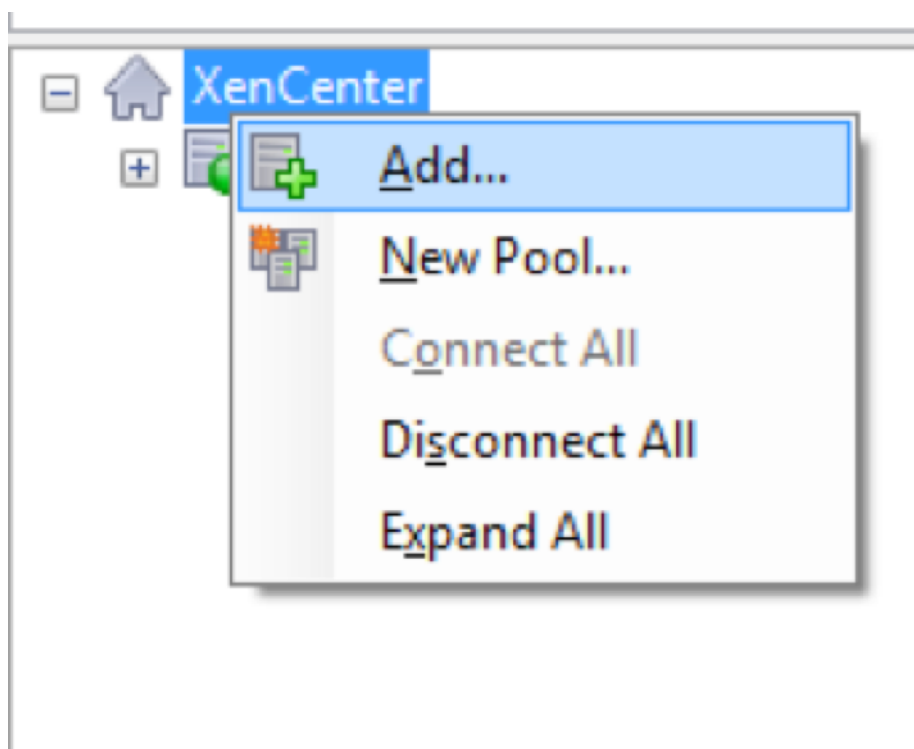
Install the XenServer server

To install the Citrix XenServer server on which you deploy the SD-WAN Orchestrator for On-premises 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:

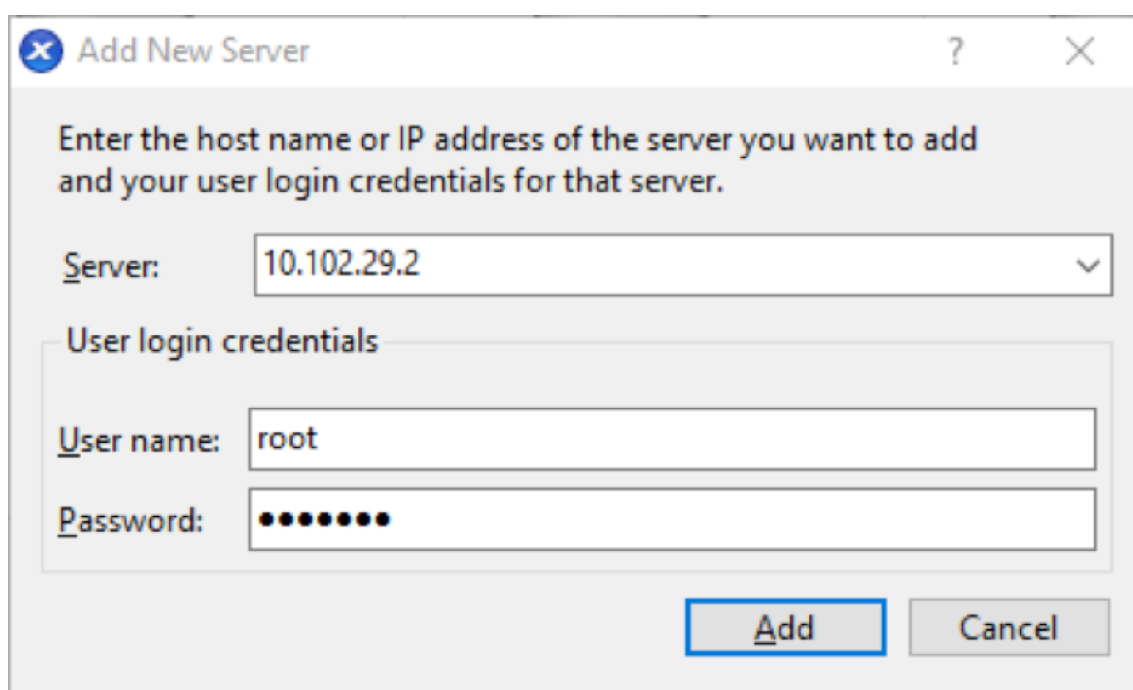
1. Open the XenCenter application on your computer.

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 hosts your SD-WAN Orchestrator for On-premises virtual machine instance.
- **User name:** Enter the server administrator account name. The default is root.
- **Password:** Enter the password associated with this administrator account.



Add New Server

Enter the host name or IP address of the server you want to add and your user login credentials for that server.

Server: 10.102.29.2

User login credentials

User name: root

Password: ●●●●●●●●

Add **Cancel**

4. Click **Add**.

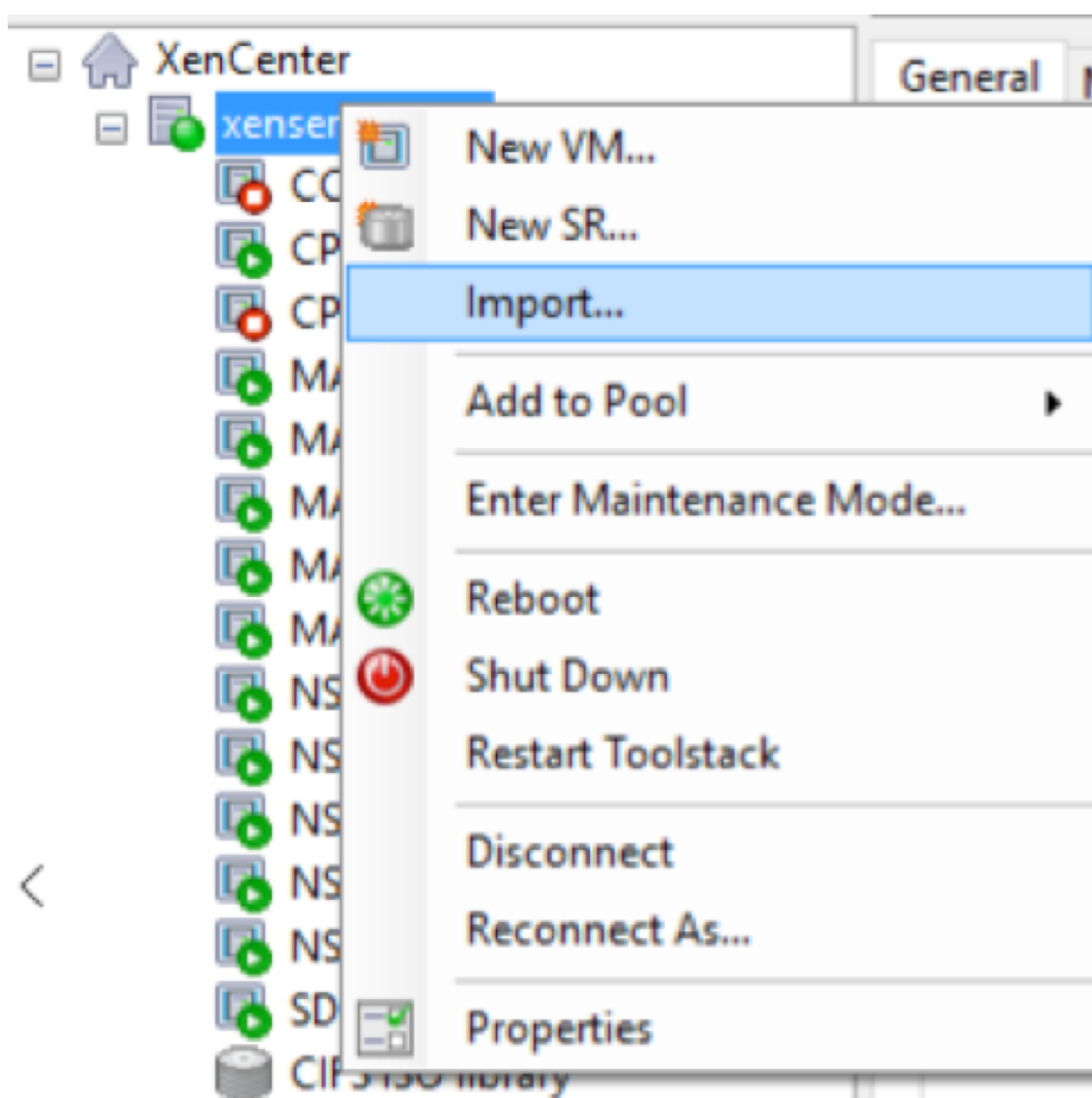
The new server's IP address appears in the left pane.

Create the SD-WAN Orchestrator for On-premises virtual machine using the XVA file

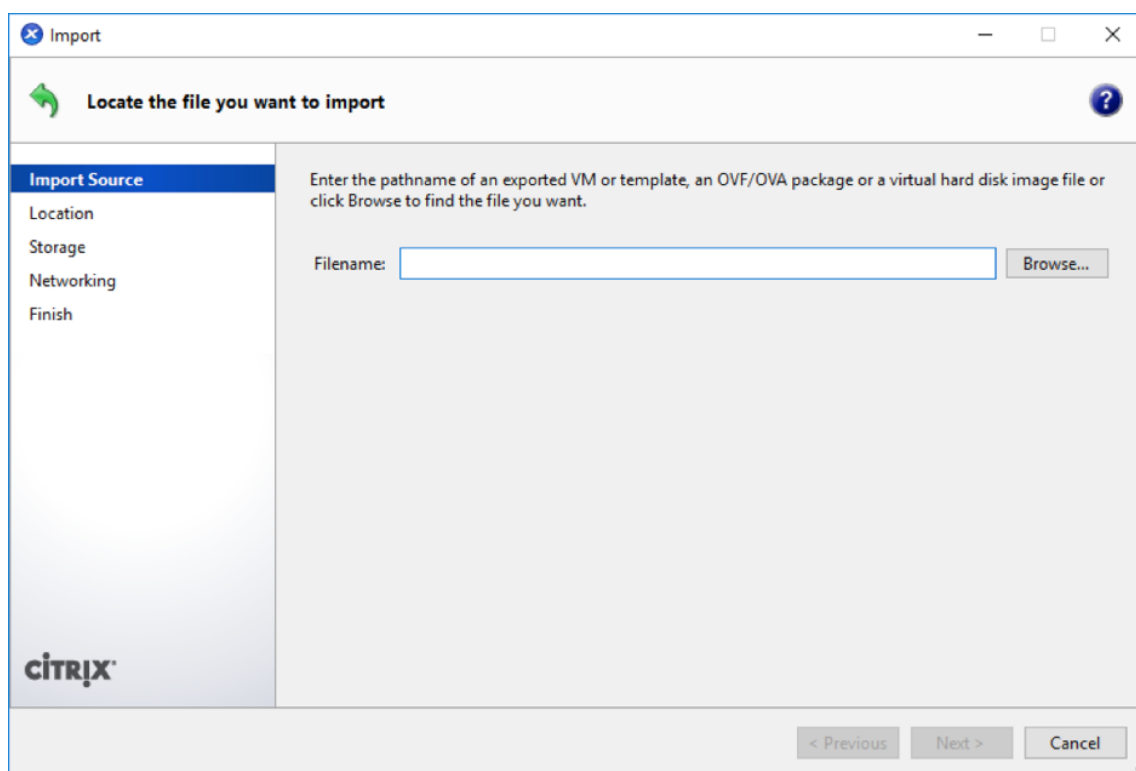
The SD-WAN Orchestrator for On-premises virtual machine software is distributed as an XVA file. If you have not already done so, download the .xva file. For more information, see [System requirements and installation](#).

To create the SD-WAN Orchestrator for On-premises virtual machine:

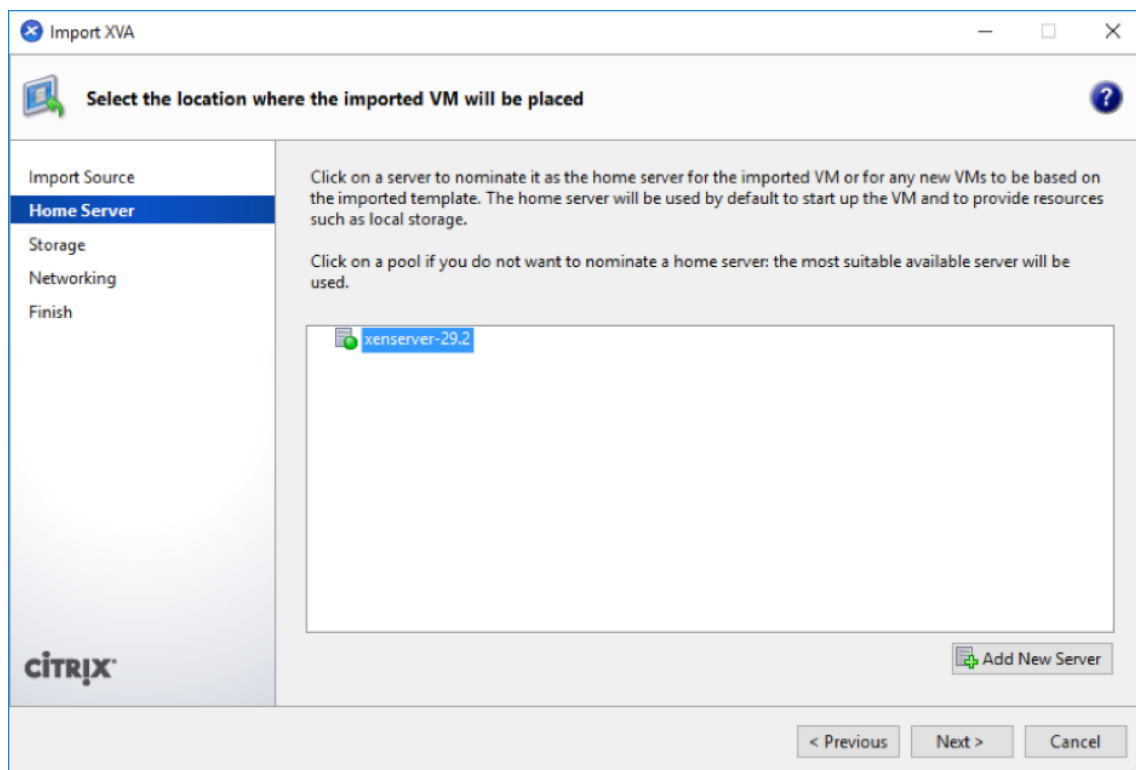
1. In XenCenter, right-click **XenServer** and click **Import**.



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



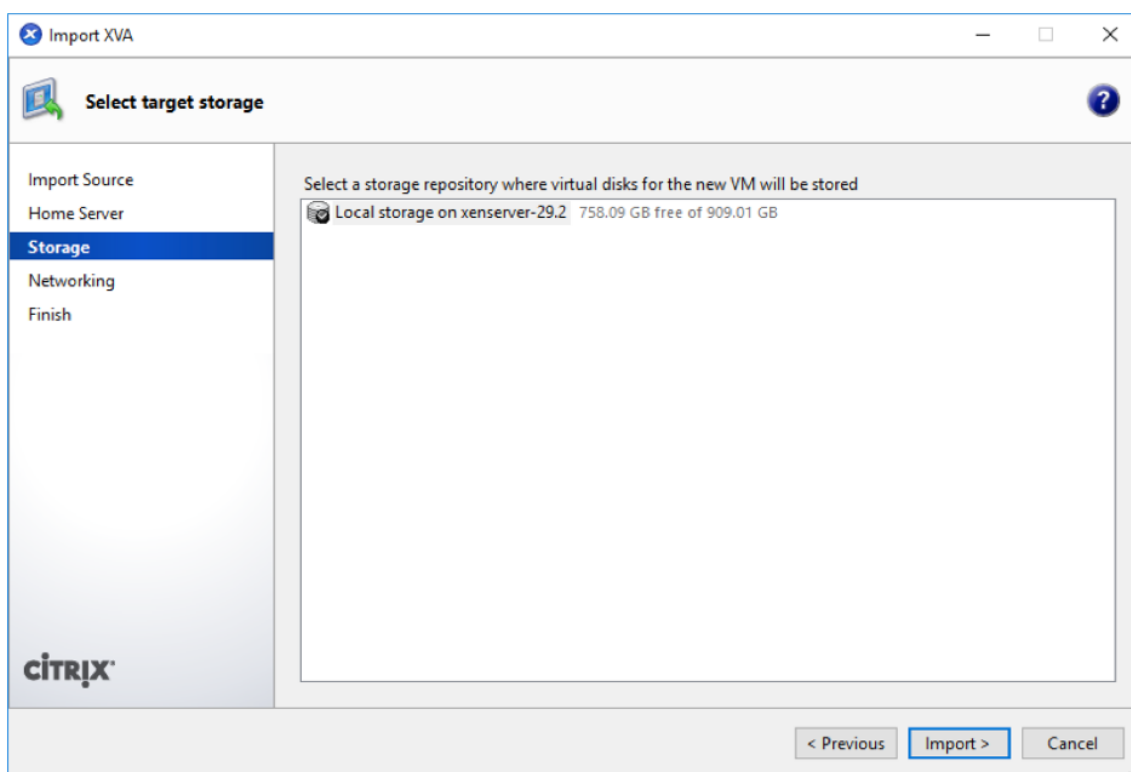
3. Select a previously created XenServer server as the location to which to import the virtual machine, and click **Next**.



4. Select a storage repository where the virtual disk for the new virtual machine is stored, and click

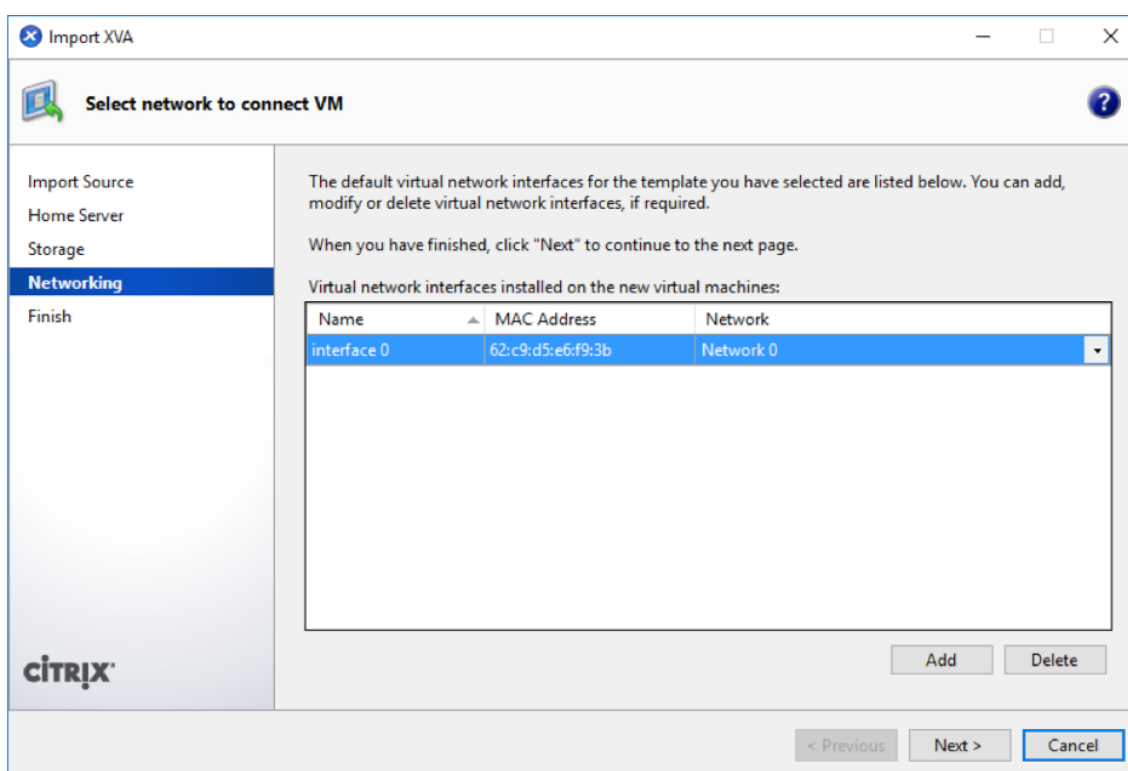
Import.

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



The imported SD-WAN Orchestrator for On-premises virtual machine appears in the left pane.

5. Select a network to which to connect the virtual machine, 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 SD-WAN Orchestrator for On-premises virtual machine, use this IP address to log into the SD-WAN Orchestrator for On-premises 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 SD-WAN Orchestrator for On-premises virtual machine and select **Start**.
2. When the virtual machine is started, click the **Console** tab.

```
sdwan-onprem login: admin
Password:
You are required to change your password immediately (administrator enforced)
Changing password for admin.
Current password:
New password:
Retype new password:
Last login: Wed Nov 25 09:13:56 on tty1
Console to Citrix acquired

SDWORCH>management_ip

IP Address:          10.105.59.125
Subnet Mask:         255.255.255.0
Gateway IP Address:  10.105.59.1

Which would you like to do?
  "set interface <ip address> <subnet mask> <gateway>" - Stage New Setting
s for IP Address, Subnet Mask, and Gateway IP Address
  "clear" - Clear the management interface IP settings
  "main_menu" - Return to the Main Menu

set_management_ip>_
```

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 virtual machine. The default login credentials for the new SD-WAN Orchestrator for On-premises virtual machine are as follows:

Login: admin

Password: password

Note

It is mandatory to change the default admin user account password on a first time logon. This change is enforced using both CLI and UI.

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

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

1. When the virtual machine is started, click the Console tab.
2. Log into the virtual machine. The default login credentials for the new SD-WAN Orchestrator for On-premises virtual machine 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.
5. Are you sure you want to change your Management Interface IP settings?
You may lose connectivity to the appliance. <y/n>?
Press “y” to change the IP and access the management IP configured after nearly 6–7 minutes.

SD-WAN Orchestrator for On-premises log-in

February 11, 2021

This article describes how a customer can first time log in to the SD-WAN Orchestrator for On-premises. Following are the prerequisites that you need to have before login to the SD-WAN Orchestrator for On-premises:

- You must have a Citrix Cloud Account. For more information, see [Customer accesses SD-WAN Orchestrator](#).
- To use SD-WAN Orchestrator for On-premises, you must have an account in the Citrix SD-WAN Orchestrator service. For more information, see [Onboarding Citrix SD-WAN Orchestrator service](#).
- Create an administrator with custom privileges.
- Create a client from the API Access page to get the customer ID, ID, and Secret detail. These details are needed during the on-premises Orchestrator log on.

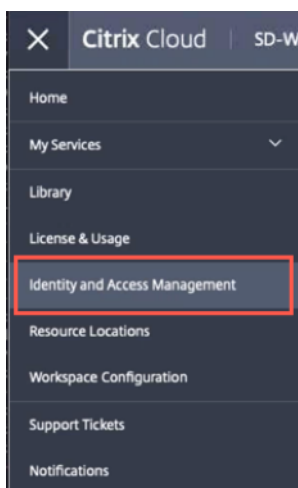
Note

Without the Cloud login, you cannot proceed to the local login.

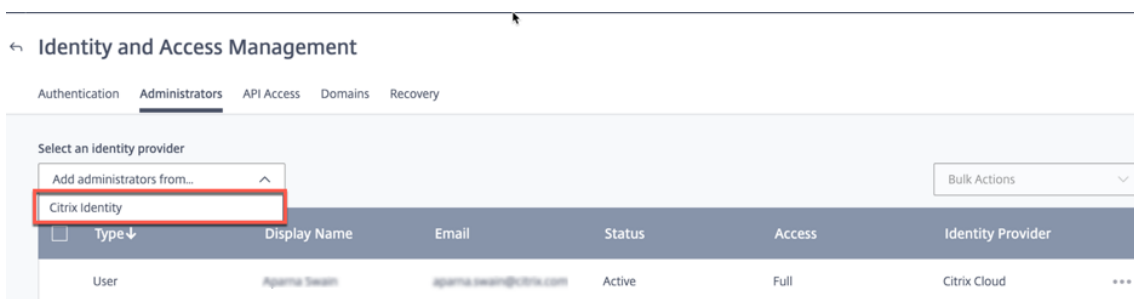
Create Administrator

An enterprise customer can invite an administrator to manage their SD-WAN network. Perform the following steps to invite an administrator:

1. Log in to the Citrix Cloud and navigate to **Identity and Access Management**.



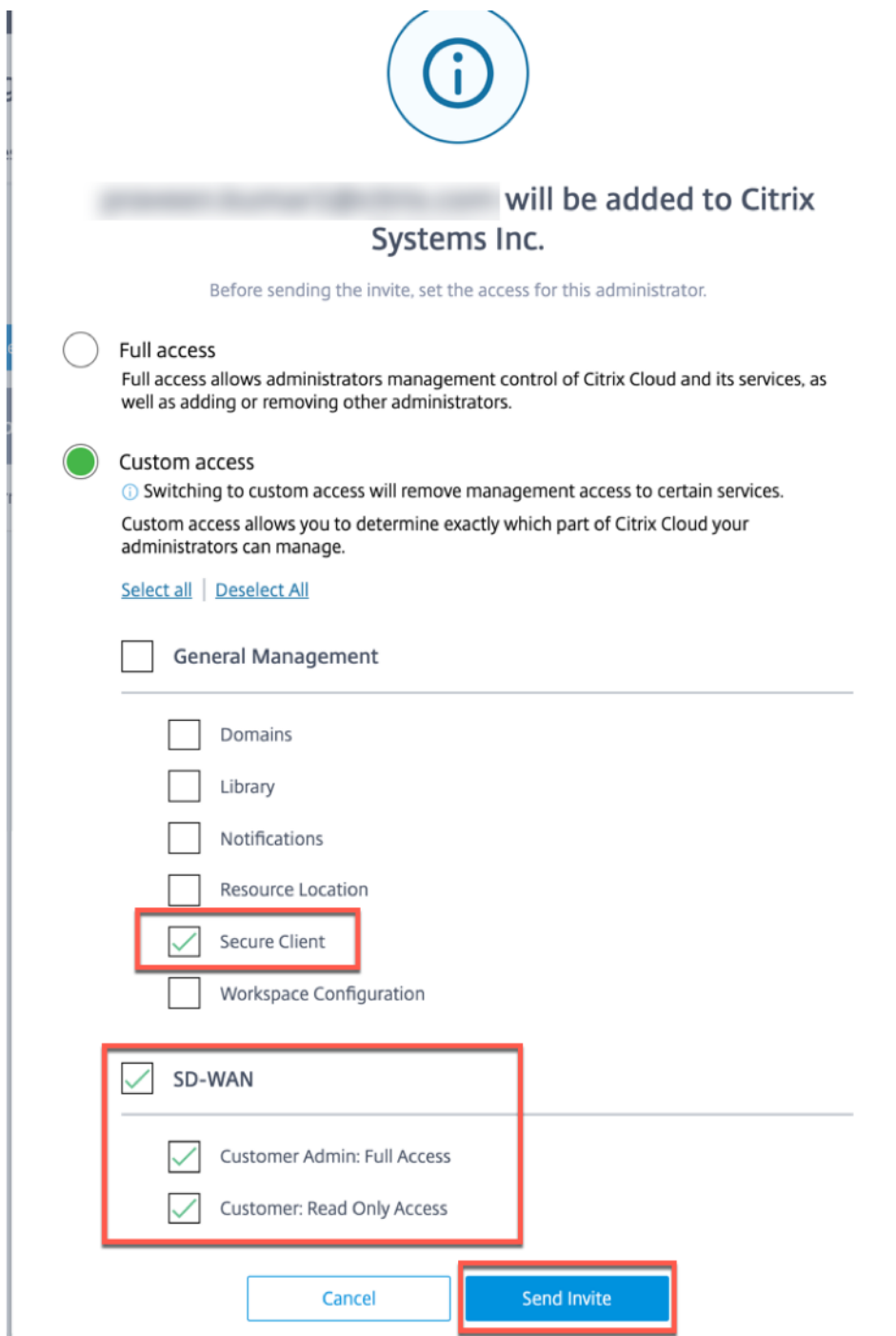
2. Go to **Administrators** page and select **Citrix Identity** from the identity provider drop-down list.




3. Enter the new administrator email id and click **Invite**.



4. It is recommended to set the custom access for the administrator. Select the **Custom access** radio button. Select the **Secure Client** check box from the **General Management** section and **SD-WAN** check box.






will be added to Citrix Systems Inc.

Before sending the invite, set the access for this administrator.

☐ Full access
Full access allows administrators management control of Citrix Cloud and its services, as well as adding or removing other administrators.

☒ Custom access
 Switching to custom access will remove management access to certain services.
Custom access allows you to determine exactly which part of Citrix Cloud your administrators can manage.
[Select all](#) | [Deselect All](#)

☐ General Management

☐ Domains

☐ Library

☐ Notifications

☐ Resource Location

☒ Secure Client

☐ Workspace Configuration

☒ SD-WAN

☒ Customer Admin: Full Access

☒ Customer: Read Only Access

[Cancel](#) [Send Invite](#)

5. Click **Send Invite**.

Once you created the administrator account, login through the administrator account to generate the **API** keys.

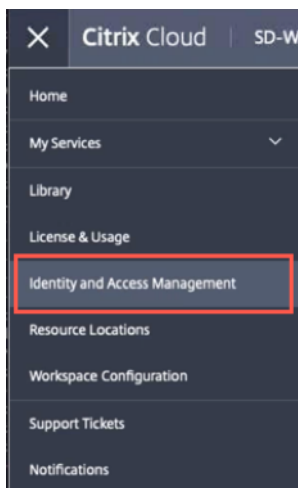
Note

If you already have a custom administrator role, they you can use it to create the API token.

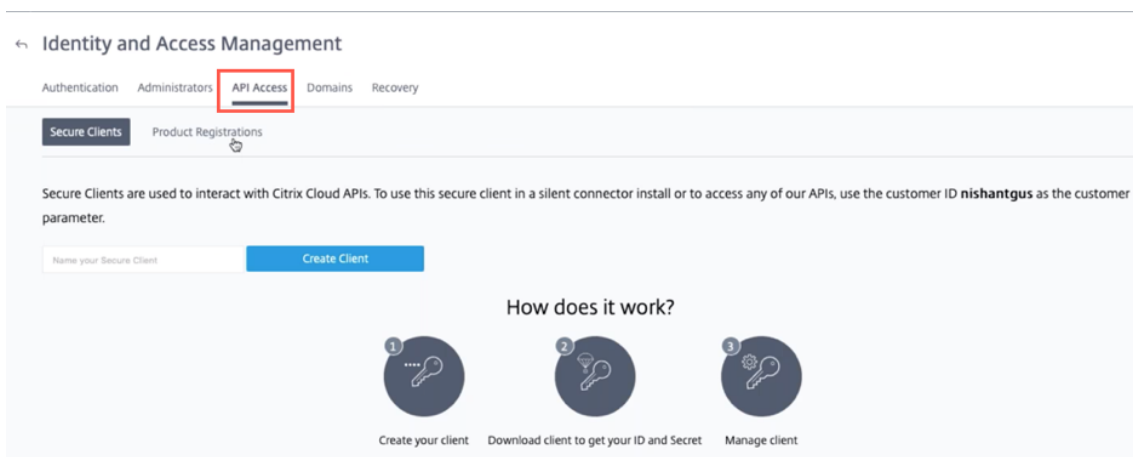
Generate API token

Perform the following steps to log in to the on-premises Orchestrator.

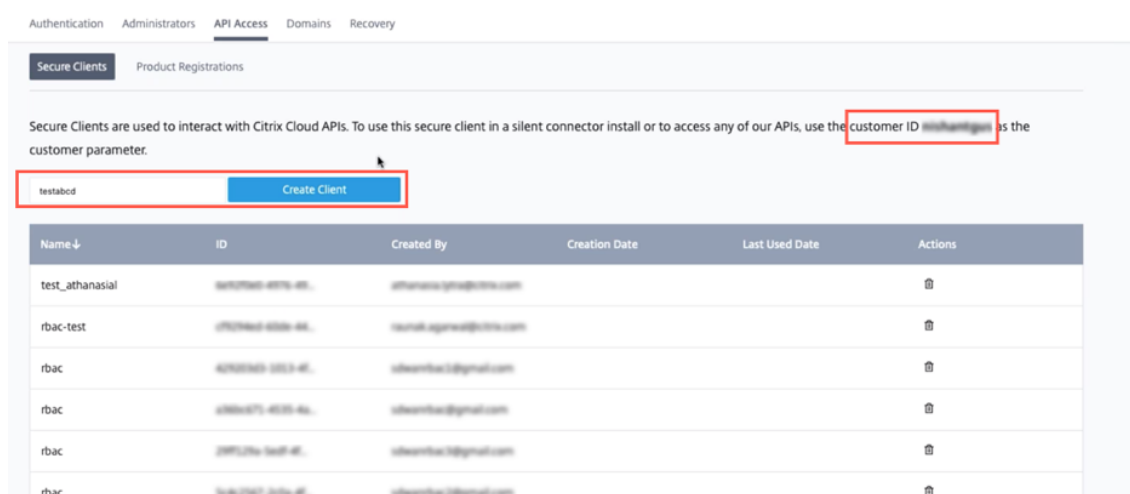
1. Log in to the Citrix Cloud and navigate to **Identity and Access Management**.



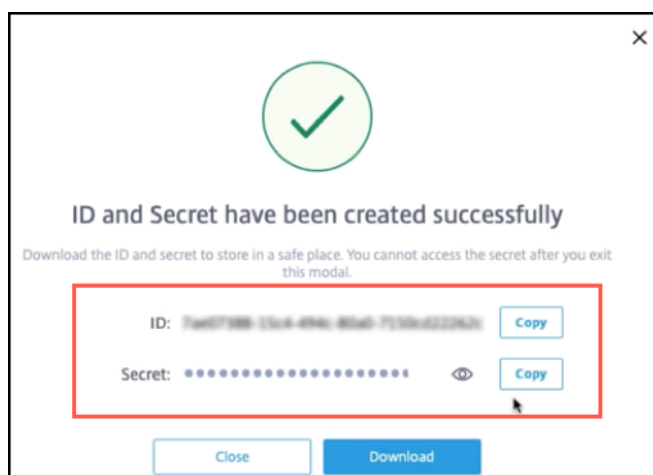
2. Go to **API Access** page.



3. Create a client. Note down the **Customer ID** that you need later for login to the on-premises Orchestrator.



- On click of **Create Client**, it provides you the **ID** and a **Secret key** that you can copy and save, or download.



- Go to your Citrix Hypervisor (XenServer/VMware) and boot up the on-premises Orchestrator.
- Once the SD-WAN Orchestrator for On-premises is booted up, provide the default user name (admin) and Password (password).

Note

It is mandatory to change the default admin user account password on a first time login. This change is enforced using both CLI and UI.

- If the DHCP server is not configured in the SD-WAN network, you have to manually enter a static IP address. To configure a static IP address as the management IP address:
 - In the console, enter the CLI command `management_ip`.
 - Enter the command `set interface <ipaddress> <subnetmask> <gateway>`.

Note

- The management IP address is the IP address of the Citrix on-premises SD-WAN Orchestrator virtual machine, use this IP address to log into the Citrix on-premises SD-WAN Orchestrator Web UI.
- The management interface can be configured via the two methods – CLI and DHCP.

8. Once the SD-WAN Orchestrator for On-premises is booted up, by default it is configured with DNS servers 9.9.9.9 & 149.112.112.112 as primary and secondary respectively. If necessary, you can change the DNS server IP address using the following commands:

- In the console, enter the CLI command `set_dns`.
- Enter the command `set primary <ipaddress>` and then enter `y` to confirm the change.
- Enter the command `set secondary <ipaddress>` and enter `y` to confirm the change.

```
SDWORCH>set_dns

Primary :          nameserver 9.9.9.9
Secondary :        nameserver 149.112.112.112

Which would you like to do?
  "set primary <ip address>" - Stage New Primary DNS IP Address
  "set secondary <ip address>" - Stage New Primary DNS IP Address
  "clear" - Clear all DNS IP Address
  "main_menu" - Return to the Main Menu

set_dns>set primary 8.8.8.8

Are you sure you want to change your Domain Name Server IP settings? <y/n>?
y

Primary :          nameserver 8.8.8.8
Secondary :        nameserver 149.112.112.112

Which would you like to do?
  "set primary <ip address>" - Stage New Primary DNS IP Address
  "set secondary <ip address>" - Stage New Primary DNS IP Address
  "clear" - Clear all DNS IP Address
  "main_menu" - Return to the Main Menu

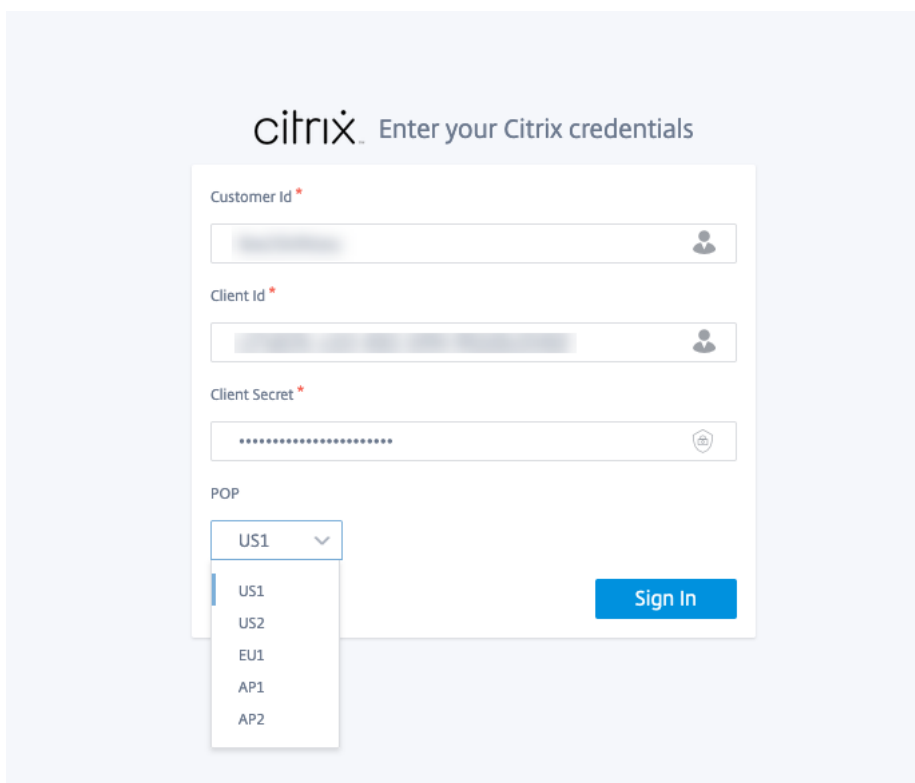
set_dns>set secondary 9.9.9.9

Are you sure you want to change your Domain Name Server IP settings? <y/n>?
y

Primary :          nameserver 8.8.8.8
Secondary :        nameserver 9.9.9.9

Which would you like to do?
  "set primary <ip address>" - Stage New Primary DNS IP Address
  "set secondary <ip address>" - Stage New Primary DNS IP Address
  "clear" - Clear all DNS IP Address
  "main_menu" - Return to the Main Menu
```

9. Open a new browser using the management IP. The following screen appears:

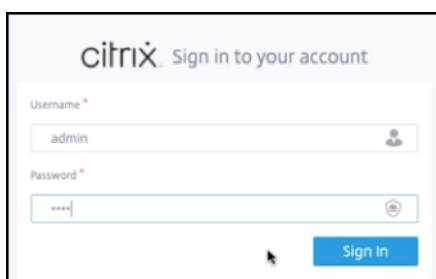
The image shows the Citrix login page for a cloud account. The header says "citrix Enter your Citrix credentials". There are four input fields: "Customer Id" with a red asterisk, "Client Id" with a red asterisk, "Client Secret" with a red asterisk, and "POP" with a dropdown menu. The "Client Secret" field is masked with dots. The "POP" dropdown menu is open, showing options: US1, US2, EU1, AP1, and AP2. A blue "Sign In" button is located to the right of the input fields.

10. Provide the **Customer ID**, **Client ID**, and **Client Secret** that you saved or downloaded earlier while creating the client from the cloud Orchestrator. Select the POP in which your cloud account was on boarded. You cannot change the POP after a successful login.

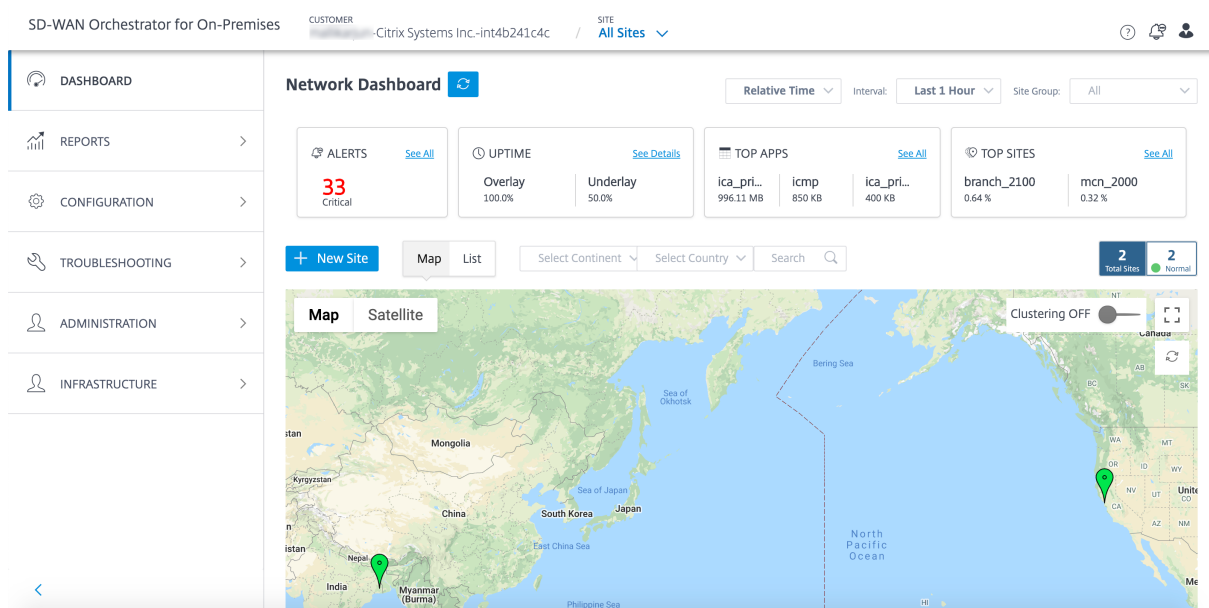
Note

This screen appears once in 15 days. For the subsequent log on/out, you see only the local login page.

11. Provide the default user name and password on the local login page.

The image shows the Citrix local login page. The header says "citrix Sign in to your account". There are two input fields: "Username" with a red asterisk and "Password" with a red asterisk. The "Username" field contains the text "admin". The "Password" field is masked with dots. A blue "Sign In" button is located to the right of the input fields.

You can see the SD-WAN Orchestrator for On-premises Dashboard page appears.



SD-WAN Orchestrator for On-premises licensing

March 17, 2021

SD-WAN Orchestrator for On-premises licensing is applicable for Do It Yourself (DIY) customers – Direct Enterprise Customers.

As a prerequisite for SD-WAN Orchestrator for On-premises licensing ensure that you are logged into the Citrix Cloud. For more information, see [SD-WAN Orchestrator for On-premises login](#).

SD-WAN Orchestrator for On-premises deployment is available free of charge, but the customer needs to bear the cost of management server infrastructure and maintenance.

Trial Mode

The customer's SD-WAN Orchestrator for On-premises account is provisioned in trial mode. The trial mode continues for a default period of 60 days.

After the trial period expires, the customer's data paths are brought down. Additional changes cannot be deployed until valid licenses are uploaded. The customer's Citrix Cloud entitlement for SD-WAN Orchestrator for On-premises changes from Trial to Production when the first valid license is hosted on it. Based on the number and type of licenses uploaded, an equivalent number of sites can come up with the right bandwidth entitlements. A persistent message "Your Trial has expired. Upgrade to Production by retrieving at least one valid license entitlement on the Orchestrator to restore the network functionality and continue the usage." is displayed for prepaid customers. For more information, see [Retrieve and assign entitlements for prepaid billing model](#).

Prepaid Billing Model

A prepaid billing model is provided for SD-WAN Orchestrator for On-premises customers. The following three types of prepaid billing models are available:

- **Prepaid annual subscription:** The prepaid subscription has a 1-year and a 3-year plan. The subscription expires on the expiry date. The Orchestrator and the maintenance license are included and no need to purchase them separately. All the appliances in the customer network have a prepaid annual subscription.
- **Prepaid perpetual:** With prepaid perpetual the licenses have no time limit, restricted duration, or expiration. However, the Orchestrator entitlements and hardware maintenance license must be purchased separately. All the appliances in the customer network have a prepaid perpetual subscription.

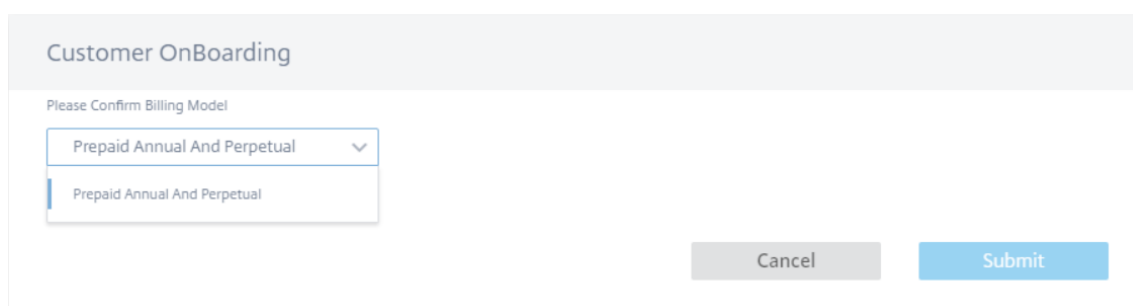
To view the billing model in SD-WAN Orchestrator for On-premises, at the network level navigate to **Administration > Licensing > Select Billing Model**. The billing model is displayed as **Prepaid Annual and Prepetual**.

Upload the licenses to all the customer sites. For more information, see Retrieve and assign entitlements for prepaid billing model.

Retrieve and assign entitlements for prepaid billing model

You can retrieve the license entitlements using the Access Code provided by Citrix via email. Alternatively, the customer can also view the Access Code in the [license management](#) portal within Citrix Cloud. The customer can have either **Prepaid Perpetual**, or **Prepaid Annual Subscription** billing model in the network.

1. In the SD-WAN Orchestrator for On-premises UI navigate to **Administration > Licensing** and click **Select Billing Model**. Select a billing model and click **Submit**.



Customer OnBoarding

Please Confirm Billing Model

Prepaid Annual And Perpetual ▼

Prepaid Annual And Perpetual

Cancel Submit

2. Click **Retrieve Licenses**.

Network Administration : Licensing

Licensing Model: None

Retrieve Licenses

Upgrade to Production

License View

Site View

Search

SDWAN Entitlements

Device Model	Software Edition	Bandwidth	Expiration Date	License Type	License Access Code	Licenses Available	Assigned To Sites	Actions
--------------	------------------	-----------	-----------------	--------------	---------------------	--------------------	-------------------	---------

Page Size: 25

Showing 0 - 0 of 0 items

Page 1 of 1

3. Click **+ License Access Code**, enter the required number of access codes to retrieve the entitlements and click **Submit**.

Retrieve Licenses

+ License Access Code

Enter License Access Cc

Enter License Access Cc

Submit

Cancel

The SD-WAN Orchestrator for On-premises retrieves the entitlements and populates the license table.

Device Model	Software Edition	Bandwidth	Expiration Date	License Type	Activation Code	Licenses Available	Assigned To Sites	Actions
CB210	SE	20	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB210	SE	20	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB210	SE	20	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB210	SE	50	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB210	SE	50	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB210	SE	50	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB210	SE	20	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB210	SE	50	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB1100	SE	200	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB1100	SE	200	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB210	SE	20	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB210	SE	20	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB210	SE	20	PERPETUAL	SD-WAN software Perpetual		1	0	Assign/Unassign
CB210	SE	20	PERPETUAL	SD-WAN software Perpetual		1	0	Assign/Unassign
CB210	SE	50	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB210	SE	50	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB210	SE	50	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign
CB210	SE	20	PERPETUAL	SD-WAN software Perpetual		1	1	Assign/Unassign

Note

The billing model is automatically selected based on the Access Code entered by the customer.

- Click **Assign/Unassign** and select **All Unlicensed**. All the unlicensed sites with configured bandwidth equal to or less than the license bandwidth is displayed.

Details of UnLicensed Sites

View: ☐ All Licensed ☒ All Unlicensed

<input type="checkbox"/>	Site	Device	Platform	Configured Bandwidth
<input checked="" type="checkbox"/>	Test_MCN	primary	VPX	200

Page Size: 25 Showing 1 - 1 of 1 items Page 1 of 1

- Select the sites, click **Assign** and then click **Upgrade to Production**.

In the **All Licensed** view, a list of licensed sites is displayed. You can choose to unassign the licenses and release it back to the pool.

Details of Licensed Sites

View: ☒ All Licensed ☐ All Unlicensed

<input type="checkbox"/>	Site	Device	Platform	Configured Bandwidth	Expiration Date
<input checked="" type="checkbox"/>	Test_MCN	primary	VPX	200	
<input checked="" type="checkbox"/>	Test_Branch1	primary	VPX	20	

Page Size: 25 Showing 1 - 2 of 2 items Page 1 of 1

Under **Site View**, the sites are automatically matched with licenses based on the configured bandwidth and license bandwidth, enabling you to allocate licenses quickly.

Note

To assign a license to the appliance, an appliance must have a verified serial number.

License View

Site View

Search

Site	License Status	HA Role	Device Model	Configured Bandwidth	Licensed Bandwidth	License Expiration	Software Maintenance	License Type	Action
Test_MCN	Active	primary	CBVPX	200	200	PERPETUAL	May 25, 2020 5...	SD-WAN softwar...	Unassign
Test_Branch1	Active	primary	CBVPX	20	200	PERPETUAL	May 25, 2020 5...	SD-WAN softwar...	Unassign

Page Size: 25 Showing 1 - 2 of 2 items Page 1 of 1

License Expiry

When the license expires, a grace period of 30 days is granted. The partner/customer is expected to renew their licenses during this time. After the grace period expires, the customer's network data paths are brought down, and additional changes cannot be deployed until the licenses are renewed.

Connectivity with Citrix SD-WAN appliances

February 11, 2021

After configuring sites on SD-WAN Orchestrator for On-premises, establish connectivity between Citrix SD-WAN appliances on the sites with SD-WAN Orchestrator for On-premises. You can establish connectivity in one of the following ways:

- **One-way Authentication:** The SD-WAN appliance authenticates SD-WAN Orchestrator for On-premises. On enabling one-way authentication, you must download the SD-WAN Orchestrator for On-premises certificate and upload it on the SD-WAN appliance.
- **Two-way Authentication:** The SD-WAN authenticate each other using the exchanged certificates. On enabling two-way authentication, you must upload the SD-WAN appliance certificate on SD-WAN Orchestrator for On-premises and also SD-WAN Orchestrator for On-premises certificate on the SD-WAN appliance.
- **No Authentication:** The connectivity is established between the SD-WAN Orchestrator for On-premises and SD-WAN appliances with no authentication. You need not use the SD-WAN Appliance or SD-WAN Orchestrator for On-premises Certificate. You can use No Authentication when you have a secure network such as MPLS.

Note

It is recommended to use only **one-way authentication** or two-way authentication. In the case of no Authentication, you have to choose the secure DNS server.

You can configure connectivity with each site manually or use the automated zero-touch deployment.

Note

Citrix SD-WAN 11.3.0 is the minimum software version required for an appliance to connect to SD-WAN Orchestrator for On-premises.

Zero-touch deployment

Zero-touch deployment is an automated process to configure connectivity between the appliances and SD-WAN Orchestrator for On-premises. The NITRO API running in the back-end handles download and upload of certificates. It downloads the certificate from SD-WAN Orchestrator for On-premises, logs in to the SD-WAN appliance, and uploads the certificate. It also downloads the SD-WAN appliance certificate and uploads it on SD-WAN Orchestrator for On-premises.

Note

Zero-touch deployment is supported on SD-WAN appliances running with the 11.2.1 release or later.

Zero-touch deployment supports only **one-way authentication** and **two-way authentication**. **No authentication** is not supported. If **Authentication Type** is enabled on **Administration > Certificate Authentication** page, then two-way authentication is established. If **Authentication Type** is disabled, then one-way authentication is established.

To configure Zero-touch deployment:

1. Navigate to **Administration > Site ZTD Settings**, and click **+ Site**.
2. Select a site from the **Site Name** drop-down list and enter the **Management IP** address of the Citrix SD-WAN appliance.
3. Enter the **Username** and **Password**.
4. Select the **Freshly Provisioned** check box if you are adding a newly provisioned site and enter a **New Password**.

NOTE

For a newly provisioned site, it is mandatory to change the default password at the time of first login.

5. Click **+** to add more sites.
6. Click **Add**. The configuration status of the sites is displayed in the **Auto Configured Sites** section.

i
Site ZTD Settings helps to configure On-prem SD-WAN Orchestrator Information on SD-WAN Appliances running 11.2.1 and above releases.

Add Sites

Site Name	Management IP	Username	Freshly Provisioned	Password	New Password	
branch_2100 ▾	<div style="background-color: #d3d3d3; width: 100px; height: 20px;"></div>	<div style="border: 1px solid #ccc; padding: 2px;">admin</div>	<input checked="" type="checkbox"/>	<div style="background-color: #d3d3d3; width: 100px; height: 20px;"></div>	<div style="background-color: #d3d3d3; width: 100px; height: 20px;"></div>	<div style="background-color: #007bff; color: white; width: 30px; height: 20px; margin: 0 auto; line-height: 20px;">+</div> <div style="background-color: #6c757d; color: white; width: 30px; height: 20px; margin: 0 auto; line-height: 20px;">-</div>

Add

Cancel

Manual Connectivity Configuration

While configuring connectivity manually, you must download the SD-WAN Orchestrator for On-premises certificate and upload it on each appliance in the network. It involves logging into each appliance manually for uploading the certificates.

To configure connectivity manually:

1. Navigate to **Administration > Certificate Authentication** and enable **Authentication Type**.

When Authentication Type is enabled, the SD-WAN appliance can connect to SD-WAN Orchestrator for On-premises only through Two-way Authentication. When Authentication Type is disabled, the SD-WAN appliance can connect to SD-WAN Orchestrator for On-premises either through No Authentication, One-way Authentication, or Two-way Authentication.

2. Click **Regenerate** and **Download** the SD-WAN Orchestrator for On-premises certificate.
3. Choose an appliance from the **Appliance Certificate** section and upload the corresponding certificate downloaded from the SD-WAN appliance. For detailed information on downloading the appliance certificate, see [Citrix SD-WAN Orchestrator on-premises configuration on SD-WAN appliance](#).

NOTE

Only .pem file type is supported.

4. Log on to the SD-WAN appliance UI, navigate to **Configuration > Virtual WAN > On-prem SD-WAN Orchestrator**. Upload the certificate downloaded from SD-WAN Orchestrator for On-premises. For detailed information, see [SD-WAN Orchestrator for On-premises configuration on SD-WAN appliance](#).

☒ Authentication Type

On-prem Orchestrator Certificate

Certificate Details:

Certificate Fingerprint: F2:3F: E:9F

Start Date: January 09 05:45:54 2021 GMT

End Date: January 07 05:45:54 2031 GMT

Regenerate Download

Appliance Certificate

Select an appliance

Click here to select the file or drag and drop the selected file.
 Allowed file type is .pem

Upload

Verify Connectivity

To verify the connectivity status of the appliance, navigate to **Configuration > Network Configuration Home**, and check the **Cloud Connectivity** column corresponding to your site.

Network Dashboard

Relative Time Interval: Last 1 Hour Site Group: All

ALERTS [See All](#)

UPTIME [See Details](#)

TOP APPS [See All](#)

TOP SITES [See All](#)

+ New Site

Map List

Select Continent Select Country Search

1 Total Sites 1 Inactive

Availability	Cloud Connectivity	Site Name	Site Role	Device Model	Serial Number	Bandwidth Tier	Management IP
●	Online	test	Branch	210		20	Unknown

Page Size: 25 Showing 1 - 1 of 1 items Page 1 of 1

Note

You can publish the desired software to upgrade the appliances under **Infrastructure > Orchestrator Administration > Software Images > Appliance**. For more information, see [Publish software](#).

March 8, 2021

Network configuration

This section offers enterprise network level configuration capabilities, and the starting point for configuring the SD-WAN network of an enterprise.

Network configuration: Home

This section act as an anchor for network configuration. The **Home** page provides the ability to initiate most of the commonly needed configuration actions, such as the ability to:

- Add a site
- Batch adds multiple sites at once
- Deploy configuration or upgrade software, and track the progress
- Back up/Review Checkpoints
- Perform the following operations:
 - Browse and Upload Config
 - Download Config JSON
 - Download Config DB
 - Add Region
 - Add Group

All the configured sites are displayed here. You can edit, update, delete, reset, and update the password of any site. You can also reboot the devices associated with a site.

Network Configuration: Home Site Group: All ▼

Software Version : 11.2.2.14 ▼

[+ Add Site](#)
[Batch Add Sites](#)
[Deploy Config/Software](#)
[Back Up/Review Checkpoints](#)
[More Actions ...](#)
[Deployment Tracker](#)

Availability	Cloud Connectivity	Site Name	Site Role	Device Model	Bandwidth Tier	Actions
●	● Online	HQ (HA)	MCN	VPX-SE	200	i edit ...
●	● Online	BR3	Branch	VPX-SE	200	i edit ...
●	● Online	BR1 (HA)	Branch	VPX-SE	200	i edit ...
●	● Online	BR2	Branch	VPX-SE	200	i edit ...

Page Size: 50 ▼ Showing 1-4 of 4 items Page 1 of 1 ◀ ▶

You can upgrade the SD-WAN software on all the appliances across the network, by simply selecting an appliance software version from the **Software Version** drop-down list.

Only the software versions that are published under **Infrastructure > Orchestrator Administration > Software Images > Appliance** get listed in the **Software Version** drop-down list. For more information, see [Publish software](#).

Network Configuration: Home

Software Version :


+ Add Site **Back Up/Review Checkpoint**

Availability	Cloud Connec
●	● Onl
●	● Onl
●	● Onl
●	● Onl

11.3.0.5022
11.3.0.5024
11.3.1.1
11.3.1.12
11.3.1.18
11.3.1.23
11.3.1.25
11.3.1.26
11.3.1.28
11.3.1.33

Deploy Config/Software

A confirmation message appears. Click **Proceed**.

 **SOFTWARE UPGRADE**

Are you sure you want to change the software across the network to 11.3.1.1 ? The change will be reflected on next deployment. Please confirm

Proceed **Cancel**

Add site

Use the **+ Add Site** option to add a new site. For more information on site configuration workflow, see [Site Configuration](#).

Batch add sites

The **Batch Add Sites** option allows you to quickly add several sites as a batch. You can also select a site profile to be used for each site, leaving you only with unique parameters such as IP addresses that remain to be configured for each site.

Network Configuration: Home

Site Group: All

of Sites 10

+

Site Profile: None

⌵

Show Lat/Lng

Site Name	Site Address	Site Profile (Optional)	Actions
Enter a Site Name	Search for a Site Address	None <div>⌵</div>	
Enter a Site Name	Search for a Site Address	None <div>⌵</div>	
Enter a Site Name	Search for a Site Address	None <div>⌵</div>	
Enter a Site Name	Search for a Site Address	None <div>⌵</div>	
Enter a Site Name	Search for a Site Address	None <div>⌵</div>	
Enter a Site Name	Search for a Site Address	None <div>⌵</div>	
Enter a Site Name	Search for a Site Address	None <div>⌵</div>	
Enter a Site Name	Search for a Site Address	None <div>⌵</div>	
Enter a Site Name	Search for a Site Address	None <div>⌵</div>	
Enter a Site Name	Search for a Site Address	None <div>⌵</div>	

CancelSave

Deploy Config/Software

The **Deploy Config/Software** option allows you to deploy the current configuration and software across the network, once the sites are configured. For more information on the deployment process, see **Deployment Tracker** section.

Deployment tracker

The **Deploy Config/Software** option takes you to the **Deployment Tracker** section to help verify the configuration, stage, and activate the same across the network.

Home **Verify Config** Current Deployment Deployment History Change Management Settings Site Details

Software Version : 11.4.0.96

Cancel Stage ✗ **Activate** ☐ Ignore Incomplete

1/2
Staged Appliances

0/2
Activated Appliances

Total Appliances	Ready For Activation	Activated	Failed	Offline
2	1	0	1	0

Search

Online	Site	Status	HA State	Software Version	Actions
Yes	main	Staging Complete	Not Configured	11.4.0.92.888881	
Yes	branch	Staging Failed	Not Configured	11.4.0.92.888881	

Page Size: 50 Showing 1-2 of 2 items Page 1 of 1

- **Stage:** Once the verification of configuration is successful, click **Stage** to distribute the configuration files to all the appliances in your network.
- **Active:** Click **Activate** to activate the staged configuration on all the sites across the network.

The **Deployment History** section helps to review the previous deployment operations and results.

Home **Verify Config** Current Deployment Deployment History Change Management Settings Site Details

Started At	Total Appliances	Total Activated	Total Failed	Not Needed	Offline
February 15, 2021 3:...	9	6	0	0	3
February 15, 2021 12:...	9	6	0	0	3
February 12, 2021 3:...	9	6	0	0	3
February 11, 2021 4:...	9	3	0	3	3
February 11, 2021 3:...	9	7	0	0	2
February 10, 2021 6:...	9	7	0	0	2
February 10, 2021 3:...	9	3	0	4	2
February 10, 2021 11:...	9	3	0	4	2
February 9, 2021 4:...	9	3	0	4	2
February 9, 2021 3:1...	9	7	0	0	2
February 8, 2021 3:...	9	7	0	0	2

HA near-hitless software upgrade

During software upgrade (11.0.x and earlier versions), the staging, and activation of all the appliances in the network are done at the same time. This includes the High Availability (HA) pair, leading to network downtime. With the HA near-hitless software upgrade feature, the SD-WAN Orchestrator for On-premises ensures that the downtime during the software upgrade (11.1.x and above) process is not

more than the HA switch over time.

Note

The HA near-hitless software upgrade is applicable for the following:

- The sites that are deployed in High Availability (HA) mode. It is not applicable for Non-HA sites.
- SD-WAN Orchestrator for On-premises based deployments only and not for the networks that are managed using the SD-WAN Center or MCN.
- Software upgrade only and not configuration updates. If there is configuration change along with the software as part of the upgrade, the SD-WAN Orchestrator for On-premises does not perform HA near-hitless software upgrade and continues to upgrade in the earlier fashion (single-step upgrade).

The upgrade sequence summary:

1. SD-WAN Orchestrator for On-premises checks for the HA state of all the appliances in the network.
2. Upgrades all the secondary appliances that are in **Standby** state.
3. HA switch-over is triggered and the state of the **Active** and **Standby** appliances are switched.
4. Upgrades the primary appliances that are now in **Standby** state.

The HA near-hitless software upgrade is a two-step upgrade process:

Step-1: During software upgrade, after the 11.1 release, the SD-WAN Orchestrator for On-premises first performs software upgrade on all the appliances that are in the **Standby** state across the network. The network is still up and running with the **Active appliances** in place.

After all the **Standby** appliances are upgraded to the latest software, the HA switch-over is triggered across the network. The **Standby** appliances (with the latest software) become **Active**.

Step-2: The current **Standby** appliances with an old software version are upgraded to the latest software and will continue to run in **Standby** mode.

During this software upgrade process, all other Non-HA sites will also be activated with the latest software.

For more information, see the [FAQs](#).

You can view the upgrade status by navigating to **Deployment Tracker > Current deployment**.

Software Version : 11.3.0.168

Stage ✓ **Activate** ✓ ☐ Ignore Incomplete

Staged Appliances 1/1

Activated Appliances 1/1

Total Appliances	Staged	Activated	Failed	Offline	Not Needed
3	1	1	0	0	2

Configuration Changes did not affect 2 sites. Sites displayed in the below table are being staged and the rest would just receive a timestamp update.

Online	Site	Status	HA State	Software Version
Yes	mcn1	Activation Complete	Not Configured	11.2.1.56.864672

- **Stage:** Click Stage to distribute the configuration files to all the appliances in your network.
- **Active:** Click Activate to activate the staged configuration on all the sites across the network.

Auto-correction for configuration and software upgrade

In the SD-WAN Orchestrator for On-premises, the auto-correction feature is implemented in the change management workflow.

When the staging failed for one site, and if the site that had failed staging is a control node, you need to restage after getting the staging failure message. The **Activate** button will not be enabled if the staging fails for the control nodes. In case, the site that had failed staging is a branch node, you are still allowed to move ahead with the activation. But to bring that branch in sync with the network, perform another round of change management.

Note

- The auto-correction check starts only after the **Activate** button has been clicked and stops once the next stage is issued from the SD-WAN Orchestrator for On-premises UI.
- The maintenance mode functionality is only applicable for the auto-correction feature. If you initiate a **Staging** and **Activation**, the appliance with the maintenance mode enabled also gets updated with the software and configuration changes.

With the auto-correction feature enhancement, when a staging failure happens, the auto-correction mechanism pushes the expected software and configuration version to the failed branch and tries to bring it up in sync with the current network. The auto-correction feature is applicable for staging failure on the branch node and activation failure on any node.

The following are the two trigger points when the auto-correction starts:

- In the SD-WAN Orchestrator for On-premises deployment tracker UI, once you get a **Staging Failed** or **Activation Failed** message, the auto-correction starts running in the background. The auto-correction check starts once the activation is completed.
- In the case of a software and configuration mismatch, where the appliance didn't come up with the expected software and configuration version, the SD-WAN Orchestrator for On-premises starts pushing the actual required software and configuration copy down to the appliance for activation.

To troubleshoot an appliance manually, enable the maintenance mode check box under the **Change Management Settings**. This check box is used to control if the device needs to be checked for auto-correction or not. Once the maintenance mode check box is cleared, auto-correction brings the appliance in sync with the network software and configuration version.

[Home](#)
[Verify Config](#)
[Current Deployment](#)
[Deployment History](#)
[Change Management Settings](#)

Scheduling Information				
Site Name	HA State	Scheduling Information	Maintenance Mode	Actions
HQ (Primary)	Active	2021-02-09 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 day)	<input type="checkbox"/>	
HQ (Secondary)	Standby	2021-02-09 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 day)	<input type="checkbox"/>	
BR2	Not Configured	2021-02-09 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 day)	<input type="checkbox"/>	
BR1 (Primary)	Standby	2021-02-09 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 day)	<input type="checkbox"/>	
BR1 (Secondary)	Active	2021-02-09 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 day)	<input type="checkbox"/>	
BR3	Not Configured	2021-02-09 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 day)	<input type="checkbox"/>	

Back up/Review checkpoints

The **Back Up/Review Checkpoints** option has the ability to back-up and restores the configuration, or review the saved checkpoints.

[Home](#)
[Verify Config](#)
[Back Ups / Checkpoints](#)

Back Up Current Config			
Config Checkpoint Name	Time of Creation	Comments	Actions
Autosaved-Running-Config	2021-2-9 1:52pm	Auto-generated	...
Autosaved-Previously-Loaded-Config	2021-2-2 10:00am	Auto-generated	...

Page Size: 50 Showing 1-2 of 2 items Page 1 of 1

Click **Verify Config** to validate any audit error.

Click **Back Up Current Config** option to back up the current configuration as a checkpoint for future use.

Backup Network

Backup Current Config As*

Enter a name for this backup

Comments (Optional)

Enter any comments

Cancel

Save

Click the cloud icon (under **Action**) to load a saved configuration. Click **Proceed**.

Load Configuration

Review the differences between the current configuration and the configuration checkpoint you're trying to load, in terms of the sites configured, as a quick sanity check. Are you sure you want to load the selected configuration checkpoint?

Site	Current Config	Saved Checkpoint About To Be Loaded
BR3	✓	✓
BR1	✓	✓
BR2	✓	✓
HQ	✓	✓

Cancel

Proceed

Click the book icon (under **Action**) to make a similar copy of an existing configuration. You can also download, edit, and delete the saved configuration checkpoints. These operations are available under **Action**.

More actions

Following are some of the additional actions available under **More Actions**:

- **Browse and Upload Config:** Browse and upload one of the previously saved configurations, and have that serve as the active configuration for the network.
- **Download Config JSON:** Allows you to download and export the current configuration in JSON format, for offline review.
- **Download Config DB:** Allows you to download and export the current configuration in DB format.
- **Add Region:** Create a Region.
- **Add Group:** Create a Custom Group of sites.

Update password

You can change the password of the SD-WAN appliances at different sites, across the network, through the SD-WAN Orchestrator for On-premises.

To change the password, for an appliance that is online click the more icon and select **Update Password**.

Network Configuration: Home Site Group: All

Software Version: 11.2.2.14

[+ Add Site](#)
[Batch Add Sites](#)
[Deploy Config/Software](#)
[Back Up/Review Checkpoints](#)
[More Actions ...](#)
[Deployment Tracker](#)

Availability	Cloud Connectivity	Site Name	Site Role	Device Model	Bandwidth Tier	Actions
●	● Online	HQ (HA)	MCN	VPX-SE	200	Clone
●	● Online	BR3	Branch	VPX-SE	200	Delete
●	● Online	BR1 (HA)	Branch	VPX-SE	200	Reboot
●	● Online	BR2	Branch	VPX-SE	200	Reset

Page Size: 50 Showing 1-4 of 4 items

Update Password

Provide the values for the following fields:

- **User Name:** Select a user name for which you want to change the password from the list of users configured at the site.
- **Current Password:** Enter the current password. This field is optional for admin users.
- **New Password:** Enter a new password of your choice.

- **Confirm Password:** Reenter the password to confirm it.

Update Device Password

User Name *

admin

Current Password *

.....

New Password *

.....

Confirm Password *

.....

Cancel

Save

March 8, 2021

Delivery services

Delivery services allow you to configure delivery services such as the Internet, Intranet, IPsec, and LAN GRE. The delivery services are defined globally and applied to WAN links at individual sites, as applicable.

Each WAN link can apply all or a subset of the relevant services, and setup relative shares of bandwidth (%) among all the delivery services.

Virtual Path service is available on all the links by default. The other services can be added as needed.

Delivery Services are delivery mechanisms available on Citrix SD-WAN to steer different applications or traffic profiles using the right delivery methods based on business intent.

Delivery Services can be broadly categorized as the following:

- **Virtual Path Service:** The dual-ended overlay SD-WAN tunnel that offers secure, reliable, and high-quality connectivity between two sites hosting SD-WAN appliances or virtual instances.
 - Click the **Setting** option next to the **Virtual Path** service to enable the auto-bandwidth provisioning across virtual paths. Set the minimum reserved bandwidth for each virtual path in Kbps. This setting is applied to all the WAN links across all sites in the network.

The screenshot shows a configuration window titled "Global Default per Link: Relative Bandwidth Provisioning across Virtual Paths". It contains a checkbox labeled "Enable Auto-Bandwidth Provisioning across Virtual paths" which is checked. Below this is a label "Minimum Reserved Bandwidth for each Virtual Path (Kbps) : *" followed by a text input field containing the value "80". At the bottom of the window are two buttons: "Cancel" and "Save".

- **Internet Service:** Direct channel between an SD-WAN site and public internet, with no SD-WAN encapsulation involved. Citrix SD-WAN supports session load-balancing capability for internet-bound traffic across multiple Internet links.
- **Intranet Service:** Underlay link based connectivity from an SD-WAN site to any non-SD-WAN site.


The traffic is unencapsulated or can use any non-virtual path encapsulation such as IPsec, GRE. You can set up multiple Intranet services.















Service and bandwidth

Under **Service and Bandwidth** tab, you can view an internet service is created by default. The branch traffic uses the transit sites to reach the internet. This section allows you to define new delivery services and default bandwidth allocation proportion (%) across all the delivery services. The bandwidth allocation needs across delivery services might vary based on the type of link involved.

For example, if you are using multiple SaaS applications, allocate a large proportion of bandwidth on your internet links for **Internet service** for direct internet breakout. On your MPLS links, allocate more bandwidth for **Virtual path service** or **Intranet Service** depending on whether your SD-WAN sites have most of the traffic going to other SD-WAN sites or non-SD-WAN sites.

Based on your requirements, you can define global bandwidth share defaults across delivery services for each link type – Internet links, MPLS links, and Private Intranet links.


Verify Config
Service & Bandwidth

Delivery Services		Global Service Bandwidth Defaults for each Link type					
		Internet Links		MPLS Links		Private Intranet Links	
Virtual Path  		100 %		100 %		100 %	
Internet  		0 %		0 %		0 %	
Citrix Secure Access Service   (Preview)		0 %		0 %		0 %	
Cloud Direct Service  		0 %		0 %		0 %	
Intranet + Service		0 %		0 %		0 %	
1.	Zscaler  	0 %		0 %		0 %	
2.	Azure Virtual WAN  	0 %		0 %		0 %	
3.	Non_SDWAN_Sites  	0 %		0 %		0 %	

Save

The default values can be overridden on individual links. While configuring WAN links, you can choose to use these global defaults or configure link specific service bandwidth settings. Configuration of a non-zero bandwidth share is required for any delivery service to be enabled and active on a link.

Internet service

Internet Service is available by default as part of the Delivery services. You can configure the internet service route cost relative to other delivery services. You can also preserve the route to the internet from the link even if all the associated paths are down.

Internet Service

Service Name
Cost

Advance Settings

☒ Preserve route to Internet from link even if all associated paths are down

Cancel
Save

Intranet service

You can create multiple intranet services. Once the intranet service is created at the global level, you can reference it at the WAN Link level. Provide a **Service Name**, select the desired **Routing Domain** and **Firewall Zone**. Add all the intranet IP addresses across the network, that other sites in the network might interact. You can also preserve the route to intranet from the link even if all the associated paths are down.

Intranet Service

Service Name *

Routing Domain

Firewall Zone

Intranet1

Default_RoutingDomain

Default_LAN_Zone

Intranet Networks

+ Network

Network IP / Prefix	Actions
10.29.30.1/22	

Advance Settings


☒ Preserve route to Intranet from link even if all associated paths are down

Cancel

Save

GRE service

You can configure SD-WAN appliances to terminate GRE tunnels on the LAN.

[Verify Config](#)[Service & Bandwidth](#)

GRE Details

Service Type	Name *	Routing Domain	Firewall Zone
LAN	GRE1	Default_RoutingDomain	<Default>
MTU	Keepalive (sec)	Keepalive Retries (sec)	<input checked="" type="checkbox"/> checksum
1500	10	3	

Site Bindings

Site Name	Source IP *	Public Source IP
Kansas	192.113.59.5	192.113.59.6
Destination IP *	Tunnel IP/Prefix *	Tunnel Gateway IP *
10.199.81.237	10.199.106.2/20	10.199.106.1
LAN Gateway IP *		
192.1.1.1		

CancelDone

GRE details

- **Service Type:** Select the service that the GRE tunnel uses.
- **Name:** Name of the LAN GRE service.
- **Routing Domain:** The routing domain for the GRE tunnel.
- **Firewall Zone:** The firewall zone chosen for the tunnel. By default, the tunnel is placed into the Default_LAN_Zone.
- **MTU:** Maximum transmission unit — the size of the largest IP datagram that can be transferred through a specific link. The range is from 576 to 1500. Default value is 1500.
- **Keep alive:** The period between sending keep alive messages. If configured to 0, no keep alive packets is sent, but the tunnel stays up.
- **Keep alive Retries:** The number of times that the Citrix SD-WAN Appliance sends keep alive packets without a response before it brings the tunnel-down.
- **Checksum:** Enable or disable Checksum for the tunnel's GRE header.

Site bindings

- **Site Name:** The site to map the GRE tunnel.
- **Source IP:** The source IP address of the tunnel. This is one of the Virtual Interfaces configured

at this site. The selected routing domain determines the available Source IP addresses.

- **Public Source IP:** The source IP if the tunnel traffic is going through NAT.
- **Destination IP:** The destination IP address of the tunnel.
- **Tunnel IP/Prefix:** The IP address and Prefix of the GRE Tunnel.
- **Tunnel Gateway IP:** The next hop IP Address to route the Tunnel traffic.
- **LAN Gateway IP:** The next hop IP Address to route the LAN traffic.

IPsec service

Citrix SD-WAN appliances can negotiate fixed IPsec tunnels with third-party peers on the LAN or WAN side. You can define the tunnel end-points and map the sites to the tunnel end-points.

You can also select and apply an IPsec security profile that define the security protocol and IPsec settings.

To configure an IPsec tunnel:

1. Specify the service details.
 - **Service Name:** The name of the IPsec service.
 - **Service Type:** Select the service that the IPsec tunnel uses.
 - **Routing Domain:** For IPsec tunnels over LAN, select a routing domain. If the IPsec Tunnel uses an intranet service, the intranet service determines the routing domain.
 - **Firewall Zone:** The firewall zone for the Tunnel. By default, the Tunnel is placed into the Default_LAN_Zone.
2. Add the tunnel end-point.
 - **Name:** When **Service Type** is Intranet, choose an Intranet Service the tunnel protects. Otherwise, enter a name for the service.
 - **Peer IP:** The IP address of the remote peer.
 - **IPsec Profile:** IPsec security profile that define the security protocol and IPsec settings.
 - **Pre Shared Key:** The pre-shared key used for IKE authentication.
 - **Peer Pre Shared Key:** The pre-shared key used for IKEv2 authentication.
 - **Identity Data:** The data to be used as the local identity, when using manual identity or User FQDN type.
 - **Peer Identity Data:** The data to be used as the peer identity, when using manual identity or User FQDN type.
 - **Certificate:** If you choose Certificate as the IKE authentication, choose from the configured certificates.
3. Map sites to the tunnel end-points.
 - **Choose Endpoint:** The end-point to be mapped to a site.
 - **Site Name:** The site to be mapped to the end-point.

- **Virtual Interface Name:** The virtual interface at the site to be used as the end-point.
 - **Local IP:** The local virtual IP address to use as the local tunnel end-point.
 - **Gateway IP:** The next hop IP address.
4. Create the protected network.
 - **Source Network IP/Prefix:** The source IP address and Prefix of the network traffic that the IPsec tunnel protects.
 - **Destination Network IP/Prefix:** The destination IP address and Prefix of the network traffic that the IPsec tunnel protects.
 5. Ensure that the IPsec configurations are mirrored on the peer appliance.

Service Details

Service Name *

Service Type *

Routing Domain

Firewall Zone

Default_RoutingDomain

<Default>

Tunnel End Points Across Network

Name *

Peer IP *

IPsec Profile

[+ IPsec Profile](#)

Pre Shared Key

Peer Pre Shared Key

Identity Data

Peer Identity Data

Certificate

Cancel

Done

Map Sites to Tunnel End Points

Choose Endpoint

Bindings

Site Name *

Virtual Interface Name *

Local IP *

Protected Networks

+

Source Network IP/Prefix

Destination Network IP/Prefix

Cancel

Done


For more information, see [How to configure IPsec tunnels for virtual and dynamic paths](#).

Dynamic virtual path settings

The global dynamic virtual path settings allow admins to configure dynamic virtual path defaults across the network.

A dynamic virtual path is instantiated dynamically between two sites to enable direct communication, without any intermediate SD-WAN node hops. Similarly, the dynamic virtual path connection is removed dynamically too. Both the creation and removal of dynamic virtual paths are triggered based on bandwidth thresholds and time settings.

Network Configuration : Dynamic Virtual Paths

 [Verify Config](#) [Dynamic Virtual Paths](#)

Dynamic Virtual Path

☐ Enable Dynamic Virtual Paths Across the Network

Route Cost
5

Max Paths Per Site
4

QoS Profile
Standard

Dynamic Virtual Path Creation Criteria

Measurement interval (s)
1

Throughput threshold (kbps)
600

Throughput threshold (pps)
45

Dynamic Virtual Path Removal Criteria

Measurement interval (m)
2

Throughput threshold (kbps)
45

Throughput threshold (pps)
35

Timers

Wait Time to flush dead virtual paths (m)
1

Hold Time before recreation of dead virtual paths (m)
10

Save

Click **Verify Config** to validate any audit error.

The following are some of the supported settings:

- Provision to enable or disable dynamic virtual paths across the network
- The route cost for dynamic virtual paths
- The QoS Profile to be used – **Standard** by default.

- Dynamic Virtual Path Creation Criteria:
 - **Measurement interval (seconds):** The amount of time over which the packet count and bandwidth are measured to determine if the dynamic virtual path must be created between two sites – in this case, between a given Branch and the Control Node.
 - **Throughput threshold (kbps):** The threshold of total throughput between two sites, measured over the **Measurement interval**, at which the Dynamic Virtual Path is triggered. In this case the threshold applies to the Control Node.
 - **Throughput threshold (pps)** - The threshold of total throughput between two sites, measured over the **Measurement interval**, at which the Dynamic Virtual Path is triggered.
- Dynamic Virtual Path Removal Criteria:
 - **Measurement interval (minutes):** The amount of time over which the packet count and bandwidth are measured to determine if a Dynamic Virtual Path must be removed between two sites – in this case, between a given Branch and the Control Node.
 - **Throughput threshold (kbps)** - The threshold of total throughput between two sites, measured over the **Measurement interval**, at which the Dynamic Virtual Path is removed.
 - **Throughput threshold (pps)** - The threshold of total throughput between two sites, measured over the **Measurement interval**, at which the Dynamic Virtual Path is removed.
- Timers
 - **Wait time to flush dead virtual paths (m):** The time after which a DEAD Dynamic Virtual Path is removed.
 - **Hold time before the recreation of dead virtual paths (m):** The time after which a Dynamic Virtual Path removed for being DEAD can be recreated.

IPsec encryption profiles

To add an IPsec encryption profile, navigate to **Configuration > Delivery Services > select IPsec Encryption Profiles**.



IPsec provides secure tunnels. Citrix SD-WAN supports IPsec virtual paths, enabling third-party devices to terminate IPsec VPN Tunnels on the LAN or WAN side of a Citrix SD-WAN appliance. You can secure site-to-site IPsec Tunnels terminating on an SD-WAN appliance by using a 140-2 Level 1 FIPS certified IPsec cryptographic binary.

Citrix SD-WAN also supports resilient IPsec tunneling using a differentiated virtual path tunneling mechanism.

IPsec profiles are used while configuring IPsec services as delivery service sets. In the IPsec security profile page, enter the required values for the following **IPsec Encryption Profile**, **IKE Settings**, and **IPsec Settings**.

Click **Verify Config** to validate any audit error.

IPsec encryption profile information

- **Profile Name:** Provide a profile name.
- **MTU:** Enter the maximum IKE or IPsec packet size in bytes.
- **Keep Alive:** Select the check box to keep the tunnel active and enable route eligibility.
- **IKE Version:** Select an IKE protocol version from the drop-down list.

The screenshot shows the 'IPsec Encryption Profile Information' form. It has a title bar 'IPsec Encryption Profile Information'. Below the title bar are four fields: 'Profile Name' with a red asterisk, 'MTU' with the value '1500', 'Keep Alive' with an unchecked checkbox, and 'IKE Version' with a dropdown menu showing 'IKEv1'.

IKE settings

- **Mode:** Select either Main mode or Aggressive mode from the drop-down list for the IKE Phase 1 negotiation mode.
 - **Main:** No information is exposed to potential attackers during negotiation, but is slower than Aggressive mode. **Main** mode is FIPS compliant.
 - **Aggressive:** Some information (for example, the identity of the negotiating peers) is exposed to potential attackers during negotiation, but is faster than Main mode. **Aggressive** mode is Non-FIPS compliant.
- **Authentication:** Choose the authentication type as Certificate or Pre-shared Key from the drop-down menu.
- **Identity:** Select the identity method from the drop-down list.
- **Peer Identity:** Select the peer identity method from the drop-down list.
- **DH Group:** Select the Diffie-Hellman (DH) group that are available for IKE key generation.
- **Hash Algorithm:** Choose a hashing algorithm from the drop-down list to authenticate IKE messages.
- **Encryption Mode:** Choose the Encryption Mode for IKE messages from the drop-down list.
- **Lifetime (s):** Enter the preferred duration (in seconds) for an IKE security association to exist.
- **Lifetime (s) Max:** Enter the maximum preferred duration (in seconds) to allow an IKE security association to exist.
- **DPD timeout (s):** Enter the Dead Peer Detection timeout (in seconds) for VPN connections.

The screenshot shows the 'IKE Settings' configuration page. It features a title bar 'IKE Settings' and a grid of configuration options. The 'Mode' dropdown is empty. 'Authentication' is set to 'Pre-Shared Key'. 'Identity' and 'Peer Identity' are both set to 'Auto'. 'DH Group' is set to 'Group1(MODP768)', 'Hash Algorithm' is 'MD5', and 'Encryption Mode' is 'AES 128-Bit'. The 'Lifetime (s)' field contains '3600', 'Lifetime (s) Max' contains '86400', and 'DPD timeout (s)' contains '300'.

IKE Settings		
Mode	Authentication	
<input type="text"/>	<input type="text" value="Pre-Shared Key"/>	
Identity	Peer Identity	
<input type="text" value="Auto"/>	<input type="text" value="Auto"/>	
DH Group	Hash Algorithm	Encryption Mode
<input type="text" value="Group1(MODP768)"/>	<input type="text" value="MD5"/>	<input type="text" value="AES 128-Bit"/>
Lifetime (s)	Lifetime (s) Max	DPD timeout (s)
<input type="text" value="3600"/>	<input type="text" value="86400"/>	<input type="text" value="300"/>

IPsec settings

- **Tunnel Type:** Choose **ESP**, **ESP+Auth**, **ESP+NULL**, or **AH** as the tunnel encapsulation type from the drop-down list. These are grouped under FIPS compliant and Non-FIPS compliant cate-

gories.

- **ESP:** Encrypts the user data only
 - **ESP+Auth:** Encrypts the user data and includes an HMAC
 - **ESP+NULL:** Packets are authenticated but not encrypted
 - **AH:** Only includes an HMAC
- **PFS Group:** Choose the Diffie-Hellman group to use for perfect forward secrecy key generation from the drop-down menu.
 - **Encryption Mode:** Choose the Encryption Mode for IPsec messages from the drop-down menu.
 - **Hash Algorithm:** The MD5, SHA1, and SHA-256 hashing algorithms are available for HMAC verification.
 - **Network Mismatch:** Choose an action to take if a packet does not match the IPsec Tunnel's Protected Networks from the drop-down menu.
 - **Lifetime (s):** Enter the amount of time (in seconds) for an IPsec security association to exist.
 - **Lifetime (s) Max:** Enter the maximum amount of time (in seconds) to allow an IPsec security association to exist.
 - **Lifetime (KB):** Enter the amount of data (in kilobytes) for an IPsec security association to exist.
 - **Lifetime (KB) Max:** Enter the maximum amount of data (in kilobytes) to allow an IPsec security association to exist.

The screenshot shows the 'IPsec Settings' dialog box. It features a title bar and several configuration fields arranged in two rows. The first row includes 'Tunnel Type' (set to ESP), 'PFS Group' (set to Group1(MODP768)), 'Encryption Mode' (set to AES 128-Bit), 'Hash Algorithm' (empty), and 'Network Mismatch' (empty). The second row includes 'Lifetime (s)' (28800), 'Lifetime (s) Max' (86400), 'Lifetime (KB)' (0), and 'Lifetime (KB) Max' (0). At the bottom of the dialog are 'Cancel' and 'Save' buttons.

Network location service

Network location service (NLS) is a Citrix Cloud service that determines if the user connecting to Citrix Virtual Apps and Desktops is from the internal network. Using NLS, you can avoid manually configuring IP addresses of Citrix SD-WAN deployed locations through the PowerShell script. For detailed information on NLS, see [Citrix Workspace Network Location Service](#).

You can enable NLS for all sites within the network or specific sites. The site enabled for NLS shares the Public IP address of all its internet WAN links along with other site details such as geographical location, time zone with the NLS database. With these details, the network location service determines if the user connecting to Citrix Virtual Apps and Desktops is on a network front ended by Citrix SD-WAN.

If a user request is coming from a network front ended by Citrix SD-WAN, the user is connected directly to Citrix Virtual Apps and Desktops Virtual Delivery Agent bypassing the Citrix Gateway service.

To enable NLS, at the network level, navigate to **Configuration > Delivery Services > Network Location Service**.

Select **Enable** if you want to enable NLS for all sites in the network. To enable NLS for specific sites, click **Add/Remove Sites**. Choose the **Region** and select the sites accordingly.

Click **Review** to view the sites that you have selected and click **Done**. Click **Deploy**.

The screenshot shows the 'Network Location Service' configuration page. At the top, there is a home icon, a 'Verify Config' button, and the page title 'Network Location Service'. Below this, there is a checkbox labeled 'Enable'. To the left of the main content area is a 'Select Region/Groups' panel with a 'Select All' checkbox (checked) and a 'Default' checkbox (checked). To the right is a 'Select Sites' panel with a 'Select All' checkbox (unchecked) and a list of sites: 'BR1' (checked), 'DC' (checked), 'Home110LTE' (unchecked), 'OnPrem210LTE' (unchecked), and 'BR1100' (unchecked). At the bottom left are 'Cancel' and 'Review' buttons, and a 'Deploy' button. At the bottom right, a status bar shows 'Showing 1 - 6 of 6 items' and 'Page 1 of 1' with navigation arrows.

Routing

April 29, 2021

The **Routing** section provides the following options:

- Routing Policies
- Routing Domains
- Import Route Profiles
- Export Route Profiles
- Transit Nodes

Routing policies

Routing policies help to enable traffic steering. Based on the selection (Application routes and IP Routes) you can use different ways to steer traffic.

Network Configuration : Routing Policies

Home **Verify Config** Application Routes IP Routes

Cost Ranges: Custom Application (1-20) Application (21-40) Application Group (41-60) IP (1-65535)

+ Application Route Search for Route


No	Match Type	Name	Delivery Service	Routing Domain	Sites	Cost	Actions
1	Application	iperf	Virtual Path- Belgium	Default_RoutingDomain	San Francisco	40	
2	Application Group	O365_Group	Internet Breakout	Default_RoutingDomain	Global	50	

Application Routes

Click **+ Application Route** to create application route.

- **Custom Application Match Criteria:**
 - **Match Type:** Select the match type as **Application/Custom Application/Application Group** from the drop-down list.
 - **Application:** Choose one application from the list.
 - **Routing Domain:** Select a routing domain.
- **Scope:** You can scope the application route at the global level or site and group specific level.
- **Traffic Steering;**
 - **Delivery Service:** Choose one delivery service from the list.
 - **Cost:** Reflects the relative priority of each route. Lower the cost, higher the priority.
- **Eligibility Based on Path:**
 - **Add Path:** Choose a site and WAN links. If the chosen path goes down, then the application route does not receive any traffic.

Network Configuration : Routing Policies


[Verify Config](#)
[Application Routes](#)
[IP Routes](#)

Cost Ranges: [Custom Application \(1-20\)](#) [Application \(21-40\)](#) [Application Group \(41-60\)](#) [IP \(1-65535\)](#)

Application Match Criteria

Match Type:
 Application*:
 Routing Domain:

Scope

☒ Global Route
 ☐ Site / Group Specific Route

Traffic Steering

Delivery Service:
 Cost*:

If a new application route gets added, then the route cost must be in the following range:

- **Custom application:** 1–20
- **Application:** 21–40
- **Application group:** 41–60

Office 365 optimization

The Office 365 Optimization features adhere to the [Microsoft Office 365 Network Connectivity Principles](#), to optimize Office 365. Office 365 is provided as a service through several service endpoints (front doors) located globally.

To achieve optimal user experience for Office 365 traffic, Microsoft recommends redirecting Office365 traffic directly to the Internet from branch environments and avoiding practices such as backhauling to a central proxy. This is because Office 365 traffic such as Outlook, Word are sensitive to latency and backhauling traffic introduces more latency resulting in poor user experience. Citrix SD-WAN allows you to configure policies to break out Office 365 traffic to the Internet. For more information, see [Office 365 Optimization](#).

In SD-WAN Orchestrator for On-premises, by-default every network have the office 365 rule under **Application Group**. To navigate, go to **Network Configuration > Routing > Routing Policies > Application Routes**.

The screenshot shows the 'Application Routes' configuration page in the SD-WAN Orchestrator. The left sidebar contains navigation options like Dashboard, Reports, Configuration, and Alerts. The main area displays a table of application routes. The second route, 'O365Optimize_InternetBreakout', is highlighted with a red border. Below the table, there are tabs for 'Verify Config', 'Application Routes', and 'IP Routes'. The 'Application Routes' tab is active, showing a list of routes with columns for No, Match Type, Name, Delivery Service, Routing Domain, Sites, Cost, and Actions.

No	Match Type	Name	Delivery Service	Routing Domain	Sites	Cost	Actions
1	Application Group	Default Cloud Dir...	Cloud Direct Service	Any	Global	45	
2	Application Group	O365Optimize_InternetBreakout	Internet Breakout	Any	Global	50	
3	Application Group	Citrix_Cloud_and...	Internet Breakout	Any	Global	50	

You cannot delete the rule but can configure the settings as required.

The screenshot shows the configuration settings for the 'O365Optimize_InternetBreakout' route. The left sidebar is the same as the previous screenshot. The main area displays the 'Application Group Match Criteria' configuration page. The 'Match Type' is set to 'Application Group' and the 'Application Group' is 'O365Optimize_InternetBreakout'. The 'Scope' is set to 'Global Route'. The 'Traffic Steering' section is expanded, showing 'Delivery Service' set to 'Internet Breakout'. Below this, there are sections for 'O365 Network Optimization Settings' and 'Allow' settings, including checkboxes for 'Teams Realtime', 'Exchange Online', 'SharePoint Optimize', 'Teams TCP Failback', 'Exchange Mail', 'SharePoint Allow', 'O365 Common', 'Default', 'Enable Beacon Service', and 'Enable O365 Intelligent Path Selection'. A warning message at the bottom states: 'Warning: Default Office 365 breakout policy is applicable only to app endpoints marked "required" in Default category. Please refer Microsoft Office 365 App Endpoints.'

Click the office 365 rule to view the default settings **Match Type, Application Group, Delivery Service**, and so on. You cannot modify these default settings.

Office 365 endpoints are a set of network addresses and subnets. From Citrix SD-WAN 11.4.0 onwards, Office 365 endpoints are classified into **Optimize**, **Allow**, and **Default** categories. Citrix SD-WAN provides a more granular classification of the **Optimize** and **Allow** categories, enabling selective bookending to improve the performance of network-sensitive Office 365 traffic. Directing network-sensitive traffic to SD-WAN in the cloud (Cloud Direct or an SD-WAN VPX on Azure), or from an at-home SD-WAN device to an SD-WAN at a nearby location with more reliable Internet connectivity, enables QoS and superior connection resilience compared to simply steering the traffic to the nearest Office 365 front door, at the cost of an increase in latency. A bookended SD-WAN solution with QoS reduces

VoIP dropouts and disconnects, reduces jitter and improves media-quality mean opinion scores for Microsoft Teams. Endpoints are segregated into the following three categories:

- **Optimize** - These endpoints provide connectivity to every Office 365 service and feature, and are sensitive to availability, performance, and latency. It represents over 75% of Office 365 bandwidth, connections, and volume of data. All the Optimize endpoints are hosted in Microsoft data centers. Service requests to these endpoints must be breakout from the branch to the Internet and must not go through the data center.

The **Optimize** category is classified into the following subcategories:

- Teams Realtime
 - Exchange Online
 - SharePoint Optimize
- **Allow** - These endpoints provide connectivity to specific Office 365 services and features only, and are not so sensitive to network performance and latency. The representation of Office 365 bandwidth and connection count is also lower. These endpoints are hosted in Microsoft data centers. Service requests to these endpoints might be breakout from the branch to the Internet or might go through the data center.

The **Allow** category is classified into the following subcategories:

- Teams TCP Fallback
 - Exchange Mail
 - SharePoint Allow
 - O365 Common

NOTE

The **Teams Realtime** subcategory uses the UDP real-time transport protocol to manage Microsoft Teams traffic, whereas the **Teams TCP Fallback** subcategory uses the TCP transport layer protocol. As media traffic is highly latency sensitive, you might prefer this traffic to take the most direct path possible and to use UDP instead of TCP as the transport layer protocol (most preferred transport for interactive real-time media in terms of quality). While UDP is a preferred protocol for Teams media traffic, it requires certain ports to be allowed in the firewall. If the ports are not allowed, Teams traffic uses TCP as a fallback, and enabling optimization for Teams TCP Fallback ensures better delivery of the Teams application in this scenario. For more information, see [Microsoft Teams call flows](#).

- **Default** - These endpoints provide Office 365 services that do not require any optimization, and can be treated as normal Internet traffic. Some of these endpoints might not be hosted in Microsoft data centers. The traffic in this category is not susceptible to variations in latency. Therefore, direct breaking out of this type of traffic does not cause any performance improvement when compared to Internet breakout. In addition, the traffic in this category may not always be

Office 365 traffic, hence it is recommended to disable this option when enabling the Office 365 breakout in your network.

NOTE

By default, options of the Default category and the Optimize and Allow subcategories are disabled. You cannot delete these settings but can enable as needed.

- **Enable Beacon Service** - Citrix SD-WAN allows you to perform beacon probing and determines the latency to reach Office 365 endpoints through each WAN link. Office 365 Beacon services are enabled by default. You can disable it by clearing this option. For more information, see [Office 365 Beacon service](#).

You can view the beacon probing availability and latency reports at [Network level](#) and [Site level](#).

- **Enable O365 Intelligent Path Selection** - Citrix SD-WAN allows you to choose the best available WAN link to manage Office 365 traffic. For example, if there are 2 WAN links configured for an Internet service, out of which one WAN link has a higher latency and the other WAN link has a lower latency, enabling intelligent path selection would select the WAN link with the lowest latency provided, the probes from the WAN link are not lossy.

You can view details about the WAN links with lowest latency and the total decisions taken at [O365 Metrics](#).

Note

If probes are lossy, Citrix SD-WAN uses the default Internet load-balancing logic to select the best WAN link although intelligent path selection is enabled.

SD-WAN appliance upgrade considerations

Optimize and Allow category:

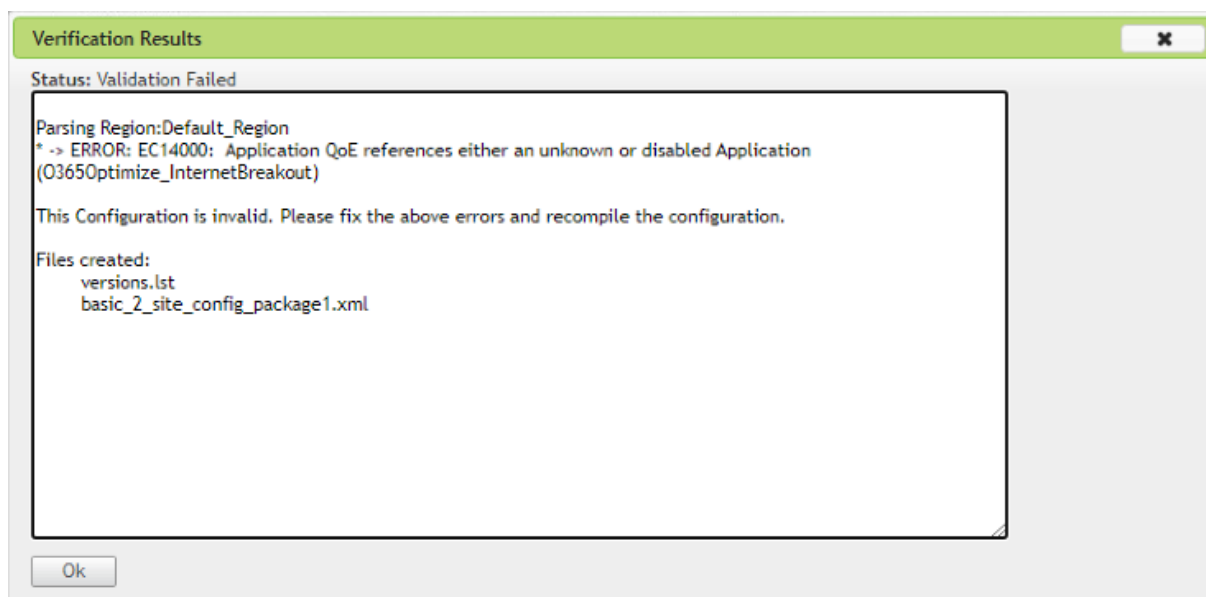
If you have enabled the Internet breakout policy for the **Optimize** and **Allow** Office 365 categories, Citrix SD-WAN automatically enables the Internet breakout policy for the corresponding subcategories upon upgrade to Citrix SD-WAN 11.4.0.

When you downgrade to a software version older than Citrix SD-WAN 11.4.0, you must manually enable Internet breakout for the **Optimize** or **Allow** Office 365 category irrespective of whether you enabled the corresponding subcategories in the Citrix SD-WAN 11.4.0 version or not.

Office 365 application objects:

If you have created rules/routes using the **O365Optimize_InternetBreakout** and **O365Allow_InternetBreakout** auto-generated application objects, ensure to delete the rules/routes before upgrading to Citrix SD-WAN 11.4.0. After the upgrade, you can create rules/ routes using the corresponding new application objects.

If you proceed with Citrix SD-WAN 11.4.0 upgrade without deleting the rules/routes, you see an error and thus, upgrade will not be successful. In the below example, a user has configured an Application QoE profile and is seeing an error while trying to upgrade to Citrix SD-WAN 11.4.0 without deleting the rules/routes.



Note

This upgrade is not required for auto-created rules/routes. It applies only to rules/ routes that you have created.

DNS:

If you have created DNS Proxy rules or DNS transparent forwarder rules using the **Office 365 Optimize** and **Office 365 Allow** applications, ensure to delete the rules before upgrading to Citrix SD-WAN 11.4.0. After the upgrade, you can create the rules again using the corresponding new applications.

If you proceed with Citrix SD-WAN 11.4.0 upgrade without deleting the old DNS proxy or transparent forwarder rules, you do not see any error and upgrade will be successful too. However, the DNS proxy rules and transparent forwarding rules will not take effect in Citrix SD-WAN 11.4.0.

Note

This activity does not apply to auto-created DNS rules. It applies only to DNS rules that you have created.

IP Routes

Go to **IP Routes** tab and click **+ IP Route** to IP Route policy to steer traffic.

- **IP Protocol Match Criteria:**

- **Destination Network:** Add the destination network that helps to forward the packets.
- **Use IP Group:** You can add a destination network or enable the **Use IP Group** check box to select any IP group from the drop-down list.
- **Routing Domain:** Select a routing domain from the drop-down list.

- **Scope:** You can scope the IP route at the global level or site and group specific level.

- **Traffic Steering:**

- **Delivery Service:** Choose one delivery service from the drop-down list.
- **Cost:** Reflects the relative priority of each route. Lower the cost, higher the priority.

If a new IP route gets added, then the route cost must be in 1-20 range.

- **Eligibility Criteria:**

- **Export Route:** If the **Export Route** check box is selected and if the route is a local route, then the route is eligible to be exported by default. If the route is an INTRANET/INTERNET based route, then for the export to work, WAN to WAN forwarding has to be enabled. If the **Export Route** check box is cleared, then the local route is not eligible to be exported to other SD-WAN and has local significance.

- **Eligibility based on Path:**

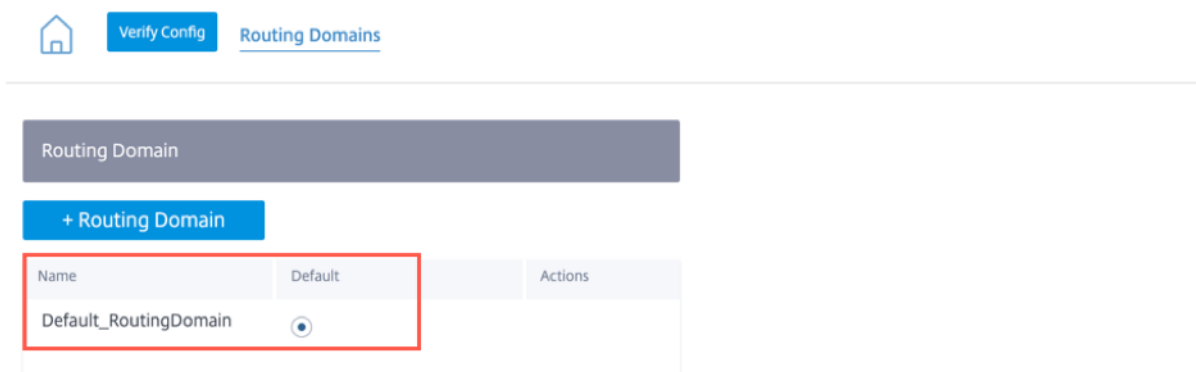
- **Add Path:** Choose a site and WAN links. If the added path goes down, then the IP route does not receive any traffic.

Click **Verify Config** to validate any audit error.

Routing domains

Routing Domains are used for segregate traffic through VLAN. Once the routing domains are created, you can reference them at the global level (for Intranet services) or interface level.

You can also select the default routing domain that applies to all the sites.



Name	Default	Actions
Default_RoutingDomain	<input checked="" type="radio"/>	

To match routes from a specific routing domain, click **+ Routing Domain** and choose one of the configured Routing Domains from the drop-down list. Click **Save**.

Network Configuration : Routing Domains

[Verify Config](#)[Routing Domains](#)

Routing Domain

Routing Domain Name

site1

VirtualInterface-1

MCN-2100

MCN-DC1

ServerVPX197

DC-410

Click **Verify Config** to validate any audit error.

For more information, see [Routing Domain](#).

Inter-routing domain service

SD-WAN Orchestrator for On-premises provides Static Inter-Routing Domain Service, enabling route leaking between Routing Domains within a site or between different sites. This eliminates the need for an edge router to handle route leaking. The Inter-VRF routing service can further be used to set up routes, firewall policies, and NAT rules.

For more information see, [Inter-routing domain service](#).

To configure the Inter-Routing Domain service through the SD-WAN Orchestrator for On-premises:

1. At the network level, navigate to **Configuration > Routing > Routing Domains > Inter-Routing Domain Service**.
2. Click **+ Inter-Routing Domain** and enter values for the following parameters:
 - **Name:** The name of the Inter-Routing Domain Service.
 - **Routing Domain 1:** The first Routing Domain of the pair.
 - **Routing Domain 2:** The second Routing Domain of the pair.
 - **Firewall Zone:** The Firewall Zone of the Service.
 - **Default:** The **Inter_Routing_Domain_Zone** firewall zone is assigned.
 - **None:** The service behaves like a conduit, which has no Zone and maintains the original zone of the packet.
 - All Zones configured in the network might be selected.

The screenshot displays the 'Network Configuration : Routing Domains' section. Under the 'Routing Domains' heading, there is a table listing existing domains: 'Default_RoutingDomain' (selected as default), 'RD1', and 'RD2'. Below this, the 'Inter Routing Domain Service' configuration form is shown, enclosed in a red box. The form contains the following fields:

- Name:** A text input field containing 'vrf_1'.
- Routing Domain1:** A dropdown menu with 'Default_RoutingDomain' selected.
- Routing Domain2:** A dropdown menu with 'RD1' selected.
- Firewall Zone:** A dropdown menu with '<Default>' selected.

At the bottom of the form are 'Cancel' and 'Save' buttons.

To create routes using the Inter-routing domain service, create a route with Service type as Inter-Routing Domain Service and select the inter-routing domain service. For more information on configuring Routes, see [Routing policies](#).

Network Configuration : Routing Policies

Verify Config Application Routes IP Routes

IP Protocol Match Criteria

Destination Network * ☐ Use IP Group Routing Domain

Scope

☒ Global Route ☐ Site / Group Specific Route

Traffic Steering

Delivery Service Service Name * Cost *

Eligibility Criteria

☒ Export Route

Cancel Save

Also add a route from the other Routing Domain pair, to establish connection to and fro between the two routing domains.

You can also configure firewall policies to control the flow of traffic between routing domains. In the firewall policies, select Inter-Routing domain service for the source and destination services and select the required firewall action. For information on configuring Firewall Policies, see [Firewall policies](#).

Network Configuration : Firewall Policies

Verify Config Firewall Policies

Match Criteria

Match Type Application * Routing Domain

Filtering Criteria

Source Zone Destination Zone

Source Service Type Source Service Name *

Dest Service Type Dest Service Name *

Source IP Source Port

Dest IP Dest Port

IP Protocol DSCP

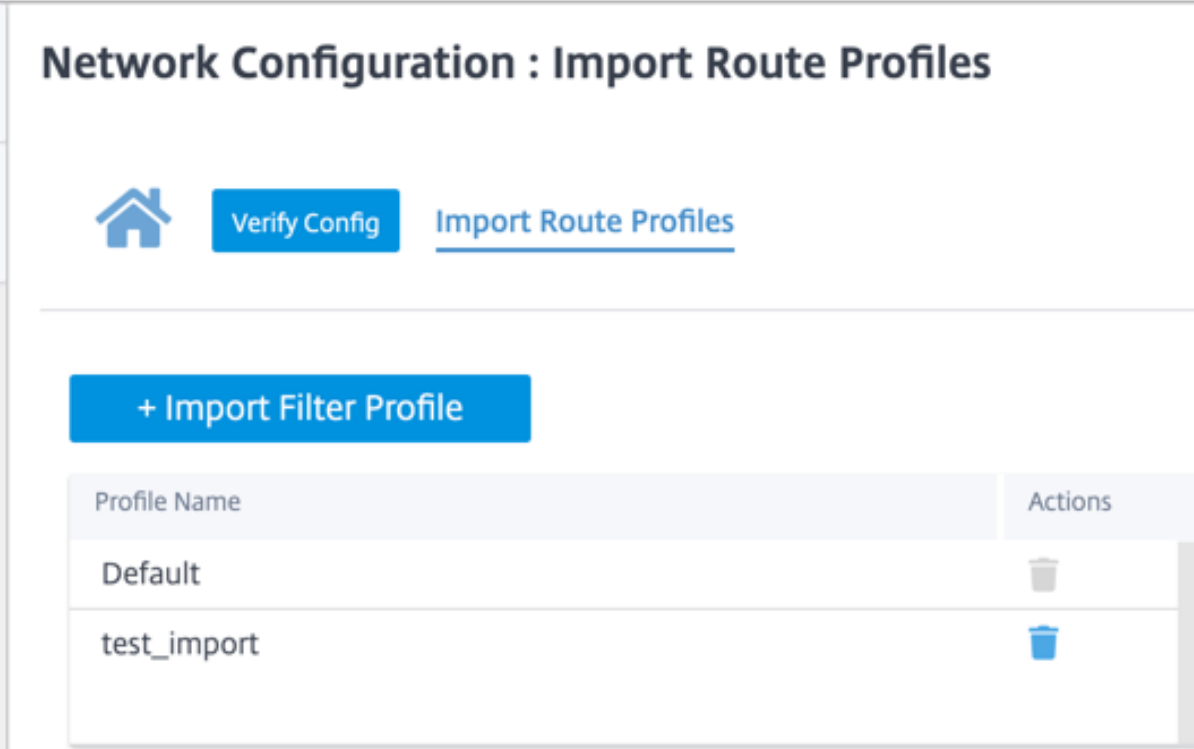
☒ Allow Fragments ☐ Reverse Also ☒ Match Established

You can also choose Intranet service type to configure Static and Dynamic NAT policies. For More information on configuring NAT policies, see [Network Address Translation](#).

Import route profiles

You can configure Filters to fine-tune how route-learning takes place.



Import filter rules are rules that have to be met before importing dynamic routes into the SD-WAN route database. By default, no routes are imported.



Network Configuration : Import Route Profiles


Home Verify Config Import Route Profiles

+ Import Filter Profile

Profile Name	Actions
Default	
test_import	

Add an **Import Filter Profile** with the **Import Profile Name**, **Profile Availability**, and **Import Filters** along with the following fields:

- **Protocol** - Select the protocol from the list.
- **Routing Domain** - To match routes from a specific routing domain, choose one of the configured Routing Domains from the list.
- **Source Router** - Enter the IP address and netmask of the configured network object that describes the route's network.
- **Destination IP** - Enter the destination IP address.
- **Prefix** - To match routes by prefix, choose a match predicate from the list and enter a Route prefix in the adjacent field.
- **Next Hop** - Enter the next hop destination.
- **Route Tag** - Fill the route tag.
- **Cost** - The method (predicate) and the SD-WAN Route Cost that are used to narrow the selection of routes exported.

[Verify Config](#)[Import Route Profiles](#)

Import Filter Profile

Import Profile Name *

MCN_KVMVPX

Import Filters

Protocol	Routing Domain	Source Router	Destination IP	<input type="checkbox"/> Use IP Group	Prefix	Next Hop	Route Tag	Cost
Any	Default_RoutingDomain	*	*		eq	*	*	eq

☒ Include☒ Export Route to Citrix SD-WAN Appliances

Citrix SD-WAN Cost *

6

Service Type

Local

Cancel

Done

Profile Availability


Site Name
<input type="checkbox"/> abcde
<input type="checkbox"/> Delhi Vikram
<input type="checkbox"/> Berlin
<input type="checkbox"/> Colombia
<input type="checkbox"/> Miami

Done

Click **Verify Config** to validate any audit error.

Export route profiles

Define the rules that have to meet when advertising SD-WAN routes over dynamic routing protocols. By default, all routes are advertised to peers.

[Verify Config](#)[Export Route Profiles](#)

Export Filter Profile

Export Profile Name *

Enter Template Name

Export Filters

Routing Domain

Default_RoutingDomain

Network Address/Mask

*

Use IP Group

☐

Prefix

eq

*

Cost

eq

*

Service Type

Local

Gateway IP Address

*

Export OSPF Route Type

Type 5 AS External

Export OSPF Route Weight

Weight

Include

☒

Cancel

Done

Profile Availability

	Site Name
<input type="checkbox"/>	abcde
<input type="checkbox"/>	Delhi Vikram
<input type="checkbox"/>	Berlin
<input type="checkbox"/>	Colombia
<input type="checkbox"/>	Miami

Done

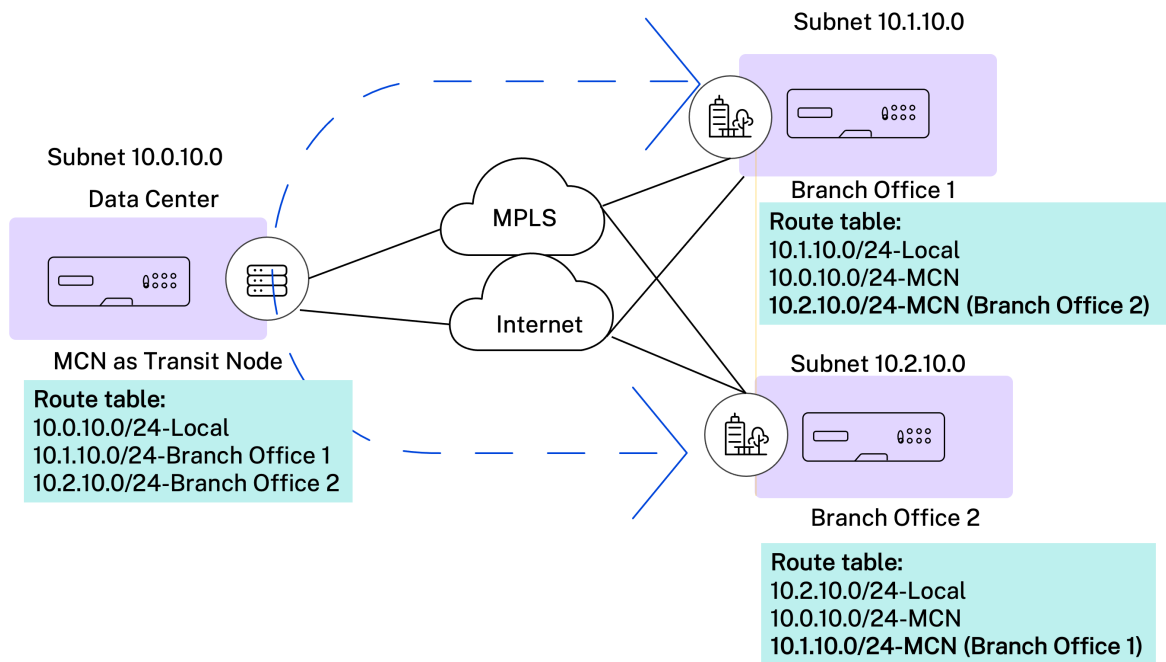
Click **Verify Config** to validate any audit error.

Transit nodes

Virtual overlay Transit Node

Transit nodes are the sites that are able to forward traffic between one or more branches within a region.

The traffic between two nodes can be influenced to pick transit node as an intermediate hop by adjusting the route cost. Transit nodes are used to route data to non-adjacent nodes. For example, if three nodes are connected in series A-B-C, then data from A to C can be routed via B. You can specify the transit node and the sites to be routed through the transit node in the Citrix SD-WAN Orchestrator service. The virtual paths are chosen in the ascending order of cost. Lower the cost, higher the priority.



Default global virtual overlay transit nodes

You can specify the control nodes (MCN/RCN) and the geo-control nodes (Geo-MCN/RCN) to act as the default global virtual overlay transit nodes in a network. Enabling hub-and-spoke communication as part of global settings allows all the sites to use the configured control nodes as transit nodes, by default, for site-to-site communication.

☒ Enable Hub-and-Spoke communication by default across the network (Recommended)

Restore Default

Default Global Virtual Overlay Transit Nodes

+ Add Node

Transit on Control Node	Default Virtual Path Cost (Site to Control Node)
<input checked="" type="checkbox"/> Greece_Site Clone	6
<input checked="" type="checkbox"/> Germany_Masternode	6

Save

+ Add Geo-Node

Transit on Geo-Control Node	Default Virtual Path Cost (Site to Geo-Control Node)
<input checked="" type="checkbox"/> London_Site	8

Add the control node and geo-control nodes that you want to use as virtual overlay transit nodes and specify the virtual path cost. The control nodes and geo-control nodes have 6 and 7 as the respective default virtual path costs. You can choose to change the virtual path cost as per your network requirement. Click **Restore Default** to restore the default virtual path costs for the default transit nodes.

Note

You can add a maximum of 3 control nodes and 3 geo-control nodes as transit nodes.

By default, WAN-to-WAN forwarding is enabled on all the paths associated with the selected control and geo-control nodes. WAN-to-WAN forwarding allows a site to act as an intermediate hop between two adjacent sites for any site-to-site, internet or intranet traffic and to act as a mediator for Dynamic Virtual Paths.

You can enable or disable route exporting on all the paths of a transit Node. Enabling control transit node settings (green button), enables virtual path-to-virtual path forwarding and route exporting (WAN-to-WAN forwarding) on all the site paths. Disabling the green button enables only virtual path-to-virtual path forwarding and disables route exporting on all the site paths.

Default Global Virtual Overlay Transit Nodes

+ Add Node

Transit on Control Node	Default Virtual Path Cost (Site to Control Node)
<input checked="" type="checkbox"/> Greece_Site Clone	6
<input checked="" type="checkbox"/> Germany_Mastermode	6

+ Add Geo-Node

Transit on Geo-Control Node	Default Virtual Path Cost (Site to Geo-Control Node)
<input checked="" type="checkbox"/> London_Site	8

Save

Site specific preferences for virtual overlay transit nodes

Site-specific preferences for virtual overlay transit nodes allow you to override the global virtual overlay transit node settings for all the sites in your network. You can also choose a non-control node as the primary transit node for a site. Choose a control node or geo-control node as the secondary and the tertiary transit nodes. If the primary transit node is down, the sites use the secondary transit node. If both primary and secondary transit nodes are down, the sites use the tertiary transit node. Specify the cost for the transit nodes and select the sites to which the site-specific virtual overlay transit node settings are applied.

Site Specific Preferences for Virtual Overlay Transit Nodes

Primary Transit Node *

Germany_Masternode

Cost

6

Secondary Transit Node

London_Site

Cost

7

Tertiary Transit Node

Greece_Site_Clone

Cost

8

Sites to be Routed via Intermediate Node

Select Region/Groups

☒ Select All

☒ default

Select Sites

☒ Select All

☒ London_Site

Cancel

Review

Showing 1 - 2 of 2 items

Page 1 of 1

Internet Transit Node

You can add sites as Internet transit sites to enable Internet access to the sites. Sites that need direct internet connectivity, must have at least one link with Internet service enabled. That means, at least one link set to a non-zero bandwidth share %.

Each transit site can be assigned a route cost. The sites with internet service available access the internet directly since the direct route would be the lowest cost routing path. Sites without internet service can route to the internet through the configured transit sites. When the internet transit sites are configured, routes to the internet through these transit sites are automatically pushed to all the sites. Internet transit sites are the sites with Internet service enabled.

For example, if San Francisco and New York are configured as internet transit sites. Routes to the internet via San Francisco and New York automatically get pushed to all the sites.

The virtual overlay transit node with Internet service enabled acts as the primary internet transit node. If internet service is not enabled on the virtual overlay transit node the secondary / backup internet transit node provides a route to the internet.

© 1999-2021 Citrix Systems, Inc. All rights reserved.

80

[Verify Config](#)
[Virtual Overlay Transit Nodes](#)
[Internet Transit Nodes](#)
[Intranet Transit Nodes](#)

Primary Default Internet Transit Nodes for the Network

Transit Node	Description
Virtual Overlay Transit Node	Virtual Overlay Transit routing node for each site doubles up as the primary Internet transit node, if Internet service is enabled on the Virtual Overlay Transit node. If not, the secondary / backup transit nodes provide a route to the Internet

Secondary / Backup Internet Transit Nodes for the Network

Service Name:

Select Region/Groups

☐ Select All

☐ Default

☐ B

☒ A

Select Sites

☐ Select All

☒ BLIS_RCN

☒ CNBX_GeoRCN

☐ BC_2963_Stellenbosch_UAT

Showing 1 - 4 of 4 items Page 1 of 1

Intranet Transit Node

The intranet transit node enables all the non-intranet sites to access the configured intranet networks. Each transit site can be assigned a route cost. The available sites with intranet service, accesses the intranet networks directly since the direct route would be the lowest cost routing path. Sites without intranet service can route to the intranet networks through the configured transit sites. When the transit sites are configured, routes to intranet networks through these transit sites are automatically pushed to all the sites.

For example, if 10.2.1.0/24 is an intranet network, and Austin and Dallas are the configured transit sites. Routes to that network address through Austin and Dallas automatically get pushed to all the sites. The virtual overlay transit node with Intranet service enabled acts as the primary intranet transit node. If intranet service is not enabled on the virtual overlay transit node the secondary / backup intranet transit node provides a route to the intranet.

Primary Default Intranet Transit Nodes for the Network

Transit Node	Description
Virtual Overlay Transit Node	Virtual Overlay Transit routing node for each site doubles up as the primary Intranet transit node, if Intranet service is enabled on the Virtual Overlay Transit node. If not, the secondary / backup transit nodes provide a route to the Intranet

Secondary / Backup Transit Nodes to reach the subnets selected

Service Name: Non_SDWAN_Sites

Select Region/Groups

☐ Select All

☐ Default

☒ B

☐ A

Select Sites

☒ Select All

☒ CNBX_RCN

☒ BLIS_GeoRCN

☒ LAB_210_SITE_B

Cancel Review Save

Showing 1 - 4 of 4 items Page 1 of 1

Inter-link communication

October 21, 2020

Inter-link communication settings are used for auto-path creation between compatible WAN links. You can override these settings under **Site Configuration** and **Virtual Paths**, wherein you can select or unselect individual member paths for a given virtual path.

Currently, the following two settings are available:

- Rules to automate the creation of paths between compatible WAN links.
- Global defaults for Dynamic Virtual Paths

These settings are inherited by all WAN links in the customer network.

Click **Verify Config** to validate any audit error.

Default inter-link communication groups

Default inter-link communication groups are intended at automating the creation of paths between:

- Any two internet links
- Any two MPLS links that share the same service provider, and
- Any two Private Intranet links that share service provider

Custom inter-link communication groups

Custom inter-link communication groups enable private Intranet, public Internet, or MPLS links to automatically create paths with other private Intranet, public Internet, or MPLS links across varying service providers.

For example, consider this scenario - A company has offices in the US and India. The US offices use AT&T MPLS links, while the India offices use Airtel MPLS links. Let's say AT&T and Airtel MPLS links are compatible in terms of DSCP tags and related parameters and are amenable for the creation of paths with each other. Custom inter-link communication rules allow you to select an ISP pair (for example ATT – Airtel in this case) and enable auto-creation of paths among the links belonging to these ISPs.

Default Inter-link Communication Groups

No	Group Name	Description
1	Internet-All	All Internet links can talk to each other by default. If a sub-set of internet links need to talk only among t...
2	MPLS-Same-ISP	All MPLS links belonging to the same ISP can talk to each other by default, through auto-creation of paths
3	Private Intranet-Same-ISP	All Private Intranet links belonging to the same ISP can talk to each other by default, through auto-creati...

Custom Inter-link Communication Groups

MPLS Groups Private Intranet Groups Internet Communication Override Groups

Group the desired MPLS service provider names, to enable the corresponding links to talk to each other.

+ MPLS Inter-link Communication Group

No	Group Name	Service Providers	Actions
----	------------	-------------------	---------

- **MPLS Groups:** You can group the desired MPLS service provider names to enable the corresponding links to communicate with each other. Click **+ MPLS Inter-link Communication Group** and provide an MPLS group name, select the DSCP tag from the drop-down list. You can also add the MPLS provider by selecting the ISP name from the drop-down list. The **Enable Encryption** check box helps to enable/disable the encryption for every custom MPLS Inter-Link Communication Group.
- **Private Intranet Groups:** You can group the desired Intranet service provider names to enable the corresponding links to communicate with each other. Click **+ Private Intranet Inter-link Communication Group** and provide the private intranet group name, select the DSCP tag from the drop-down list. You can also add the private intranet provider by selecting the ISP name from the drop-down list. The **Enable Encryption** check box helps to enable/disable the encryp-

tion for every custom private Intranet Inter-Link Communication Group.

- **Internet Communication Override Groups:** If a subset of Internet links must talk only among themselves and not with the rest of the Internet links, then you can group the corresponding ISP names to enable exclusion from the default group.

The rest of the Internet links can still communicate with each other. Click **+ Public Internet Inter-link Communication Group** and provide a public internet group name, select the DSCP tag from the drop-down list. You can also add the public Internet provider by selecting the ISP name from the drop-down list. The **Enable Encryption** check box helps to enable/disable the encryption for every custom public Internet Inter-Link Communication Group.

Default Inter-link Communication Groups

No	Group Name	Description
1	Internet-All	All Internet links can talk to each other by default. If a sub-set of internet links need to talk only among themselves and not with the broad...
2	MPLS-Same-ISP	All MPLS links belonging to the same ISP can talk to each other by default, through auto-creation of paths
3	Private Intranet-Same-ISP	All Private Intranet links belonging to the same ISP can talk to each other by default, through auto-creation of paths

Custom Inter-link Communication Groups

MPLS Group Name *

DSCP Tag

☒ Enable Encryption

+ MPLS Provider

Cancel Save

QoS policies

April 22, 2021

An administrator can define application and traffic policies. These policies help to enable traffic steering, Quality of Service (QoS), and filtering capabilities for applications. Specify whether a defined rule can be applied globally across all the sites in the network or on certain specific sites.

Policies are defined in the form of multiple rules which get applied in the user-defined order.

[Verify Config](#)[QoS Policies](#)[Global Rules](#) Site / Group Specific RulesGlobal QoS Bandwidth Default Profile : Standard[QoS Bandwidth Profiles](#)

(Standard-HDX-Multistream profile recommended for multi-stream HDX users)

Custom Application Rules

Application Rules

HDX Rules (preview)

Application Group Rules

IP Rules

Default IP-Protocol Rules

No	Protocol	DSCP	Service	Transmit Mode	QoS Setting
1	SIP	ef	Virtual Path	Duplicate Paths	High : Realtime
2	ICA	Any	Virtual Path	Load Balance Paths	High : Interactive
3	ICACGP	Any	Virtual Path	Load Balance Paths	High : Interactive
4	ICAUDP	Any	Virtual Path	Load Balance Paths	High : Interactive
5	ICACGPUDP	Any	Virtual Path	Load Balance Paths	High : Interactive
6	ICMP	Any	Virtual Path	Persistent Path	Medium : Interactive
7	SSH	Any	Virtual Path	Load Balance Paths	Medium : Interactive
8	TELNET	Any	Virtual Path	Load Balance Paths	Medium : Interactive
9	RDP	Any	Virtual Path	Load Balance Paths	Medium : Interactive
10	RPC	Any	Virtual Path	Load Balance Paths	Medium : Interactive
11	LDAP	Any	Virtual Path	Load Balance Paths	Medium : Interactive
12	HTTP	Any	Virtual Path	Load Balance Paths	High : Bulk
13	ALHTTP	Any	Virtual Path	Load Balance Paths	High : Bulk
14	HTTPS	Any	Virtual Path	Load Balance Paths	High : Bulk
15	CIFS	Any	Virtual Path	Load Balance Paths	Low : Interactive
16	POP3	Any	Virtual Path	Load Balance Paths	Low : Interactive
17	SMTP	Any	Virtual Path	Load Balance Paths	Low : Interactive
18	IMAP	Any	Virtual Path	Load Balance Paths	Low : Interactive
19	FTP	Any	Virtual Path	Load Balance Paths	Medium : Bulk
20	IPERF	Any	Virtual Path	Load Balance Paths	Medium : Bulk
21	GRE	Any	Virtual Path	Load Balance Paths	Low : Interactive
22	DNS	Any	Virtual Path	Load Balance Paths	Low : Interactive
23	SNMP	Any	Virtual Path	Load Balance Paths	Low : Interactive
24	SNMP	Any	Virtual Path	Load Balance Paths	Low : Interactive
25	Any	ef	Virtual Path	Duplicate Paths	High : Realtime
26	Any	af11	Virtual Path	Persistent Path	Medium : Interactive
27	UDP	Any	Virtual Path	Persistent Path	Medium : Interactive
28	TCP	Any	Virtual Path	Load Balance Paths	Low : Interactive
29	Any	Any	Virtual Path	Persistent Path	Low : Interactive

Create new rule

An administrator needs to place the defined rule based on the priority. The priorities such as Top of the List, Bottom of the List, or in between two existing entries.

It is recommended to have **more specific** rules for applications or sub applications at the top, followed by **less specific** rules for the ones representing broader traffic.

For example, you can create specific rules for both Facebook Messenger (sub application) and Facebook (application). Put a Facebook Messenger rule on top of the Facebook rule so that the Facebook Messenger rule gets selected. If the order is reversed, Facebook Messenger being a subapplication of the Facebook application, the Facebook Messenger rule would not get select. It is important to get the order right.

Match criteria

Select traffic for a defined rule such as:


- An application
- Custom defined application
- Group of applications or IP protocol based rule

Rule scope

Specify whether a defined rule can be applied globally across all the sites in the network or on certain specific sites.

Application steering

Specify how the traffic needs to be steered.

[Verify Config](#)[QoS Policies](#)

Global Rules : Custom Application

Custom Application Match Criteria

Custom Application * [+ New Custom App](#) Routing Domain

Any

Virtual Path Traffic Policy

☒ Enable Virtual Path Traffic Policy

Virtual Path Remote Site Traffic Policy

Any (determined by routing)

Load Balance Paths

QoS Settings

QoS Class

Transfer Type * Priority *

Interactive

Medium

Note: Bandwidth share available per QoS class per overlay virtual path is determined by [QoS Profiles](#). Intelligent default values are auto-picked, with ability to override the defaults via custom QoS profiles

⚙️ Advanced Settings

Cancel

Save

+ New Custom App: Select a match criteria from the list. The administrator can add new custom application by giving a name to:

- Custom application
- protocol (such as TCP, UDP, ICMP)
- Network IP/Prefix
- port
- DSCP tag

You can also create a domain name based custom application.

Custom Application

Custom App Name *

☒ IP Protocol
☐ Domain Name Based

Match Criteria

Add Match Criteria

Application	Protocol	Network IP	Port	DSCP	Actions

Cancel

Save


Click **Verify Config** to validate any audit error.

IP Rules

You can create global and site-specific IP rules at the network level by navigating to **Configuration > QoS > QoS Policies**.

- IP Protocol Match Criteria
 - Add/Remove Sites:** (available only while creating site-specific IP rule) Select the sites, click **Review**, and **Done**.
 - Source Network:** The source IP address and subnet mask that the rule matches.
 - Destination Network:** The destination IP address and subnet mask that the rule matches.
 - Use IP Group:** Select the **Use IP Group** check box to choose any existing IP group from the drop-down list.
 - Src = Dst:** If selected, the source IP address is also used for the destination IP address.
 - Source Port:** The source port (or source port range) that the rule matches.
 - Destination Port:** The destination port (or destination port range) that the rule matches.
 - Src = Dst:** If selected, the source port is also used for the destination port.
 - IP Protocol:** The protocol that the rule matches.
 - DSCP:** The DSCP tag in the IP header that the rule matches.
 - Routing Domain:** The routing domain that the rule matches.
 - VLAN ID:** Enter the VLAN ID for the rule. The VLAN ID identifies the traffic to and from the virtual interface. Use VLAN ID as 0 to designate native or untagged traffic.
 - Rebind Flow On Change:** When selected, flows that are otherwise identical in terms of match criteria are treated as separate if their DSCP fields differ.
- Traffic Policy

- **Virtual Path Remote Site:** Select the virtual path for the remote site.
- **Traffic Policy:** Choose one of the following traffic policies as needed.
 - * **Load Balance Paths:** Application traffic for the flow is balanced across multiple paths. Traffic is sent through the best path until that path is used. The remaining packets are sent through the next best path.
 - * **Persistent Paths:** Application traffic remains on the same path until the path is no longer available.
 - * **Duplicate Paths:** Application traffic is duplicated across multiple paths, increasing reliability.
- QoS Settings
 - **Transfer Type:** Choose one of the following transfer types:
 - * **Realtime:** Used for low latency, low bandwidth, time-sensitive traffic. Real-time applications are time-sensitive but don't really need high bandwidth (for example voice over IP). Real-time applications are sensitive to latency and jitter but can tolerate some loss.
 - * **Interactive:** Used for interactive traffic with low to medium latency requirements and low to medium bandwidth requirements. The interaction is typically between a client and a server. The communication might not need high bandwidth but is sensitive to loss and latency.
 - * **Bulk:** Used for high bandwidth traffic and applications that can tolerate high latency. Applications that handle file transfer and need high bandwidth are categorized as a bulk class. These applications involve little human interference and are mostly handled by the systems themselves.
 - **Priority:** Choose a priority for the selected transfer type.
- Internet Traffic Policy
 - Select the **Enable Internet Policy** check box to configure internet traffic policy.
 - **Mode:** The method of transmitting and receiving packets for flows that match the rule. You can choose Override Service or WAN link as needed.
 - **WAN link:** The WAN link to be used by flows matching the rule when Internet Load Balancing is enabled.
 - **Override Service:** The destination service for flows matching the rule.

[Verify Config](#)[QoS Policies](#)

Global Rules : IP Protocol

IP Protocol Match Criteria

Source Network

☐ Use IP Group

Destination Network

☐ Use IP Group

☐ Src = Dest

Any

Any

Source Port

Destination Port

☐ Src = Dest

Any

Any

IP Protocol

DSCP

Any

Any

Routing Domain

Vlan Id

☐ Rebind Flow On Change

Any

Traffic Policy

Virtual Path Remote Site

Traffic Policy

Any (determined by routing)

Load Balance Paths

QoS Settings

QoS Class

Transfer Type *

Priority *

Interactive

Medium

Note: Bandwidth share available per QoS class per overlay virtual path is determined by [QoS Profiles](#).
Intelligent default values are auto-picked, with ability to override the defaults via custom QoS profiles

Internet Traffic Policy

☒ Enable Internet Policy

Internet Traffic Settings

Mode *

Override Service *

Override Service

Discard

⚙️ Advanced Settings

Cancel

Save

Click **Save** to save the configuration settings. Click **Verify Config** to validate any audit error.

QoS profiles

The Quality of Service (QoS) section helps to create the QoS profile by using the **+ QoS Profile** option. The QoS profile provides improved service to certain traffic. The goal of QoS is to provide priority including traffic type (Real-time, Interactive, and Bulk classes) and dedicated bandwidth. The band-

© 1999-2021 Citrix Systems, Inc. All rights reserved.

90

width breakups are available in % values. This also improved loss characteristics.


[Verify Config](#)
[QoS Profiles](#)

Default Global QoS Profile (Applicable to all Virtual Paths)

Default QoS Profile	Sites Count
<div>Standard</div> <div>Create New Default Profile</div>	0 / 0

Site Specific Overrides (Applicable to ""Site - Control Node"" Virtual Paths)

[+ QoS Profile](#)

QoS Profile	Sites Count	Actions
Standard-HDX-Multistream	0 / 0	Add/Remove

Click **Verify Config** to validate any audit error.

HDX QoE

April 22, 2021

Network parameters such as latency, jitter, and packet drop affect the user experience of HDX users. Quality of Experience (QoE) helps the users to understand and check their ICA quality of experience. QoE is a calculated index, which indicates the ICA traffic performance. The users can tune the rules and policy to improve the QoE.

The QoE is a numeric value between 0–100, the higher the value the better the user experience.

The parameters used to calculate QoE are measured between the two Citrix SD-WAN appliances located at the client and server side and not measured between the client or the server appliances themselves. Latency, jitter, and packet drop are measured at the flow level and it can be different from the statistics at the link level. The end host (client or server) application might never know that there is a packet loss on the WAN. If the retransmit succeeds, the flow level packet loss rate is lower than the link level loss. However, as a result, it might increase latency and jitter a bit.

You can view a graphical representation of the overall quality of HDX applications in the HDX dash-

board on Citrix SD-WAN Orchestrator service. The HDX applications are classified into the following three quality categories:

Quality	QoE Range
Good	71-100
Fair	51-70
Poor	0-50






Depending on the selected UI page, a list of the bottom (least QoE) five sites, five users, five sessions, or all of them are displayed in the HDX dashboard.

A graphical representation of the QoE for different time intervals allows you to monitor the performance of HDX applications at each site.

Configure HDX QoE

To configure HDX QoE:


1. At the network level, navigate to **Configuration > App & DNS Settings > App Quality Config** and click **+ QoE Configuration**. Add the following applications using the QoE profile that you want to use for the calculation of HDX behavior:
 - ICA Real-time (ica_priority_0)
 - ICA Interactive (ica_priority_1)
 - ICA Bulk-Transfer (ica_priority_2)
 - ICA Background (ica_priority_3)
 - Independent Computing Architecture (Citrix)(ICA)

+ QoE Configuration			
Type	Application	QoE Profile	Actions
Application	ICA Realtime	DefaultQOEProfile	
Application	ICA Interactive	DefaultQOEProfile	
Application	ICA Bulk-Transfer	DefaultQOEProfile	
Application	ICA Background	DefaultQOEProfile	
Application	Independent Compu...	DefaultQOEProfile	

These configurations provide the parameters to measure HDX performance used in HDX report through the profile. Configuration of ICA Real-time, ICA Interactive, ICA Bulk-Transfer, ICA Back-

ground are required for HDX Multi-Stream (MSI) connections, Independent Computing Architecture (Citrix) is required for Single Stream (SSI) connections.

2. Navigate to **Configuration > QoS > QoS Profiles**. Select **Standard-HDX-Multistream** as the default QoS Profile and select the **HDX Reporting** check box.

 [Verify Config](#) [QoS Profiles](#)

QOS Profile Name

Name *
Standard-HDX-Multistream

HDX Settings

Profile Mode
HDX Multi Stream

☒ DPI for HDX

☒ Multi-stream QoS for HDX

☒ HDX Reporting

Custom Defined HDX IP-Port Pairs to aid

In each QoS profile, there is a pre-defined bandwidth percentage for each class. They are configurable to adjust the bandwidth assigned to the classes that the HDX traffic is using.

Bandwidth allocation per QoS Class			
Traffic Type	Bandwidth Share		
Realtime	55 %	Realtime Classes: Bandwidth Breakup	
		HDX High	30 %
		High	10 %
		Medium	8 %
		Low	7 %
Interactive	30 %	Interactive Classes: Bandwidth Breakup	
		HDX High	8 %
		HDX Medium	4 %
		HDX Low	2 %
		High	8 %
		Medium	5 %
Bulk	15 % (Best Effort, Not Guaranteed)	Bulk Classes: Bandwidth Breakup (Relative Share)	
		High	9 %
		Medium	4 %
		Low	2 %

3. Ensure that the new QoS Profile is actively used by checking the Site Count indicator.



Verify Config

QoS Profiles

Default Global QoS Profile (Applicable to all Virtual Paths)

Default QoS Profile

Standard-HDX-Multistream

[Create New Default Profile](#)

Sites Count

11 / 11

4. Navigate to **Configuration > QoS > QoS Policies** and set the new QoS Profile with the enabled HDX reporting as the **Global QoS Bandwidth Default Profile**.



Verify Config

QoS Policies

[Global Rules](#)

Site / Group Specific Rules

Global QoS Bandwidth Default Profile :

Standard-HDX-Multistream

[QoS Bandwidth Profiles](#)(Standard-HDX-Multistream profile recommended for multi-stream HDX users)

Custom Application Rules

Application Rules

HDX Rules (preview)

5. Add HDX rules. These configurations assign proper QoS settings to HDX connections. To check the detail of any rules, click the line of the rule. To change the setting of any default rule, click the “Clone” icon and make required modification.

HDX Rules (preview)

Global QoS Bandwidth Default Profile :

Standard-HDX-Multistream

[QoS Bandwidth Profiles](#)(Standard-HDX-Multistream profile recommended for multi-stream HDX users)[+ HDX Rule](#)
☒ Top of List
 ☐ Bottom of List
 ☐ Specify Row Number

Row number

No	Application	Virtual Path	Traffic Policy	QoS Setting	Actions
1	ICA Realtime(ica_priorit...	Any	Duplicate Paths	High : HDX Realtime	
2	ICA Interactive(ica_prio...	Any	Load Balance Paths	High : HDX Interactive	
3	ICA Bulk-Transfer(ica_p...	Any	Load Balance Paths	Medium : HDX Interactive	
4	ICA Background(ica_pri...	Any	Load Balance Paths	Low : HDX Interactive	
5	Independent Computin...	Any	Load Balance Paths	Medium : Interactive	

These configurations can be modified:

- QoS class: Real-time, Interactive, Bulk
- Traffic policy:
 - Duplicate Paths: The traffic will be duplicated across multiple paths to increase reliability.
 - Persistent Path: The traffic of a flow will remain on the same path, unless the path becomes unavailable.
 - Load Balance Paths: The traffic of a flow is balanced across multiple paths.
 - Advanced Settings: Set policies retransmission, RED, and late packets.

Global Rules : Citrix HDX

Citrix HDX Match Criteria

Application *	Routing Domain
ICA Realtime(ica_priority_0)	Any
Source Network	Destination Network
Any	Any
<input type="checkbox"/> Src = Dest	
Source Port	Destination Port
Any	Any
<input type="checkbox"/> Src = Dest	

Virtual Path Traffic Policy

☒ Enable Virtual Path Traffic Policy

Virtual Path Remote Site	Traffic Policy
Any (determined by routing)	Duplicate Paths

QoS Settings

QoS Class

Transfer Type *	Priority *
HDX Realtime	High
<p>QoS class per overlay virtual path is determined by QoS Profiles, with ability to override the defaults via custom QoS profiles</p>	

- Realtime
- Interactive
- Bulk
- HDX Realtime
- HDX Interactive

HDX dashboard and reports

Citrix SD-WAN Orchestrator service provides the HDX dashboard for up-to-date, detailed measurements of Citrix Virtual Applications and Desktops user experience across the network, for each site, user, and session.

There are two types of HDX sessions – single-stream and multi-stream. A single-stream session has only one connection in the session, whereas a multi-stream session has four. Multi-stream sessions allow for more advanced QoS. The connection in a single-stream HDX session defaults to interactive class, while the top priority connection of a multi-stream HDX session defaults to real-time class and the other three to interactive class. This is configurable.

The Quality of Experience (QoE) score is a numeric value between 0–100. The higher the value the better the user experience. Real-time class traffic QoE is calculated based on jitter, latency, and loss rate. The interactive class QoE is calculated based on burst rate and loss rate. The QoE of a session is the average across all the connections in the session. The QoE of a user is the average of all the sessions launched by that user. The QoE of a site is the average of all the sessions on that site.

All the statistics are metrics:

- For HDX traffic on that site
- Experienced by that user
- Of all the connections in that session

They do not include the metrics of other types of traffic. The metrics are either the average across the selected period, or the total across the selected period.

Note

HDX reporting requires minimum software versions:

- Citrix Virtual Apps and Desktops 7–1912 LTSR (or Current Release)
- Citrix Workspace app for Windows 19.12 LTSR (or Current Release)
- SD-WAN 11.2.0 (or current version)

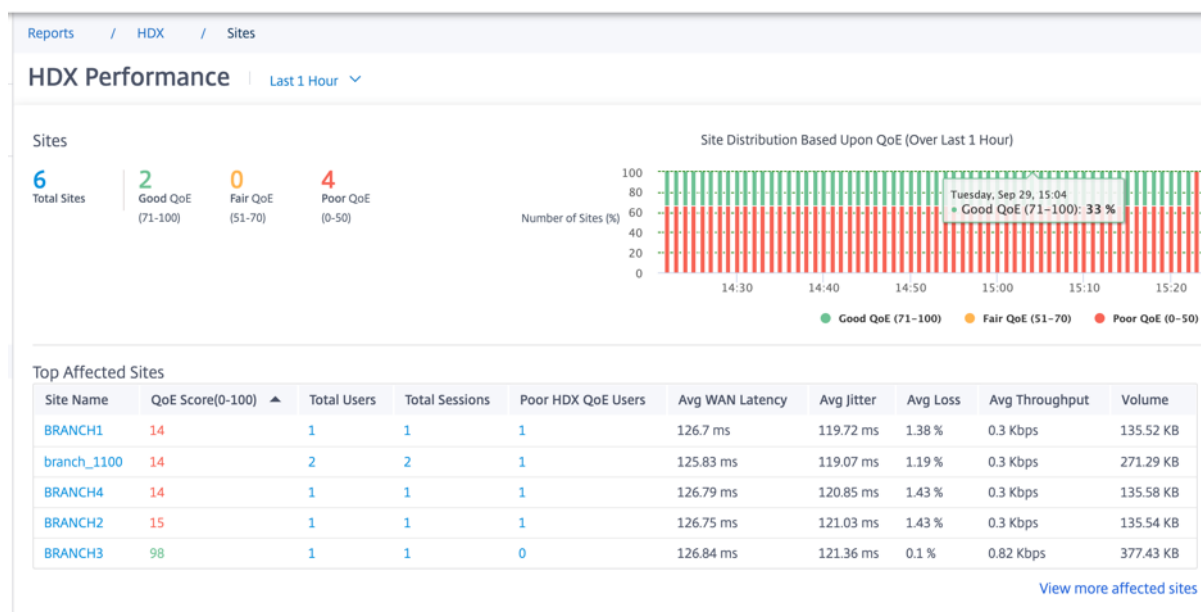
Citrix always recommends using the latest software version to get the latest bug fixes and enhancements. For instance, SD-WAN requires release 11.2.3 or 11.3.1 to have support for new EDT commands introduced in later versions of Citrix Virtual Apps and Desktops LTSR.

Mac clients and Linux clients do not have full support for multi-stream ICA and HDX reporting through Citrix SD-WAN. For instance, Linux clients support multi-stream, however lack detail such as round-trip time and delay. The [CWA feature matrix](#) provides insight into which Operating Systems support the **Multiport ICA** and **HDX Insight with NSAP VC** features.

Users need to access HDX outside of Citrix Gateway encryption, either through direct access to Store-Front or usage of [Beacon Points](#) or the [Network Location Service](#).

Sites

This HDX report provides detailed HDX data per site. To view the site statistics, navigate to **Report > HDX > Sites**.



The dashboard reports on site with HDX traffic running during the selected time interval (for example, last 5 minutes, last 30 minutes, last 1 day, last 1 month, and so on). Site performance is categorized as good (71-100), fair (51-70), or poor (0-50) based on the QoE of the site's HDX traffic. The QoE value in the summary section and the **Top Affected Sites** table is the average value across the selected period.

of time. The time series graphic report shows detailed history with time lapse. Each bar shows the percentage of good, fair, and poor QoE sites at that time.

You can also view the number of sites in percentage, having Good, Fair, and Poor QoE at that time under the **Site Distribution Based Upon QoE** graph. Hover your mouse to the color bar to see the percentage number of sites in a good/fair/poor state.

NOTE

- The statistics are collected in one direction, from the remote side into the current site. For example, for a session between site-A and site-B, the report of site-A is collected on traffic coming from site-B into site-A, whereas the report of site-B is collected on traffic coming from site-A into site-B. Therefore, the statistics of the same session on site-A and site-B can be different.
- The **Top Affected Sites** table reflects only the top 5 most affected sites. By default, it shows the 5 sites with the lowest QoE scores. But each column is sortable, ascending, or descending, and used as a query criterion. For example, clicking the **Avg Jitter** column title toggles showing either the 5 sites with the lowest average jitter or the highest average jitter. Same for other columns. To see the details of all the sites with HDX traffic during the selected period of time, click **View more affected sites**.

The following are the details of each site:

- **Site Name:** The site name.
- **QoE Score (0-100):** The average QoE score of this site.
- **Total Users:** The total number of active HDX users seen on the site during the selected period.
- **Total Sessions:** The total number of HDX sessions seen on the site during the selected period, including both single-stream and multi-stream sessions.
- **Poor HDX QoE Users:** The number of HDX users suffering from poor QoE (below 50).
- **Avg WAN Latency:** Average latency over the WAN, from the remote site to this site.
- **Avg Jitter:** The average jitter value for the selected duration.
- **Avg Loss:** The average packet loss percentage value for the selected duration.
- **Avg Throughput:** The average data throughput value for the selected duration.
- **Volume:** The total traffic volume seen on this site. The SD-WAN Orchestrator for On-premises GUI might adjust and change the unit based on the number value.

Clicking any column title shows the report sorted on that column. Click **View more affected sites** to see the reports of all sites. Clicking any single row shows the detailed report for that site.

The table in the following screenshot is an example report showing all the sites. It has the same columns as the **Top Affected Sites** table. You can search for any site using the search bar.

Reports / HDX / Sites / Details

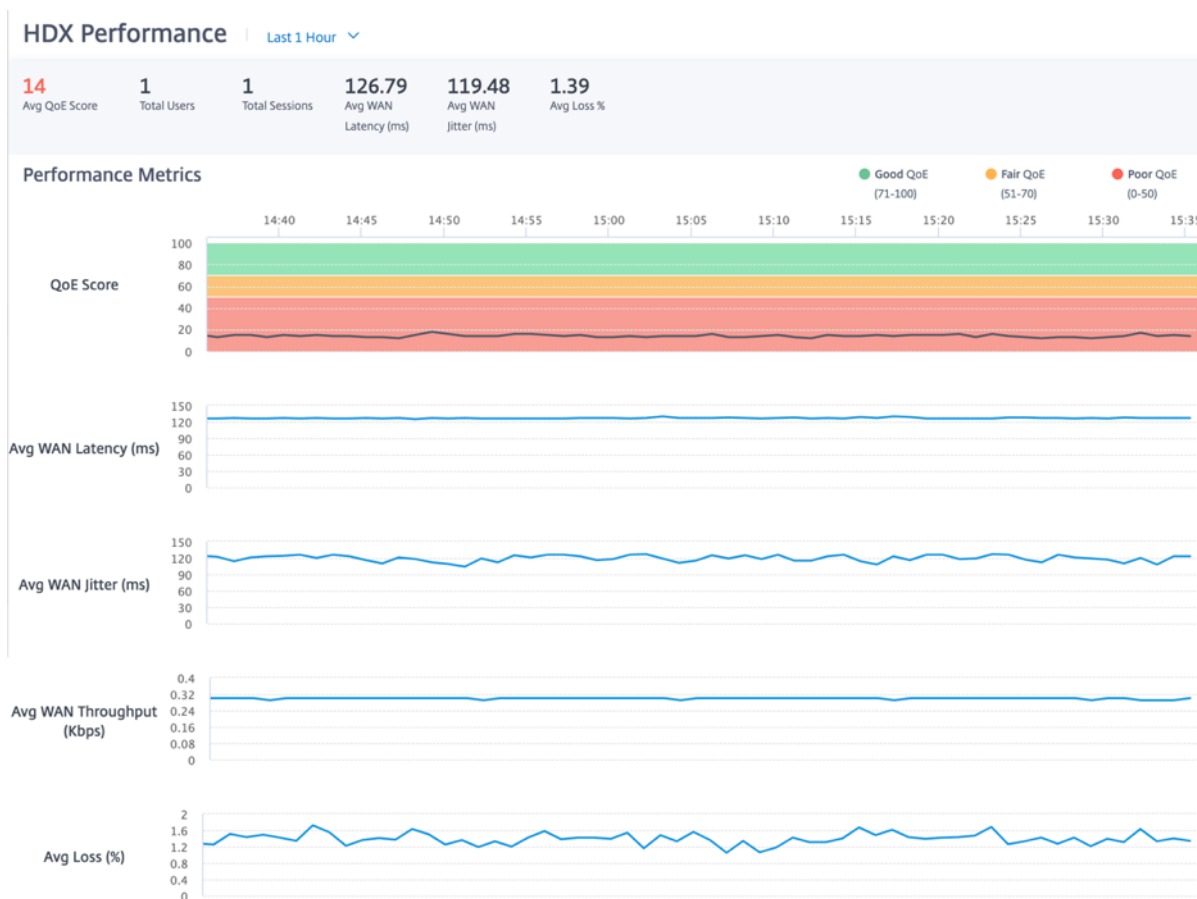
HDX Performance

Last 1 Hour

Search

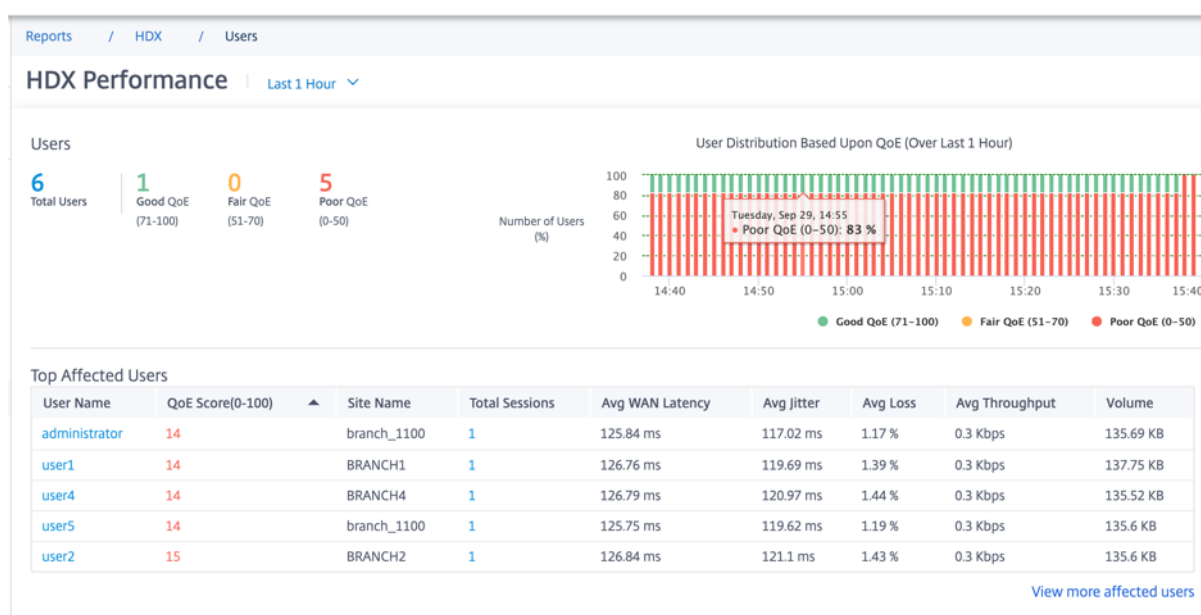
Site Name	QoE Score(0-100) ▲	Total Users	Total Sessions	Poor HDX QoE Users	Avg WAN Latency	Avg Jitter	Avg Loss	Avg Throughput	Volume
BRANCH1	14	1	1	1	126.78 ms	119.42 ms	1.39 %	0.3 Kbps	133.3 KB
branch_1100	14	2	2	1	125.81 ms	118.4 ms	1.18 %	0.3 Kbps	271.29 KB
BRANCH4	14	1	1	1	126.72 ms	120.67 ms	1.44 %	0.3 Kbps	135.52 KB
BRANCH2	15	1	1	1	126.82 ms	121.08 ms	1.44 %	0.3 Kbps	135.54 KB
BRANCH3	98	1	1	0	126.93 ms	121.16 ms	0.1 %	0.82 Kbps	377.38 KB
MCNVPX111	99	6	6	0	125.89 ms	120.7 ms	0 %	568.98 Kbps	1.56 GB

Click the individual site row to view a graphical representation of the performance metrics. Hovering the mouse over the graphic provides more details.



Users

To view the HDX Users report, navigate to **Reports > HDX > Users**.



The user report shows the performance experienced by each user during the selected period (for example, last 5 minutes, last 30 minutes, last 1 day, last 1 month, and so on). If the user has been on multiple sites during the selected period, the last site the user logged in from is shown in the report. User experience is categorized as good (71-100), fair (51-70), or poor (0-50) based on the QoE score of their HDX traffic. The QoE values in the summary section and the **Top Affected Users** table are the average values across the selected period of time. The time series graphic report shows detailed history with time lapse. Each bar shows the percentage of users with good, fair, and poor QoE at that time.

You can also view the number of users in percentage, having Good, Fair, and Poor QoE at that time under the **User Distribution Based Upon QoE** graph. Hover your mouse to the color bar to see the percentage number of users in good/fair/poor state.

Personally Identifiable Information

Currently, the HDX QoE reports have the following two Personally Identifiable Information (PII) fields:

- **User Name:** Displays the user name.
- **IP Address:** Displays the client IP address.

NOTE

- When the user name is not available, the IP address is displayed in the **User Name** field.
- The HDX user reports are based on statistics from the client side SD-WAN, not the Virtual Delivery Agent (VDA) side SD-WAN. This reflects the end user's HDX experience.
- The **Top Affected Users** table reflects only the top 5 most affected users. By default, it shows the top 5 users with the lowest QoE. But each column is sortable, ascending, or de-

scending, and used as a query criterion. For example, clicking the **Avg Jitter** column title toggles displaying either the 5 users with the lowest average jitter or the highest average jitter. To see the details of all the users that have HDX traffic during the selected period of time, click **View more affected users**.

The following are the details of each user:

- **User Name:** The user name.
- **QoE Score (0-100):** The average QoE score of this user.
- **Site Name:** The site name that the user logged in from.
- **Total Sessions:** The total number of active HDX sessions from that user, including both single-stream and multi-stream sessions.
- **Avg WAN Latency:** Average latency over the WAN, experienced at the client side.
- **Avg Jitter:** The average jitter value for the selected duration.
- **Avg Loss:** The average packet loss percentage value for the selected duration.
- **Avg Throughput:** The average data throughput value for the selected duration.
- **Volume:** The total traffic volume used by this user. The SD-WAN Orchestrator for On-premises GUI might adjust and change the unit based on the number value.

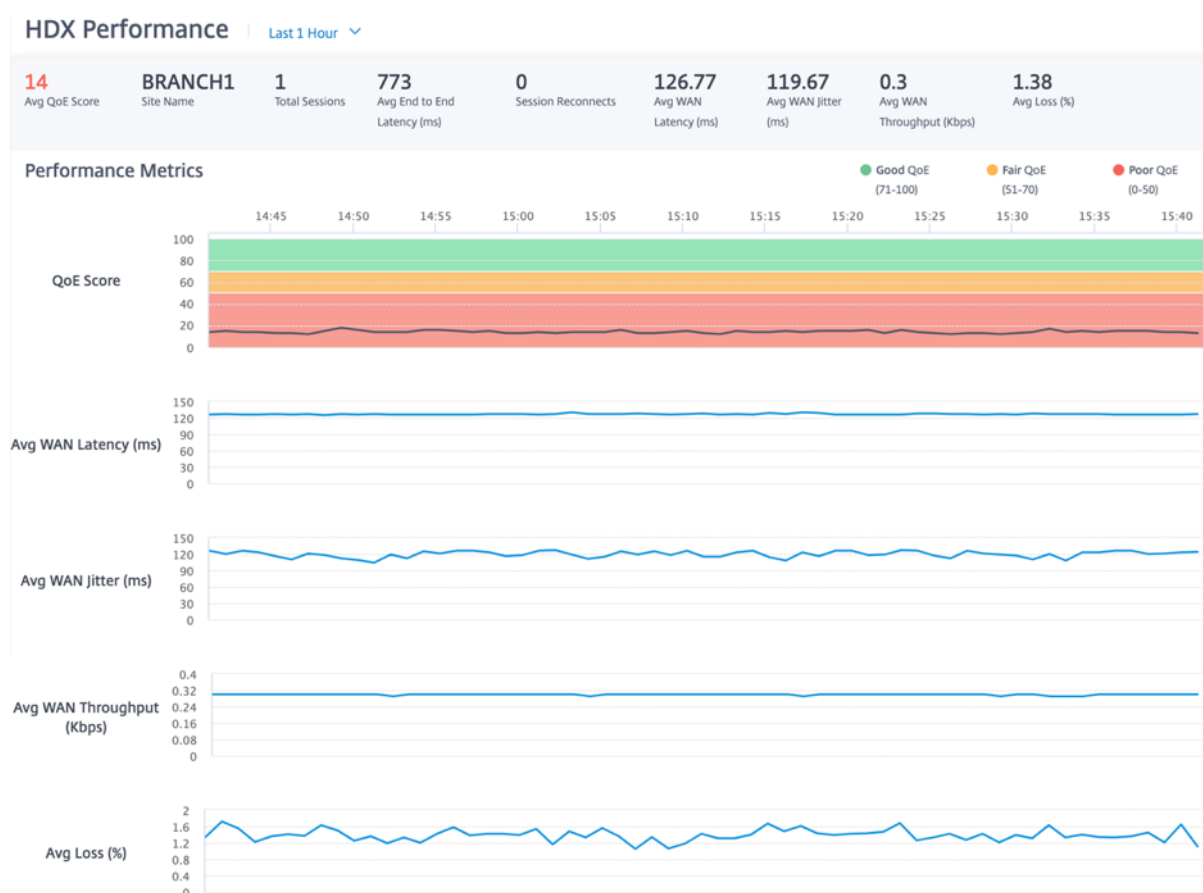
Clicking any column title shows the report sorted on that column. Click **View more affected users** to see the reports of all users. Clicking any single row shows the detailed report for that user.

The following screenshot is an example report table showing all the users. It has the same columns as the **Top Affected Users** table. You can search for any site using the search bar.

HDX Performance | Last 1 Hour ▾

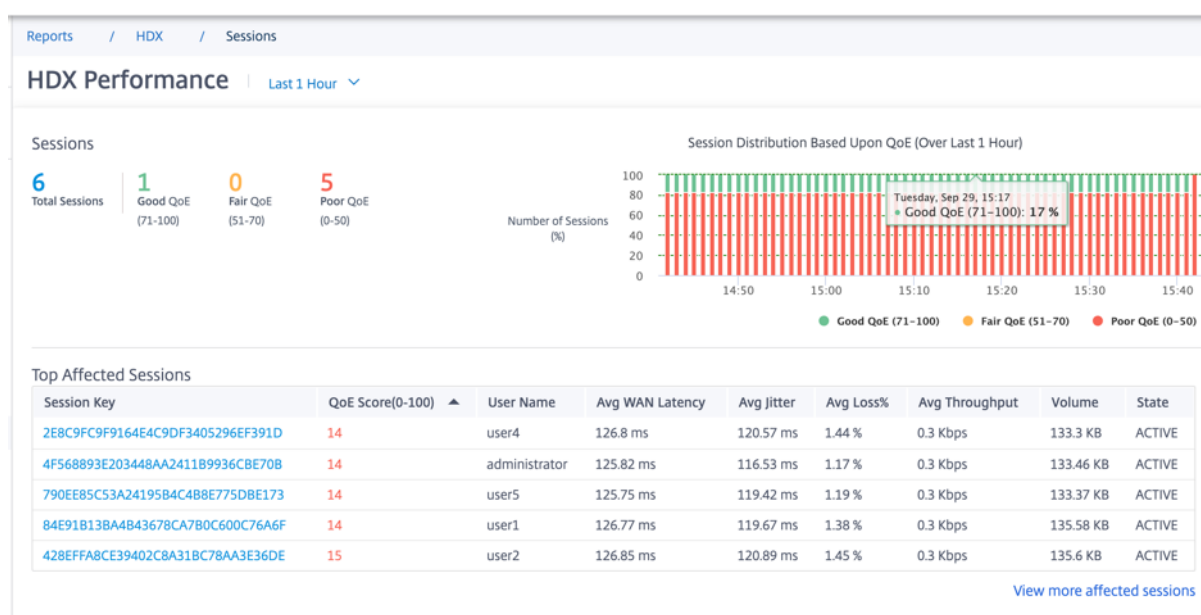
User Name	QoE Score(0-100)	▲	Site Name	Total Sessions	Avg WAN Latency	Avg Jitter	Avg Loss	Avg Throughput	Volume
administrator	14		branch_1100	1	125.84 ms	116.82 ms	1.17 %	0.3 Kbps	135.69 KB
user1	14		BRANCH1	1	126.77 ms	119.67 ms	1.39 %	0.3 Kbps	135.58 KB
user4	14		BRANCH4	1	126.8 ms	120.93 ms	1.44 %	0.3 Kbps	135.52 KB
user5	14		branch_1100	1	125.77 ms	119.56 ms	1.19 %	0.3 Kbps	135.6 KB
user2	15		BRANCH2	1	126.82 ms	121.03 ms	1.44 %	0.3 Kbps	135.6 KB
user3	98		BRANCH3	1	126.89 ms	120.85 ms	0.1 %	0.83 Kbps	377.48 KB

Click an individual user row to see a graphical representation of that user's performance metrics.



Sessions

The Session report provides details at the session level. To view the session report, navigate to **Reports > HDX > Sessions**.



The dashboard shows the reports of HDX sessions running during the selected period (for example, last 5 minutes, last 30 minutes, last 1 day, last 1 month, and so on). Sessions are categorized as good (71-100), fair (51-70), or poor (0-50) based on the QoE of that session. The QoE value in the summary section and the Top Affected table is the average value across the selected period. The time series graphic report shows detailed history with time lapse. Each bar shows the percentage of good, fair, and poor QoE sessions at that time.

You can also view the number of sessions in percentage, having Good, Fair, and Poor QoE at that time under the **Session Distribution Based Upon QoE** graph. Hover your mouse to the color bar to see the percentage number of sessions in good/fair/poor state.

Note

- The HDX session reports are based on statistics from the client side SD-WAN, not the VDA side SD-WAN. This reflects the end user's HDX experience.
- The **Top Affected Sessions** table reflects only the top 5 most affected sessions. By default, it shows the top 5 sessions with the lowest QoE. But each column is sortable, ascending, or descending, and used as a query criterion. For example, clicking the **Avg Jitter** column title toggles showing either the 5 sessions with the lowest average jitter or the highest average jitter. To see the details of all the HDX sessions during the selected period of time, click **View more affected sessions**.

The following are the Detail of the top each session:

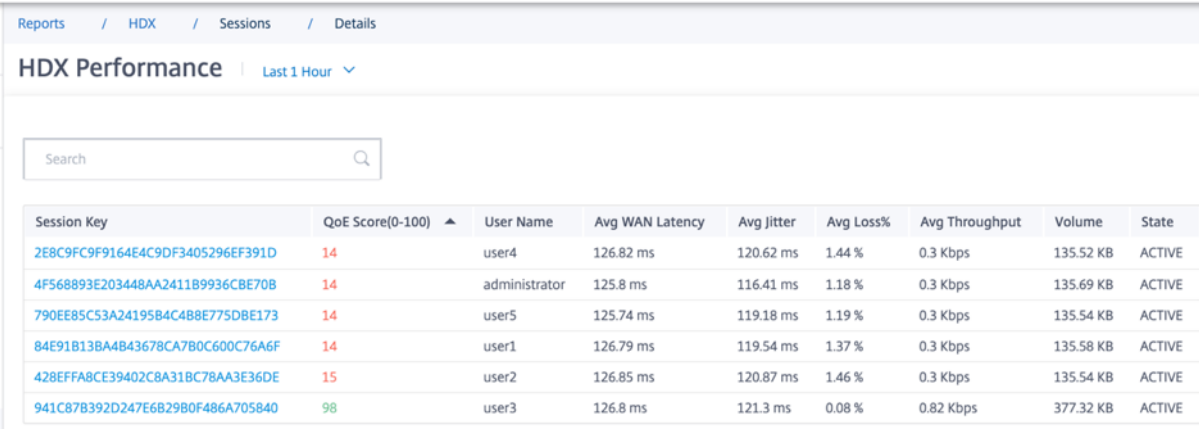
- Session Key:** The unique identity for an HDX session.
- QoE Score (0-100):** The average QoE of this session.
- User Name:** The user name.
- Avg WAN Latency:** The average WAN latency of the session for the selected duration, measured

at the client side.

- **Avg Jitter:** The average jitter value of the session for the selected duration.
- **Avg Loss:** The average loss percentage value of the session for the selected duration.
- **Avg Throughput:** The average throughput value of the session for the selected duration.
- **Volume:** The total traffic volume used by this session. The SD-WAN Orchestrator for On-premises GUI might adjust and change the unit based on the number value.

Clicking any column title, shows the report sorted on that column. Clicking on **View more affected sessions** to see the reports of all the sessions. Clicking any single row shows the detailed report on that session.

The following screenshot is an example report table showing all the sessions. It has the same columns as the **Top Affected Sessions** table.



Reports / HDX / Sessions / Details

HDX Performance | Last 1 Hour

Search

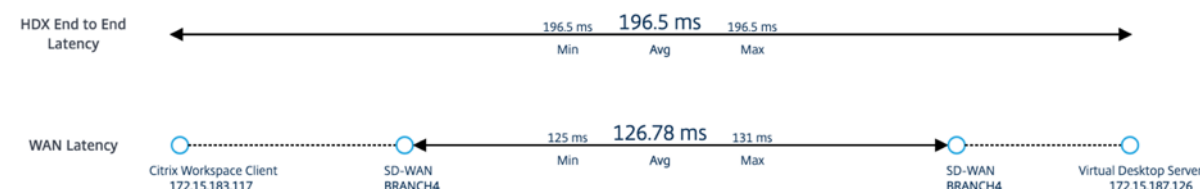
Session Key	QoE Score(0-100)	User Name	Avg WAN Latency	Avg Jitter	Avg Loss%	Avg Throughput	Volume	State
2E8C9FC9F9164E4C9DF3405296EF391D	14	user4	126.82 ms	120.62 ms	1.44 %	0.3 Kbps	135.52 KB	ACTIVE
4F568893E203448AA2411B9936CBE70B	14	administrator	125.8 ms	116.41 ms	1.18 %	0.3 Kbps	135.69 KB	ACTIVE
790EE85C53A24195B4C4B8E775DBE173	14	user5	125.74 ms	119.18 ms	1.19 %	0.3 Kbps	135.54 KB	ACTIVE
84E91B13BA4B43678CA7B0C600C76A6F	14	user1	126.79 ms	119.54 ms	1.37 %	0.3 Kbps	135.58 KB	ACTIVE
428EFA8CE39402C8A31BC78AA3E36DE	15	user2	126.85 ms	120.87 ms	1.46 %	0.3 Kbps	135.54 KB	ACTIVE
941C87B392D247E6B29B0F486A705840	98	user3	126.8 ms	121.3 ms	0.08 %	0.82 Kbps	377.32 KB	ACTIVE

Click the individual session key to view a graphical representation of the performance metrics along with the details about all the variables affecting QoE.

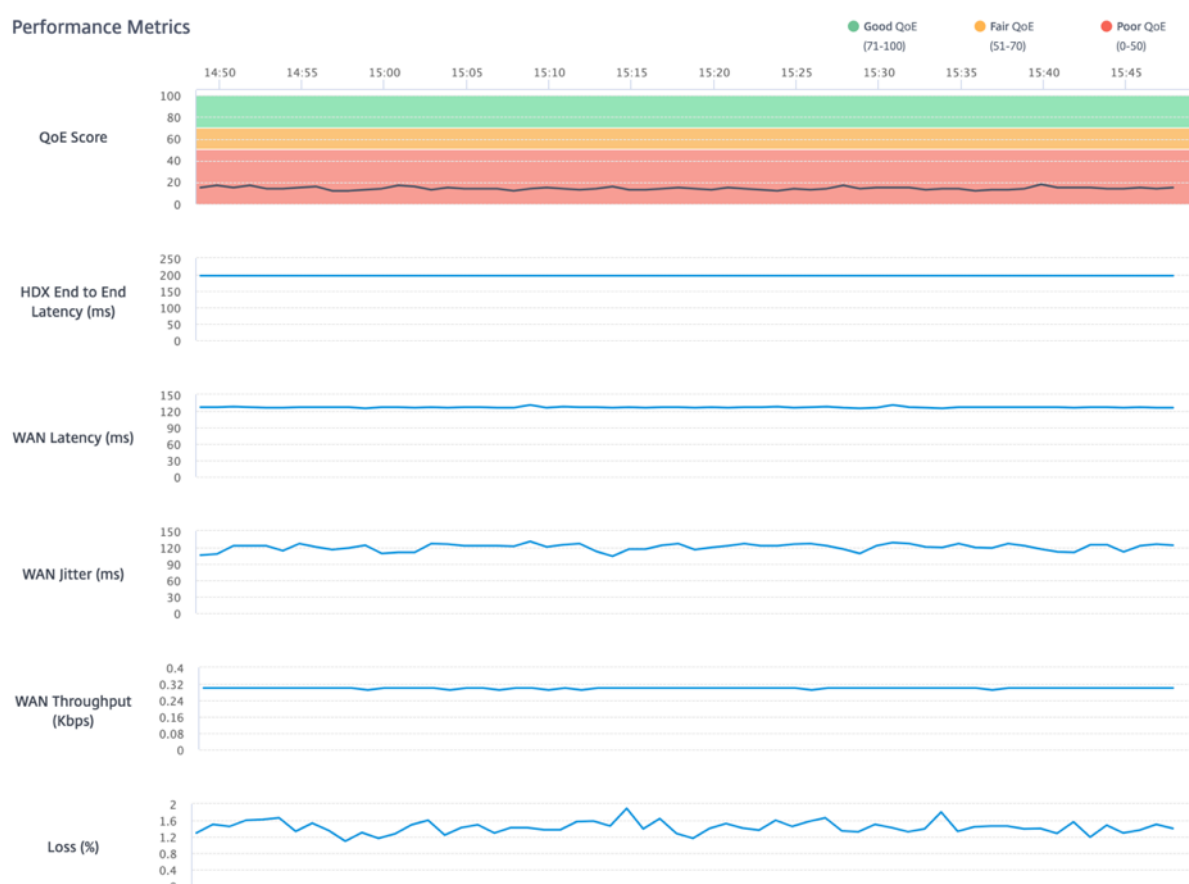
HDX Performance | Last 1 Hour ▾

Avg QoE Score	14 /100	User Name	user4	VDA Name	WIN-AV44DDIH8JC
Session Duration	60 (minutes)	Site Name	BRANCH4	VD/VA	Virtual App
Session State	ACTIVE	Session Type	Multi-Stream	WAN Optimized	No
Session Reconnects	0			Network Service	MCNVPX111-BRANCH4

Latency Distribution



Performance Metrics



- **Avg QoE Score:** The average QoE over the selected period.
- **User Name:** The user who launched this session.
- **VDA Name:** Name of the VDA from which published Desktop/Application are delivered.
- **Session Duration:** The active time of this session in the selected period.
- **Site Name:** The client site of the user when the session was launched.
- **VD/VA:** Whether this session is a **Virtual Desktop** or a **Virtual Application** session.
- **Session State:** The state of the session at the end of the selected period.
- **Session Type:** Whether the session is Multi-stream session or single-stream session the last

time the session is launched.

- **WAN Optimized:** Whether this session was WAN optimized. If the SD-WAN is PE platform, WAN Optimization is enabled for HDX, and this session is optimized, then this field shows true.
- **Session Reconnects:** If the session has been disconnect and reconnect automatically due to network issue, this field is the count of such occurrence.
- **Network Service:** This is the service name through which this session is delivered.
- **HDX End to End Latency:** Half of the value of round trip time between the VDA and the client.
- **WAN Latency:** The latency from the VDA side SD-WAN to the client side SD-WAN.

Security

January 27, 2021


You can configure the security settings such as, network encryption, virtual path IPsec, firewall, and certificates that are applicable to all the appliances across the network.

Firewall zones



You can configure zones in the network and define policies to control how traffic enters and leaves the zones. The following zones are available by default:

- **Default_LAN_Zone:** Applies to traffic to or from an object with a configurable zone, where the zone has not been set.
- **Internet_Zone:** Applies to traffic to or from an Internet service using a trusted interface.
- **Untrusted_Internet_Zone:** Applies to traffic to or from an Internet service using an untrusted interface.

Network Configuration : Firewall Zones

 [Verify Config](#) [Firewall Zones](#)

+ Firewall Zone

Name	Actions
Default_LAN_Zone	
Internet_Zone	
Untrusted_Internet_Zone	
	
	

You can also create your own zones and assign them to the following types of objects:

- Virtual Network Interfaces
- Intranet Services
- GRE Tunnels
- LAN IPsec Tunnels

Click **Verify Config** to validate any audit error.

Firewall defaults

You can configure the global default firewall actions and global firewall settings that can be applied to all the appliances in the SD-WAN network. The settings can also be defined at the site level which overrides the global setting.

Global Default Firewall Actions

Action When No Firewall Rules Match

Allow

Action When Security Profiles Cannot be Inspected

Ignore

Global Firewall Settings

☐ Default Connection State Tracking

Denied Timeout (s)

30

TCP Initial Timeout (s)	TCP Idle Timeout (s)	
120	7440	
TCP Closing Timeout	TCP Time Wait Timeout (s)	TCP closed Timeout (s)
60	120	10
UDP Initial Timeout (s)	UDP Idle Timeout (s)	
30	300	
ICMP Initial Timeout (s)	ICMP Idle Timeout (s)	
30	60	
Generic Initial Timeout (s)	Generic Idle Timeout (s)	
30	300	

Save

- **Action When No Firewall Rules Match:** Select an action (Allow or Drop) from the list for the packets that do not match a Firewall policy.
- **Action When Security Profiles Cannot be Inspected:** Select an action (Ignore or Drop) for the packets that match a firewall rule and engage a security profile but temporarily cannot be inspected by the Edge Security subsystem. If you select **Ignore**, then the relevant firewall rule is treated as not matched and the next firewall rule in order is evaluated. If you select **Drop**, the packets matching the relevant firewall rule, are dropped.
- **Default Firewall Action:** Select an action (Allow/Drop) from the list for packets that do not match a policy.
- **Default Connection State Tracking:** Enables directional connection state tracking for TCP, UDP, and ICMP flows that do not match a filter policy or NAT rule.

Note

Asymmetric flows are blocked when **Default Connection State Tracking** is enabled even when there are no Firewall policies defined. If there is the possibility of asymmetric flows at a site, the recommendation is to enable it at a site or policy level and not globally.

- **Denied Timeout (s):** Time (in seconds) to wait for new packets before closing denied connections.
- **TCP Initial Timeout (s):** Time (in seconds) to wait for new packets before closing an incomplete TCP session.
- **TCP Idle Timeout (s):** Time (in seconds) to wait for new packets before closing an active TCP session.
- **TCP Closing Timeout:** Time (in seconds) to wait for new packets before closing a TCP session after a terminate request.
- **TCP Time Wait Timeouts (s):** Time (in seconds) to wait for new packets before closing a terminated TCP session.
- **TCP Closed Timeout (s):** Time (in seconds) to wait for new packets before closing an aborted TCP session.
- **UDP Initial Timeout (s):** Time (in seconds) to wait for new packets before closing the UDP session that has not seen traffic in both directions.
- **UDP Idle Timeout (s):** Time (in seconds) to wait for new packets before closing an active UDP session.
- **ICMP Initial Timeout (s):** Time (in seconds) to wait for new packets before closing an ICMP session that has not seen traffic in both directions
- **ICMP Idle Timeout (s):** Time (in seconds) to wait for new packets before closing an active ICMP session.
- **Generic Initial Timeout (s):** Time (in seconds) to wait for new packets before closing a generic session that has not seen traffic in both directions.
- **Generic Idle Timeout (s):** Time (in seconds) to wait for new packets before closing an active generic session.

Click **Verify Config** to validate any audit error.

Firewall policies

Firewall profiles provide security by ensuring that network traffic is restricted only to a specific firewall rule depending on the match criteria and by applying specific actions. The **Firewall Policies** contains three sections.

- **Global Default** – Global default policy is an aggregation of a couple of firewall rules. The policy that you create under the **Global Default** section is applied across all the sites in the network.
- **Site Specific** – You can apply the defined firewall rules on certain specific sites.
- **Global Override** – You can override both global and site-specific policies using **Global Override Policy**.

Firewall Policies

[Global Default](#) [Site Specific](#) [Global Override](#)

+ Global Default Policy

No	Name	Active	Actions
----	------	--------	---------

You can define firewall rules and place it based on the priority. You can choose the priority order to begin from the top of the list, bottom of the list, or from a specific row.

It is recommended to have more specific rules for applications or subapplications at the top, followed by less specific rules for the ones representing broader traffic.

Firewall Policies

Policy Information

Policy Name *

☐ Active Policy

Firewall Rules

Create New Rule

☒ Top of List ☐ Bottom of List ☐ Specify Row Number

Row number

No	Match Type	Application	Src Zone	Dst Zone	Src Network	Dst Network	Action	Actions
----	------------	-------------	----------	----------	-------------	-------------	--------	---------

Cancel

Save

To create a firewall rule, click **Create New Rule**.

Firewall Policies

Profile Information

Profile Name *

☐ Active Policy

Match Criteria

Match Type

Application *

Routing Domain

Filtering Criteria

Source Zone

Destination Zone

Source Service Type

Source Service Name *

Source IP

Source Port

Dest Service Type

Dest Service Name *

Dest IP

Dest Port

IP Protocol

DSCP

☒ Allow Fragments

☐ Reverse Also

☐ Match Established

Actions

Action

☒ Connection State Tracking

☒ Log Connection Start & End Events

☒ Log Packet Statistics

Cancel

Done

- Provide a policy name and select the **Active Policy** check box if you want to apply all the firewall rules.
- The match criteria defines the traffic for the rule such as, an application, a custom defined application, group of applications, application family, or IP protocol based.
- Filtering criteria:
 - **Source Zone:** The source firewall zone.
 - **Destination Zone:** The destination firewall zone.
 - **Source Service Type:** The source SD-WAN service type – Local, Virtual Path, Intranet, IP Host, or Internet are examples of Service Types.

- **Source Service Name:** The name of a service tied to the service type. For example, if the virtual path is selected for Source Service type, it would be the name of the specific virtual path. This is not always required and depends on the service type selected.
- **Source IP:** The IP address and subnet mask the rule uses to match.
- **Source Port:** The source port the specific application uses.
- **Dest Service Type:** The destination SD-WAN service type – Local, Virtual Path, Intranet, IP Host, or Internet are examples of service types.
- **Dest Service Name:** Name of a service tied to the service type. This is not always required and depends on the service type selected.
- **Dest IP:** The IP address and subnet mask the filter use to match.
- **Dest Port:** The destination port the specific application uses (that is, HTTP destination port 80 for the TCP protocol).
- **IP Protocol:** If this match type is selected, select an IP protocol that the rule matches with. Options include ANY, TCP, UDP ICMP and so on.
- **DSCP:** Allow the user to match on a DSCP tag setting.
- **Allow Fragments:** Allow IP fragments that match this rule.
- **Reverse Also:** Automatically add a copy of this filter policy with source and destination settings reversed.
- **Match Established:** Match incoming packets for a connection to which outgoing packets were allowed.
- The following actions can be performed on a matched flow:
 - **Allow:** Permit the flow through the Firewall.
 - **Drop:** Deny the flow through the firewall by dropping the packets.
 - **Reject:** Deny the flow through the firewall and send a protocol specific response. TCP sends a reset, ICMP sends an error message.
 - **Count and Continue:** Count the number of packets and bytes for this flow, then continue down the policy list.

Apart from defining the action to be taken, you can also select the logs to be captured.

Network encryption

Select the encryption mechanism to be used across the network. You can configure the global security settings that secure the entire SD-WAN network.

Network Encryption mode defines the algorithm used for all encrypted paths in the SD-WAN network. It is not applicable for non-encrypted paths. You can set the encryption as AES-128 or AES-256.

Network Configuration : Network Encryption

[Verify Config](#) [Network Encryption](#)

Network Encryption Mode

Encryption

AES-128

Save

SSL inspection

Secure Sockets Layer (SSL) inspection is a process of intercepting, decrypting, and scanning the HTTPS and secure SMTP traffic for malicious content. SSL inspection provides security to the traffic flowing to and from your organization. You can generate and upload your organization's root CA certificate and perform the man-in-the-middle inspection of the traffic.

NOTE

SSL inspection is supported from Citrix SD-WAN 11.3.0 release onwards.

To enable SSL inspection, at the network level, navigate to **Configuration > Security > SSL Inspection > Configuration** and define the following SSL configuration settings.

- **Enable SMTPS Traffic Processing:** The secure SMTP traffic undergoes SSL inspection.
- **Enable HTTPS Traffic Processing:** The HTTPS traffic undergoes SSL inspection.
- **Block Invalid HTTPS Traffic:** By default, when the **Block Invalid HTTPS Traffic** check box is cleared, non-HTTPS traffic on port 443 is ignored and allowed to flow unimpeded. When **Block Invalid HTTPS Traffic** is selected, non-HTTPS traffic is blocked for SSL inspection. Note that it can also block the legitimate traffic that is on port 443 and not fully conform to the HTTPS specification.
- **Client Connection Protocols:** Select the required client protocols. The protocols available are SSLvHello, SSLv3, TLSv1, TLSv1.1, TLSv1.2, and TLSv1.3.

- **Server Connection Protocols:** Select the required server protocols. The protocols available are SSLvHello, SSLv3, TLSv1, TLSv1.1, TLSv1.2, and TLSv1.3.

NOTE

The versions older than TLSv1.2 are considered vulnerable and must not be enabled, unless backward compatibility is important.

SSL Inspection

The screenshot shows the 'Configuration' tab of the SSL Inspection settings. It includes three checkboxes for enabling SMTPS, HTTPS, and blocking invalid HTTPS traffic. Below these are sections for 'Client Connection Protocols' and 'Server Connection Protocols', each with checkboxes for SSLvHello, SSLv3, TLSv1, TLSv1.1, TLSv1.2, and TLSv1.3. At the bottom are 'Save' and 'Cancel' buttons.

Configuration Root Certificate Trusted Server Certificates

☐ Enable SMTPS Traffic Processing

☐ Enable HTTPS Traffic Processing

☐ Block Invalid HTTPS Traffic

Client Connection Protocols

☐ SSLvHello ☐ SSLv3 ☐ TLSv1 ☐ TLSv1.1 ☐ TLSv1.2 ☐ TLSv1.3

Server Connection Protocols

☐ SSLvHello ☐ SSLv3 ☐ TLSv1 ☐ TLSv1.1 ☐ TLSv1.2 ☐ TLSv1.3

Save **Cancel**

On the **Root Certificate** tab, copy and paste the root certificate and key of your organization root certificate authority (CA). The root CA is used to create and sign a forged copy of the certificates of the original sites, so that SSL inspection can be performed. It is implicitly assumed that the root CA certificate is installed on all client workstations and devices that can have their traffic SSL inspected.

SSL Inspection

The screenshot shows the 'Root Certificate' tab. It contains a heading 'Root Certificate and Key' and a sub-heading 'Import the files or copy paste the Root Certificate and Key'. Below these are two large text input fields labeled 'Root Certificate' and 'Root Key'. At the bottom are 'Save' and 'Cancel' buttons.

Configuration **Root Certificate** Trusted Server Certificates

Root Certificate and Key

Import the files or copy paste the Root Certificate and Key

Root Certificate

Root Key

Save **Cancel**

The default, **Trust all server certificates signed by root authority and certificates listed below** option results in SD-WAN validating all server certificates against the standard list of root CAs and the root CA previously configured. It also discards servers that have an invalid certificate. To override this behavior, upload the SSL self-signed certificate of internal servers on the **Trusted Server Certificates** tab. Click **Add Certificate** and provide a name, browse for the certificate, and upload it. Alternately, if you select **Trust all server certificates**, all the servers are considered as trusted by Citrix SD-WAN, regardless of their certificate validation status.

SSL Inspection

Configuration Root Certificate Trusted Server Certificates

Trusted Server Certificates

☐ Trust all server certificates

☒ Trust all server certificates signed by root authority and certificates listed below

Add Certificate

Certificate Name	Issued to	Issued by	Valid date	Expire date
------------------	-----------	-----------	------------	-------------

As part of security profiles, you can create SSL rules and enable them for SSL inspection. For more information on creating SSL rules for a security profile, see [Edge security](#).

Intrusion prevention

Intrusion Prevention System (IPS) detects and prevents malicious activity from entering your network. IPS inspects the network traffic and takes automated actions on all incoming traffic flows. It includes a database of over 34,000 signature detections and heuristic signatures for port scans, allowing you to effectively monitor and block most suspicious requests.

IPS uses signature based detection, which matches the incoming packets against a database of uniquely identifiable exploit and attack patterns. The signature database is automatically updated daily. Since there are thousands of signatures, the signatures are grouped into Category and Class types.

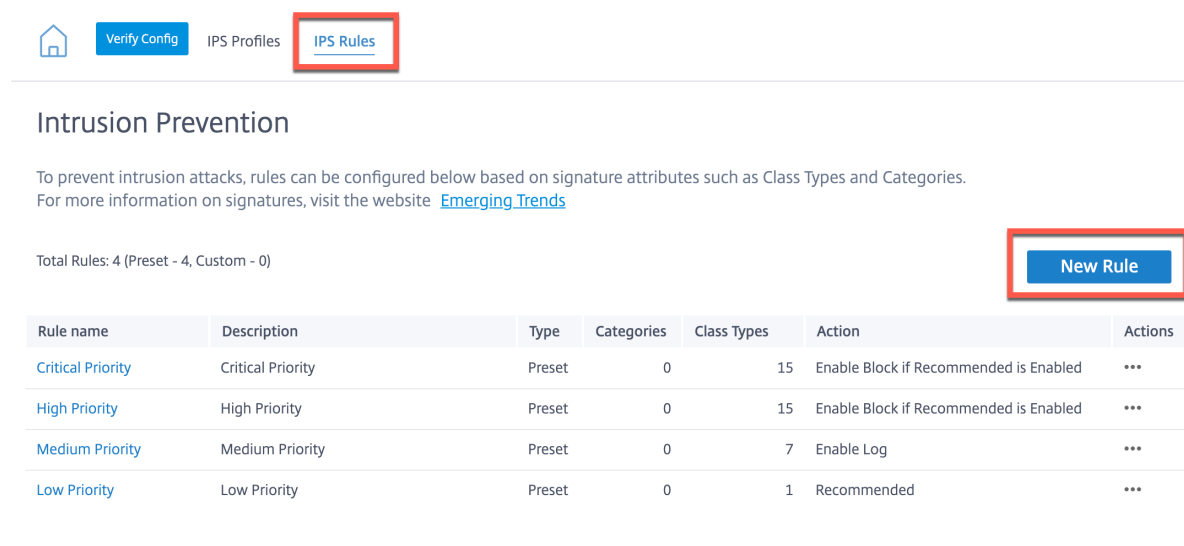
You can create IPS rules and enable only the signature categories or class types that your network requires. Since intrusion prevention is a compute sensitive process, use only the minimal set of signature categories or class types that are relevant for your network.

You can create an IPS profile and enable a combination of IPS rules. These IPS profiles can then be associated globally with the entire network or with only specific sites.

Each rule can be associated with multiple IPS profiles and each IPS profile can be associated with multiple sites. When an IPS profile is enabled, it inspects the network traffic for the sites with which

the IPS profile is associated and for the IPS rules enabled within that profile.

To create IPS rules, at the network level, navigate to **Configuration > Security > Intrusion Prevention > IPS Rules** and click **New Rule**.



Intrusion Prevention

To prevent intrusion attacks, rules can be configured below based on signature attributes such as Class Types and Categories. For more information on signatures, visit the website [Emerging Trends](#)

Total Rules: 4 (Preset - 4, Custom - 0)

Rule name	Description	Type	Categories	Class Types	Action	Actions
Critical Priority	Critical Priority	Preset	0	15	Enable Block if Recommended is Enabled	...
High Priority	High Priority	Preset	0	15	Enable Block if Recommended is Enabled	...
Medium Priority	Medium Priority	Preset	0	7	Enable Log	...
Low Priority	Low Priority	Preset	0	1	Recommended	...

Provide a rule name and description. Select the match category or class type signature attributes, select an action for the rule, and enable it. You can choose from the following rule actions:

Rule Action	Function
Recommended	There are recommended actions defined for each signature. Perform the recommended action for the signatures.
Enable Log	Allow and log the traffic matching any of the signatures in the rule.
Enable Block if Recommended is Enabled	If the rule action is Recommended and the signature's recommended action is Enable Log , drop the traffic matching any of the signatures in the rule.
Enable Block	Drop the traffic matching any of the signatures in the rule.

[← Rule](#)

Rule Name *

rule-block-chrome-dos

Description

Block denial-of-service attacks through Chrome browser.

IF THE FOLLOWING CONDITION IS MET*

Category

is

browser-chrome

OR

Class Type

is

denial-of-service

THEN DO THE FOLLOWING*

Enable Block

Enabled

Create Rule

Cancel

Note

- Since Intrusion Prevention is a compute sensitive process use only the minimal set of signature categories that are relevant to your edge security deployments.
- The SD-WAN firewall drops the traffic on all WAN L4 ports that are not port-forwarded and are not visible in the IPS engine. This provides an extra security layer against trivial DOS and scan attacks.

To create IPS profiles, at the network level, navigate to **Configuration > Security > Intrusion Prevention > IPS Profiles** and click **New Profile**.

[Home](#)

[Verify Config](#)

[IPS Profiles](#)

IPS Rules

Each IPS Profile contains one or many IPS Rules applied to sites

Total Profiles: 1

New Profile

Profile name	Description	Status	Rules	Sites	
Profile-1		<div></div>	2	0	...

Provide a name and description for the IPS profile. On the **IPS Rules** tab, enable the required **IPS Rules**.

Verify Config

IPS Profiles

IPS Rules

←

New IPS Profile

Profile Name *

Profile-1

Description

IPS Rules

Sites

Rule name	Description	Type	Status	Categories	Class Type	Action
Critical Priority	Critical Priority	Preset	<div></div>	0	15	blocklog
High Priority	High Priority	Preset	<div></div>	0	15	blocklog
Medium Priority	Medium Priority	Preset	<div></div>	0	7	log
Low Priority	Low Priority	Preset	<div></div>	0	1	default

Enable IPS Profile

Save

Cancel

Click **Sites**, select the sites, and turn on **Enable IPS Profiles**. Click **Review** and then click **Done**. Click **Create Profile**.

[Verify Config](#)
[IPS Profiles](#)
[IPS Rules](#)

[← New IPS Profile](#)

Profile Name *

Description

IPS Rules

Sites

☐ Global(All Sites)
☒ Specific Sites

Select Region/Groups

☒ Select All
☒ Default

Select Sites

☐ Select All
☐ dc2100

Cancel
Review

Showing 1 - 2 of 2 items
Page 1 of 1

☒ Enable IPS Profile

Create Profile

Cancel

You can enable or disable these IPS profiles while creating security profiles. The security profiles are used to create firewall rules. For more information, see [Security profile – Intrusion Prevention](#).

Virtual path IPsec settings

Virtual Path IPsec Settings defines the IPsec tunnel settings to ensure secure transmission of data over the Static Virtual Paths and Dynamic Virtual Paths. Select the **Static Virtual Paths IPsec** or **Dynamic Virtual Paths IPsec** tab to define the IPsec tunnel settings.

- **Encapsulation Type:** Choose one of the following security types:
 - **ESP:** Data is encapsulated and encrypted.
 - **ESP+Auth:** Data is encapsulated, encrypted, and validated with an HMAC.
 - **AH:** Data is validated with an HMAC.
- **Encryption Mode:** The encryption algorithm used when ESP is enabled.
- **Hash Algorithm:** The hash algorithm used to generate an HMAC.
- **Lifetime (s):** The preferred duration, in seconds, for an IPsec security association to exist. Enter 0 for unlimited.

For information on configuring IPsec service, see [IPsec service](#).

[Verify Config](#)[Static Virtual Paths IPsec](#)[Dynamic Virtual Paths IPsec](#)

Dynamic Virtual Path IPsec Settings

☒ Encrypt Dynamic Virtual Path with IPsec

Encapsulation Type *

ESP

Encryption Mode *

AES 128-Bit

Hash Algorithm *

SHA1

Lifetime (s) *

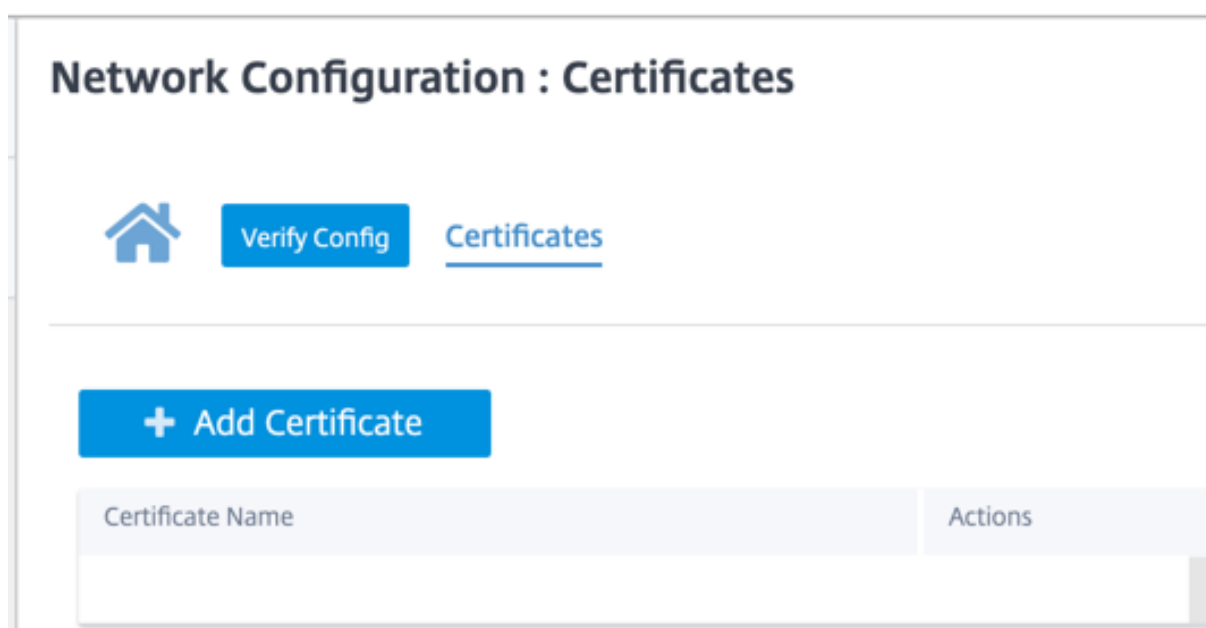
28800

Save

Click **Verify Config** to validate any audit error

Certificates

There are two types of certificates: Identity and Trusted. Identity Certificates are used to sign or encrypt data to validate the contents of a message and the identity of the sender. Trusted Certificates are used to verify message signatures. Citrix SD-WAN appliances accept both Identity and Trusted Certificates. Administrators can manage certificates in the Configuration Editor.




Click **Verify Config** to validate any audit error

To add a certificate click **Add Certificate**.

- **Certificate Name:** Provide the certificate name.
- **Certificate Type:** Select the certificate type from the drop-down list.
 - **Identity Certificates:** Identity certificates require that the certificate's private key be available to the signer. Identity Certificates or their certificate chains that are trusted by a peer to validate the contents and identity of the sender. The configured Identity Certificates and their respective Fingerprints are displayed in the Configuration Editor.
 - **Trusted Certificates:** Trusted Certificates are self-signed, intermediate certificate authority (CA) or root CA certificates used to validate the identity of a peer. No private key is required for a Trusted Certificate. The configured Trusted Certificates and their respective Fingerprints are listed here.

Network Configuration : Certificates

 [Verify Config](#) [Certificates](#)

Certificate

Certificate Name *

Enter Name

Certificate Type

Trusted

Trusted

Identity

Base64 Certificate *

Base64 Key

Cancel

Save

Hosted firewalls

SD-WAN Orchestrator for On-premises supports the following hosted firewalls:

- Palo Alto Networks
- Check Point

Palo Alto Networks

SD-WAN Orchestrator for On-premises supports hosting Palo Alto Networks Next-Generation Virtual Machine (VM)-Series Firewall on the SD-WAN 1100 platform. The following are the supported virtual machine models:

- VM 50
- VM 100

The Palo Alto Network virtual machine series firewall runs as a virtual machine on SD-WAN 1100 platform. The firewall virtual machine is integrated in Virtual Wire mode with two data virtual interfaces connected to it. Required traffic can be redirected to the firewall virtual machine by configuring policies on SD-WAN Orchestrator.

Check Point

SD-WAN Orchestrator for On-premises supports hosting **Check Point CloudGuard Edge** on SD-WAN 1100 platform.

The **Check Point CloudGuard Edge** runs as a virtual machine on SD-WAN 1100 platform. The firewall virtual machine is integrated in **Bridge** mode with two data virtual interfaces connected to it. Required traffic can be redirected to the firewall virtual machine by configuring policies on SD-WAN Orchestrator.

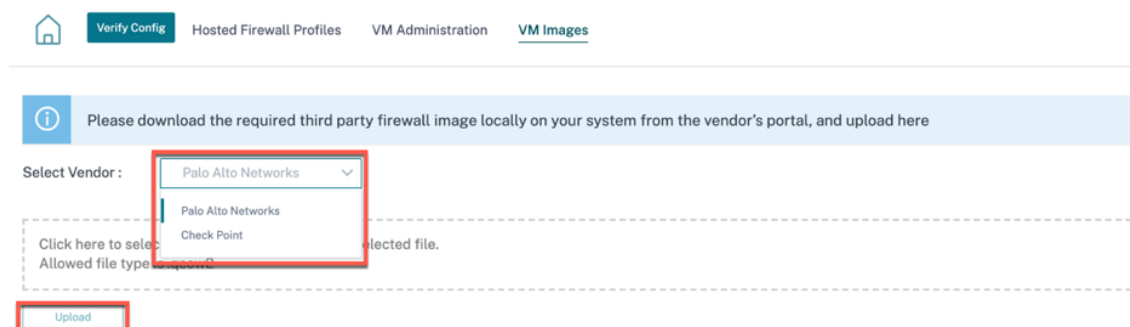
Benefits

The following are the primary goals or benefits of Palo Alto Networks integration on the SD-WAN 1100 platform:

- Branch device consolidation: A single appliance that does both SD-WAN and advanced security
- Branch office security with on-prem NGFW (Next Generation Firewall) to protect LAN-to-LAN, LAN-to-Internet, and Internet-to-LAN traffic

Perform the following steps for provisioning the firewall virtual machine through SD-WAN Orchestrator:

1. From SD-WAN Orchestrator for On-premises GUI, navigate to **Configuration > Security > select Hosted Firewall**.
2. To upload the software image, go to **VM Images** tab. Select the Vendor name as Palo Alto Networks/Check Point from the drop-down list. Click or drop the software image file in the box and click **Upload**.



A status bar appears with the ongoing upload process. Do not click **Refresh** or perform any other action until the image file shows 100% uploaded.

After the image is successfully uploaded, it will be available to use and can be selected when initiating the virtual machine provisioning.

3. Go to **VM Administration** tab and click **Provision**.

4. Provide the following details:

- **Vendor:** Select the vendor name as **Palo Alto Networks/Check Point**.
- **Model:** Select the virtual machine model number from the drop-down list.
- **Image File Name:** Select the software image from the uploaded files to provision Hosted Firewall virtual machine.

Note

The software image is provided by the vendors (Palo Alto Networks/Check Point).

- **Sites:** Select sites from the drop-down list where Hosted Firewall virtual machine has to be provisioned.
- **Panorama Primary IP or FQDN:** Enter the management server primary IP address or fully qualified domain name (Optional).

- **Panorama Secondary IP or FQDN:** Enter the management server secondary IP address or fully qualified domain name (Optional).
- **Authentication Code:** Enter the virtual authentication code to be used for licensing.
- **Authentication Key:** Enter the virtual authentication key to be used in the management server.

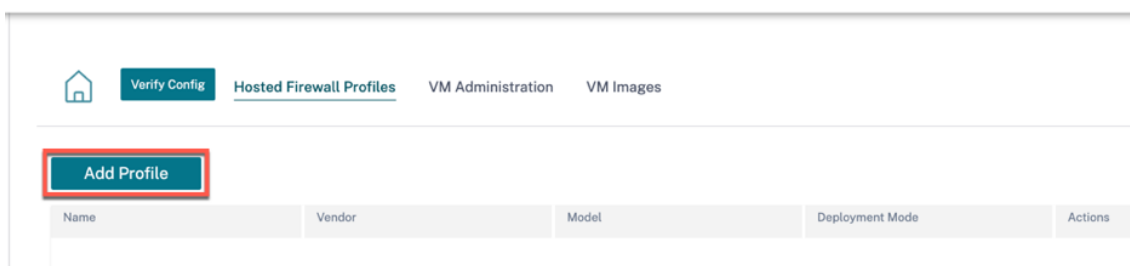
Virtual Machine Authentication Key is needed for automatic registration of the Palo Alto Networks virtual machine to the Panorama.

- Click **Provision**.

Once the virtual machine is provisioned on the SD-WAN 1100 platform, you can **Start**, **Shutdown**, or completely **De-Provision** that hosted firewall virtual machine.

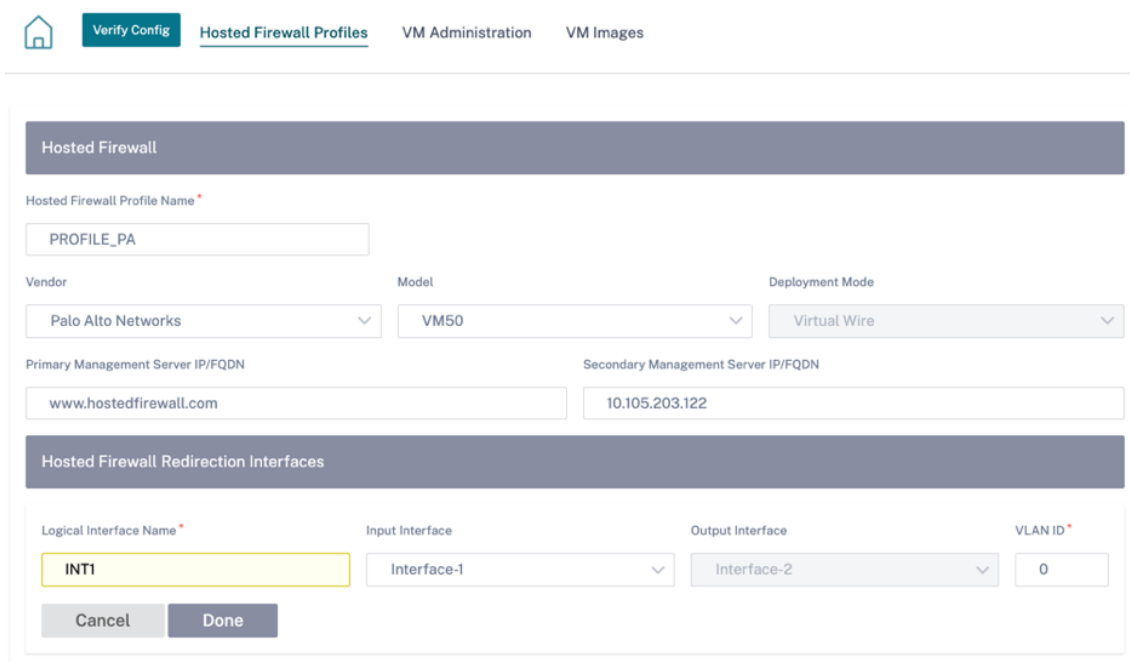
Traffic redirection

1. For traffic redirection, go to **Hosted Firewall Profiles** tab and click **Add Profile**.



The screenshot shows the top navigation bar with a home icon, a 'Verify Config' button, and tabs for 'Hosted Firewall Profiles', 'VM Administration', and 'VM Images'. Below the navigation bar, the 'Add Profile' button is highlighted with a red rectangular box. Below this button is a table with the following headers: Name, Vendor, Model, Deployment Mode, and Actions.

2. Provide the required information to add the **Hosted Firewall** template and click **Add**.



The screenshot shows the 'Hosted Firewall' configuration form. At the top, there is a header 'Hosted Firewall'. Below it, the 'Hosted Firewall Profile Name' field is filled with 'PROFILE_PA'. The 'Vendor' dropdown is set to 'Palo Alto Networks', the 'Model' dropdown is set to 'VM50', and the 'Deployment Mode' dropdown is set to 'Virtual Wire'. The 'Primary Management Server IP/FQDN' field is filled with 'www.hostedfirewall.com', and the 'Secondary Management Server IP/FQDN' field is filled with '10.105.203.122'. Below these fields is a section titled 'Hosted Firewall Redirection Interfaces'. This section contains a table with the following headers: Logical Interface Name, Input Interface, Output Interface, and VLAN ID. The 'Logical Interface Name' field is filled with 'INT1', the 'Input Interface' dropdown is set to 'Interface-1', the 'Output Interface' dropdown is set to 'Interface-2', and the 'VLAN ID' field is filled with '0'. At the bottom of this section are 'Cancel' and 'Done' buttons.

The **Hosted Firewall Template** allows you to configure the traffic redirection to the **Firewall virtual machine** hosted on SD-WAN Orchestrator. The following are the inputs needed to configure the template:

- **Hosted Firewall Profile Name:** Name of the hosted firewall template.
- **Vendor:** Name of the firewall vendor.
- **Model:** Virtual Machine model of the hosted firewall. You can select the virtual machine model number as VM 50/VM 100.
- **Deployment Mode:** The Deployment Mode field is auto populated and grayed out. For the Palo Alto Networks vendor, the deployment mode is Virtual Wire and for the Check Point vendor, the deployment mode is Bridge.
- **Primary Management Server IP/FQDN:** Primary management server IP/ fully qualified domain name of Panorama.
- **Secondary Management Server IP/FQDN:** Secondary management server IP/ fully qualified domain name of Panorama.
- **Hosted Firewall Redirection Interfaces:** These are logical interfaces used for traffic redirection between SD-WAN Orchestrator and hosted firewall.

Interface-1, Interface-2 refers to first two interfaces on the hosted firewall. If VLANs are used for traffic redirection then, same VLANs must be configured on the hosted firewall. VLANs configured for traffic redirection are internal to the SD-WAN Orchestrator and hosted firewall.

Note

Redirection input interface has to be selected from connection initiator direction. The redirection interface is automatically chosen for the response traffic. For Example, if outbound internet traffic is redirected to hosted firewall on Interface-1 then, response traffic is automatically redirected to hosted firewall on Interface-2. There is no need of Interface-2, if there is no internet inbound traffic.

Only two physical interfaces are assigned to host the Palo Alto Networks firewall and two data interfaces are assigned to Check Point virtual machine.

If traffic from multiple zones needs to be redirected to the hosted firewall then, multiple sub interfaces can be created using internal VLANs and associated to different firewall zones on the hosted firewall.

Note

SD-WAN firewall policies are auto created to Allow the traffic to/from hosted firewall management servers. This avoids redirection of the management traffic that is originated from (or) destined to hosted firewall.

Traffic redirection to firewall virtual machine can be done using SD-WAN firewall policies.

3. Navigate to **Configuration > Security > Firewall Profiles** > go to **Global Profiles** section. Click **+ Global Profile**.

The screenshot shows the 'Firewall Profiles' page. At the top, there is a navigation bar with a home icon, a 'Verify Config' button, and the 'Firewall Profiles' tab. Below this, there are three sections: 'Global Override Profiles', 'Site Specific Profiles', and 'Global Profiles'. The 'Global Profiles' section contains a red-bordered box with a '+ Global Profile' button. Below this button is a table with the following data:

No	Name	Actions
1	branch	


4. Provide a profile name and select the **Active Profile** check box. Click **Create New Rule**.

The screenshot shows the 'Firewall Rules' page. At the top, there is a navigation bar with a home icon, a 'Verify Config' button, and the 'Firewall Profiles' tab. Below this, there is a 'Profile Information' section with a 'Profile Name' field containing 'Profile1' and a checked 'Active Profile' checkbox. Below this is a 'Firewall Rules' section with a red-bordered box around a 'Create New Rule' button. Below this button are radio buttons for 'Top of List', 'Bottom of List', and 'Specify Row Number', followed by a 'Row number' input field. Below these is a table with the following data:

No	Match Type	Application	Src Zone	Dst Zone	Src Network	Dst Network	Action	Actions
----	------------	-------------	----------	----------	-------------	-------------	--------	---------

At the bottom of the page, there are 'Cancel' and 'Save' buttons.

5. Change the **Policy Type** to **Hosted Firewall**. The **Action** field is auto filled to **Redirect to Hosted Firewall**. Select the **Hosted Firewall Profile** and the **Hosted Firewall Redirection Interface** from the drop-down list.

[Verify Config](#)[Firewall Profiles](#)

Profile Information

Profile Name ^{*}
 ☒ Active Profile

Firewall Type

Match Criteria

Match Type Routing Domain

Filtering Criteria

Source Zone Destination Zone

Source Service Type Source Service Name ^{*} Source IP Source Port

Dest Service Type Dest Service Name ^{*} Dest IP Dest Port

IP Protocol DSCP ☒ Allow Fragments ☐ Reverse Also ☐ Match Established

Actions

Action Hosted Firewall Profile ^{*} Hosted Firewall Redirection Interface ^{*}

☐ Connection State Tracking

☒ Log Connection Start & End Events

☒ Log Packet Statistics

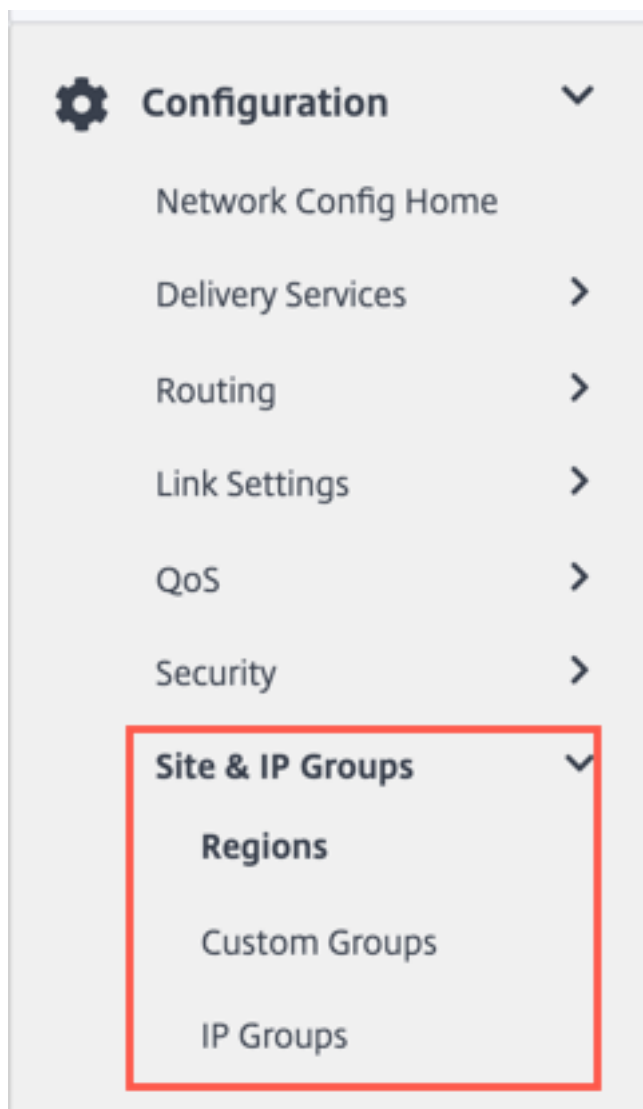
6. Fill the other match criteria as required and click **Done**.

Site and IP Groups

October 21, 2020

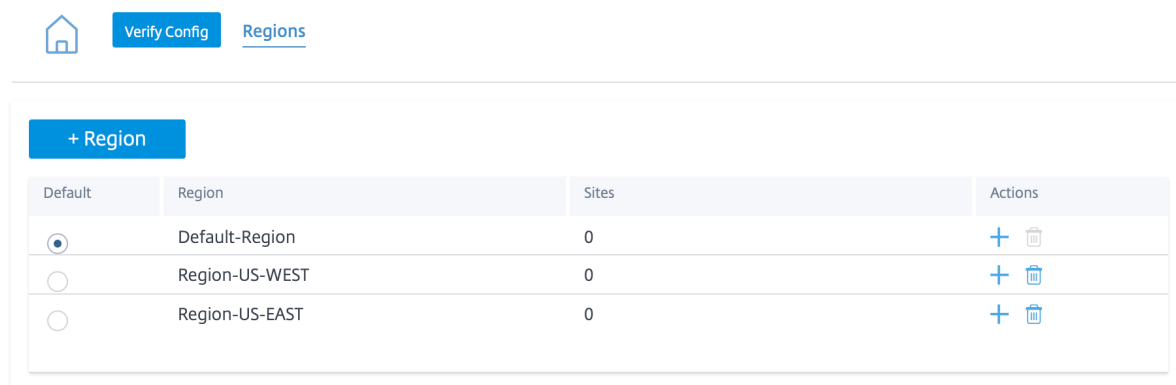
Administrators can group sites or IP addresses to simplify common application policies across multiple sites or network addresses, and also serve as filters for reports.

To view Regions, Site and IP Groups, navigate to **Configuration > Site & IP Groups**.



Regions

Regions help to create administrative boundaries within large networks spanning hundreds to thousands of sites. If your organization has a large network spanning multiple administrative (or geographical) boundaries, you can consider creating regions to segment the network.



Currently, a maximum of 550 sites are supported per region. Each region is expected to have a Regional Control Node (RCN), which serves as the hub and controller for the region. So, you would typically consider a multi-region deployment if your network has more than 500 sites. By default, all networks are single region networks, where the Master Control Node (MCN) serves as the hub and the control node for all the sites. On adding one or more regions, the network becomes a multi-region network. The region associated with the MCN is called the **default region**.

A multi-region network supports a hierarchical architecture with an MCN controlling multiple RCNs. Each RCN, in turn, controls multiple branch sites. Even in a multi-region deployment, you can have the MCN double up as the direct hub node for a subset of the sites while having the rest of the sites use their respective RCNs as hub nodes.

The sites being managed directly by the MCN that is, the RCNs and potentially some other sites directly managed by the MCN are said to be in the **default** region. The **default region** would be the only region for a network before other regions are added. After adding other regions, you can select the **Default** option to use a desired region as the default region.


To create a region:

1. Click **+ Region**. Provide a region name and description.
2. Enable Interval VIP matching based on whether you want **Forced Internal VIP Matching** or **Allow External VIP Matching**.
 - **Forced Internal VIP Matching:** When enabled, all non-private Virtual IP addresses in the Region are forced to match the configured subnets.
 - **Allowed External VIP Matching:** When enabled, non-private Virtual IP addresses from other regions are allowed to match the configured subnets.
3. Click **+ Subnets** to add subnets. Enter a **Network** address. The network address is the IP address and mask for the subnet.
4. Select the sites.

5. Click **Review** and then **Save**. The newly created region is added to the existing list of regions.

Note

A customer can only have Static or Dynamic Virtual paths within a Region.

[Verify Config](#)[Regions](#)


Region Attributes

Region Name: Region-

Description

☐ Force Internal VIP Matching ☐ Allow External VIP Matching

+ Subnets

Network	Delete
<input type="text" value="Eg: a.b.c.d/e"/>	

Sites

☒ Import Sites from other Regions

Search Sites

Select Region(s) to Import from

☒ Select All☒ Default-Region

Select Sites to be Imported

Cancel

Review

You can place sites under the region once a Region is created successfully.

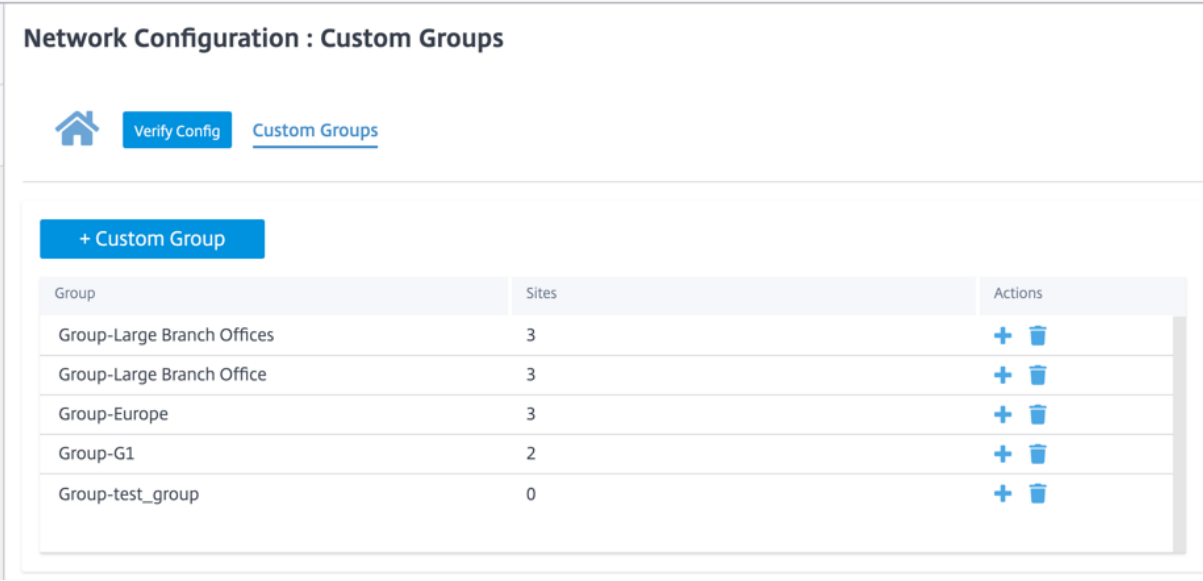
Note

Dynamic virtual paths cannot be established between branches in different regions.

Click **Verify Config** to validate any audit error.

Custom groups

Custom Groups provide users the flexibility to group sites as needed. Users can apply policies for groups of sites at once, without necessarily having to deal with each site individually. Groups can also serve as filters for dashboards, reports, or network configuration. Unlike Regions, groups can overlap in terms of sites. In other words, the same sites can be part of multiple groups.



Network Configuration : Custom Groups

Home Verify Config Custom Groups


+ Custom Group

Group	Sites	Actions
Group-Large Branch Offices	3	+
Group-Large Branch Office	3	+
Group-Europe	3	+
Group-G1	2	+
Group-test_group	0	+

For example, a user can create a group named **Business Critical Sites** to configure common policies for all your business-critical sites. The user can also monitor their health and performance separately as a group. Some of those sites can also be a part of a **Large Branch Office** group, for instance.

Custom Site Groups provide a way to logically group sites together for reporting purposes. You can create custom groups and add sites to each custom group. To create a custom group click **+ Custom Group**. Provide a group name and select or add sites. Click **Review** and then **Save**.

Network Configuration : Custom Groups

 [Verify Config](#) [Custom Groups](#)

Group Attributes

Group Name: Group-

Sites

+ Sites



Search Sites

Select Group(s) to pick from

☒ Select All
☒ Default-Region
☒ Region-Main_Office
☒ Region-Sales_office
☒ Group-Large Branch O
☒ Group-Large Branch O
☒ Group-Europe
☒ Group-G1
☒ Group-test_group

Select Sites to be Added

☐ Select All
☐ Bangalore
☐ Belgium
☐ London
☐ Madrid
☐ NewYork
☐ San Francisco

Showing 1 - 6 of 6 items Page 1 of 1  

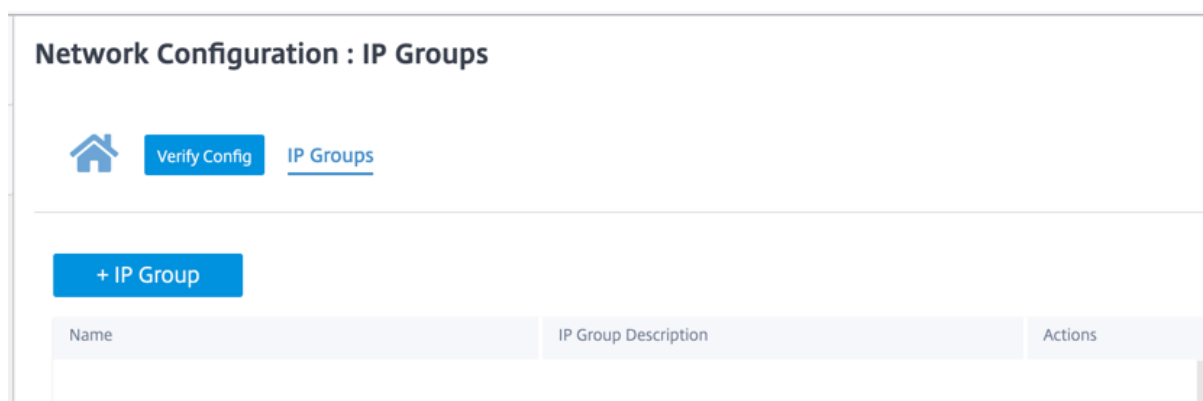
Cancel

Review

Click **Verify Config** to validate any audit error.

IP groups

Users can group IP and network addresses by using **IP Groups**. These groups can be used in configuration and policies as needed, without necessarily having to key in individual IP addresses each time.



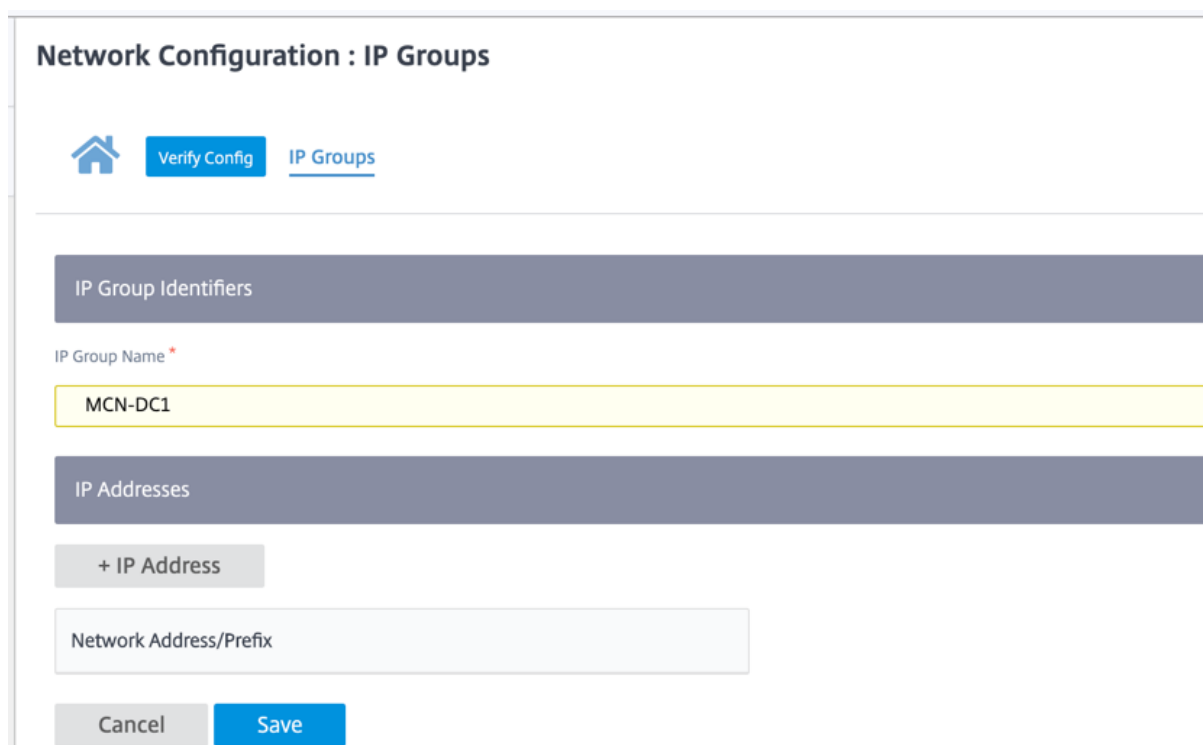
Network Configuration : IP Groups

[Home](#) [Verify Config](#) [IP Groups](#)

[+ IP Group](#)

Name	IP Group Description	Actions
------	----------------------	---------

You can create IP groups and add sites to each IP group. Network objects can be grouped based on the IP address. To create an IP group, select **IP Groups** and click **+ IP Group**. Provide a group name. Click **+ IP Address** and enter **IP addresses** to be added to the IP group.



Network Configuration : IP Groups

[Home](#) [Verify Config](#) [IP Groups](#)

IP Group Identifiers

IP Group Name *

MCN-DC1

IP Addresses

[+ IP Address](#)

Network Address/Prefix

[Cancel](#) [Save](#)

Click **Verify Config** to validate any audit error

Application and DNS settings

April 7, 2021

This section enables users to custom define applications, group applications for use in policies, QoS Profiles, and also DNS settings.

You can define an **Application Group** for both predefined and custom applications. An **Application Group** contains applications that need similar treatment when defining a security policy.

You can reuse the **Application Groups** frequently when defining policies such as application steering or firewall rules. It eliminates the need to create multiple entries for each individual application. Similarly, while using any application services, Application Groups supports common applications with a unique name for simplified and consistent reuse.

To view **Apps and DNS settings**, navigate to **Configuration > Application & DNS Settings**.

Application settings

The Citrix SD-WAN appliances perform Deep Packet Inspection (DPI) to identify and classify applications. The DPI library recognizes thousands of commercial applications. It enables real-time discovery and classification of applications. Using the DPI technology, the SD-WAN appliance analyses the incoming packets and classifies the traffic as belonging to a particular application or application family.

DPI is enabled globally, by default, for all the sites in your network. Disabling DPI stops DPI classification capability on the appliance. You can no longer use DPI classified application / application categories to configure firewall, QoS, and routing policies. You will also not be able to view the top applications and application categories report.

To disable global DPI, at the Network level, navigate to **Configuration > App & DNS Settings > Application Settings** and clear the **Enable Global DPI** check box option.

Global Application Settings

☒ Enable Global DPI

Site Overrides

Select Region/Groups

☒ Select All

☒ default

☒ Custom_Region

Select Sites

☐ Select All

☒ Germany_Masternode

☒ London_Site

☐ Greece_Site Clone

☐ Italy

Cancel

Review

Showing 1 - 5 of 5 items

Page 1 of 1

You can also choose to disable DPI for certain sites only by overriding the global DPI settings. To disable DPI for selected sites, add the sites to the **Site Overrides** list.

Custom application

The **Custom Applications** are used to create internal applications or IP-port combinations which are not available in the list of published applications. The administrator needs to define a custom application that can be used in multiple policies as needed, without referring the IP address and port number details each time.

The administrator can define a custom application based on the IP protocol or Domain name.

To create a custom application using an IP protocol, click + **Custom Application** and provide a name for the custom application. Specify the match criteria such as IP protocol, network IP address, port number, and, DSCP tag. The data flow matching this criteria is grouped as the custom application.

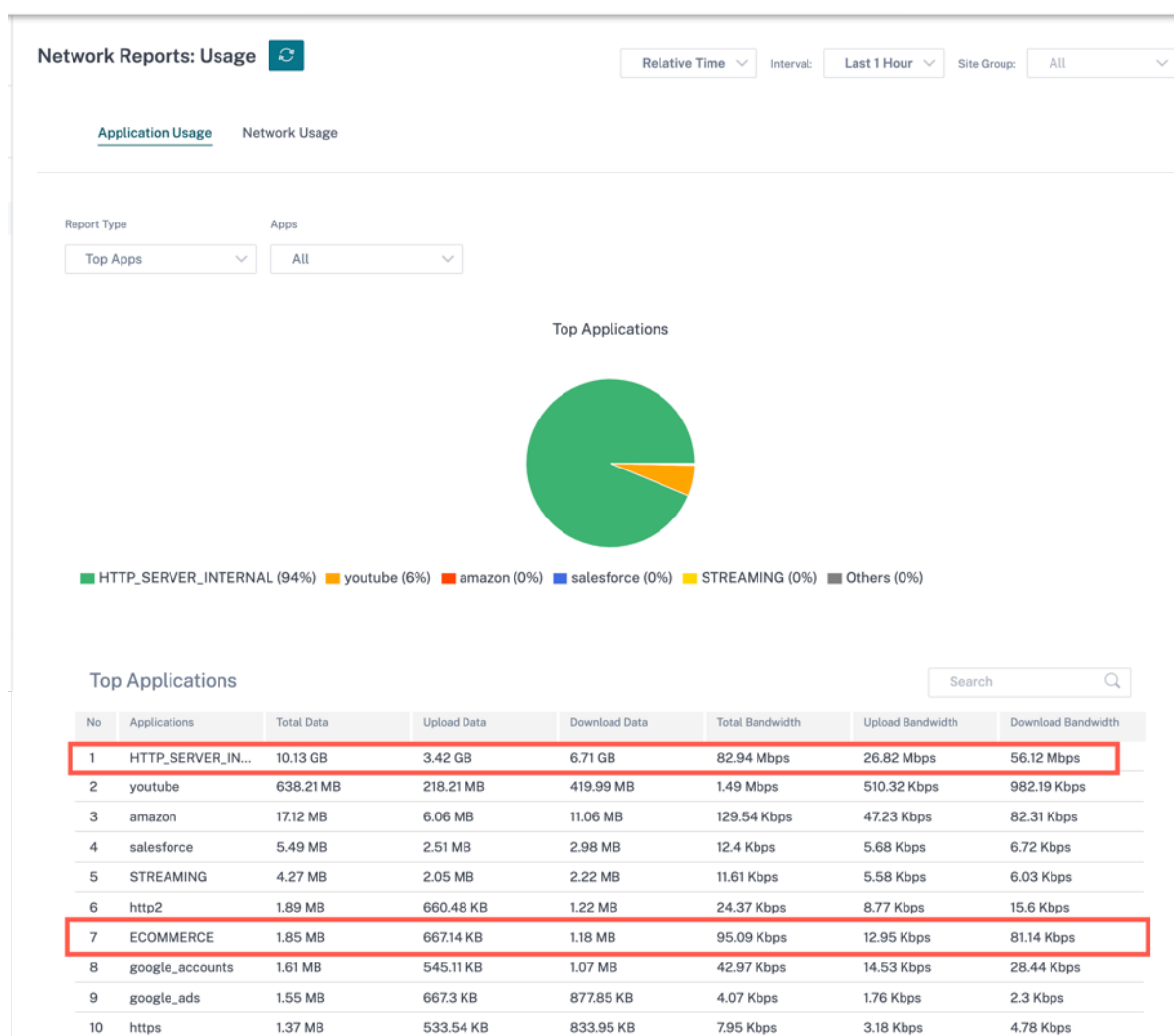
The screenshot shows the 'Custom Apps' configuration page in the SD-WAN Orchestrator. At the top, there are tabs for 'Verify Config' and 'Custom Apps'. Below the tabs, the 'Custom App Name' field is set to 'HTTP_SERVER_INTERNAL'. There are two radio buttons: 'IP Protocol' (selected) and 'Domain Name Based'. The 'Enable Reporting' checkbox is checked. The 'Reporting Priority' field is set to '100'. Below this is a 'Match Criteria' section with a table. The table has columns: Application, Protocol, Network IP, Port, DSCP, and Actions. The first row shows 'Any' for Application, 'TCP (6)' for Protocol, '*' for Network IP, '80' for Port, and 'DEFAULT' for DSCP. There are 'Cancel' and 'Save' buttons at the bottom.

Application	Protocol	Network IP	Port	DSCP	Actions
Any	TCP (6)	*	80	DEFAULT	

Once saved, the custom applications show up in a list and can be edited or deleted, as required.

The **Enable Reporting** check box is added for the IP Protocol based custom applications. You must select the **Enable Reporting** check box and provide the reporting priority.

With the **Enable Reporting** feature enhancement, you can not only view the DPI classified application report but also view the IP protocol and domain name based custom application traffic under the **Reports > Usage**.



You can also group several domain names as an application. To create custom applications based on domain name, select **Domain Name Based**. Enter the application name and the required domain names or patterns. You can either enter the full domain name or use wild cards at the beginning.

Home Verify Config Custom Apps

Custom App Name *

ECOMMERCE ☐ IP Protocol ☒ Domain Name Based

Domains

+ Domain

Domain Name/Pattern	
www.amazon.in	—
www.flipkart.com	—

Cancel Save

All the domain name based custom applications are visible in **Application Routing, Application Rule, and Firewall Profiles**.

Note

To use a custom name based application, the match criteria must be listed as Application while creating the Application Route and firewall policy.

Once you have created the custom application, to perform the application routing, navigate to **Routing > Routing Policies > + Application Route**, select the custom application under the **Application** drop-down list.

Home Verify Config Application Routes IP Routes

Cost Ranges: Custom Application (1-20) Application (21-40) Application Group (41-60) IP (1-65535)

Application Match Criteria

Match Type Application Routing Domain

Application Any

Scope

☒ Global Route ☐ Site / Group Specific

Traffic Steering

Delivery Service

Internet Breakout

Cancel Save

You can also select the DNS based custom application under the match criteria of an **IP Protocol** custom application.

Similarly, to view the custom application under the **Firewall Policies**, navigate to **Security > Firewall Policies**. The application can be used for any type of policy (Global override/Site Specific/Global Policies). Click **Create New Rule** and under **Match Criteria**, select the custom application from the drop-down list.

You can view the DNS based custom applications both under **Global or Site/Group Specific Rule**. To view the custom application under the **Application Rule**, navigate to **QoS > QoS Policies > Global Rules > Application Rule** > under **Application Match Criteria**, select the custom application from the **Application** drop-down list.

Global Rules : Application

Application Match Criteria

Application *	Routing Domain
ECOMMERCE	Any
Source Network	Destination Network
Any	Any
<input type="checkbox"/> Src = Dest	
Source Port	Destination Port
Any	Any
<input type="checkbox"/> Src = Dest	

Click **Verify Config** to validate any audit error.

Application groups

An **Application Group** helps administrators group similar applications together for use in common policies, without necessarily having to create a policy for each individual application.

Network Configuration : App Groups

Verify Config App Groups

+ Application Group

Application Group Name	Actions
O365_Group	


You can create an **Application Group** by using the **Add Application Groups** option. You can refer the same Application Group while creating a policy as per the application role. The policy that is defined for the particular group is applied to each application that matches to the specific category.

For example, you can create an **Application Group** as **Social Networking** and add social networks such as Facebook, LinkedIn, and Twitter to the group to define certain policies for social networking applications.

To create an **Application Group**, specify a group name, search, and add apps from the **Applications** list.

You can always go back and edit your settings or delete **Application Group** as needed.

Network Configuration : App Groups

[Verify Config](#)[App Groups](#)




App Group Name *

Enter Name

Applications

Search Apps

Add

Application Name	Actions
Ibay.com.mv(ibay)	
My Yahoo(my_yahoo)	
Gsshop.com(gsshop)	

Cancel

Save

Click **Verify Config** to validate any audit error.

Application quality profiles

This section enables you to view and create application quality profiles.

Application QoE is a measure of Quality of Experience of applications in the SD-WAN network. It measures the quality of applications that flow through the virtual paths between two SD-WAN appliances. The Application QoE score is a value between 0 and 10. The score range that it falls in determines the quality of an application.


Quality	Range
Good	8–10
Fair	4–8
Poor	0–4

Application QoE score can be used to measure the quality of applications and identify problematic trends.

Profile configuration

Click **+ QoE Profile** to create a QoE profile, specify a profile name, and select a traffic type from the drop-down list.

Network Configuration : App Quality Profiles


[Verify Config](#)
[App Quality Profiles](#)

Profile Configuration

Profile Name *
Traffic Type *

Hybrid

Realtime Configuration

One Way Latency (ms) *
Jitter (ms) *
Packet Loss (%) *

160
30
2

Interactive Configuration

Expected Burst Rate (%) *
Packet Loss per Flow (%) *

60
1

Cancel
Done

Real-time configuration

You can define the quality thresholds for real-time and interactive appliances using QoE profiles, and map these profiles to applications or applications objects.

The Application QoE calculation for real-time applications uses a Citrix innovative technique, which is derived from the MOS score.

The default threshold values are:

- Latency threshold (ms): 160
- Jitter Threshold (ms): 30
- Packet loss threshold (%): 2

A flow of a real-time application that meets the thresholds for latency, loss, and jitter is considered to be of good quality.

QoE for Real-time applications is determined from the percentage of flows that meet the threshold divided by the total number of flow samples.

QoE for Real-time = (No of flow samples that meet the threshold / Total no of flow samples) * 100

It is represented as QoE score ranging from 0 to 10.

Interactive configuration

The Application QoE for interactive applications uses a Citrix innovative technique based on packet loss and burst rate thresholds.

Interactive applications are sensitive to packet loss and throughput. Therefore, we measure the packet loss percentage, and the burst rate of ingress and egress traffic in a flow.

The configurable thresholds are:

- Packet loss percentage.
- Percentage of expected egress burst rate in comparison to the ingress burst rate.

The default threshold values are:

- Packet loss threshold: 1%
- Burst rate: 60%

A flow is of good quality if the following conditions are met:

- The percentage loss for a flow is less than the configured threshold.
- The egress burst rate is at least the configured percentage of ingress burst rate.

Application quality configuration

Map application or application objects to default or custom QoE profiles. You can create custom QoE profiles for real-time and interactive traffic.

Click **+QoE Configuration** to create custom QoE profiles:

- **Type:** Select the DPI application or an application object (Application, Custom Apps, and Application Groups).
- **Application:** Search and select an application or application object based on the selected Type.
- **QoE Profile:** Select a QoE profile to map to the application or application object.

Home Verify Config App Quality Config

Application QoE Configuration

Type* Application* QoE Profile*

Application ▼

- Application
- Custom Apps
- Application Groups

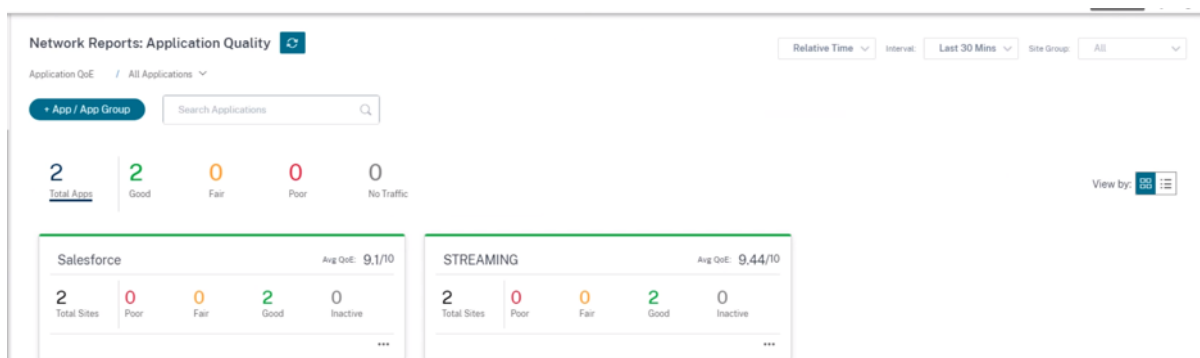
Application ▼

DefaultQOEProfile ▼

Click **Done**.

Click **Verify Config** to validate any audit error.

Once you configure the application QoE with the custom application type, a relevant application report tile is auto generated under the **Reports > Application Quality**. Any traffic that is matching with the selected application goes over the virtual path for the custom application.



DNS servers

You can configure specific DNS servers to which the DNS requests are routed.

Enter a name for the DNS server and choose **Type** as **Static** (for IPv4 addresses) or **StaticV6** (for IPv6 addresses). Specify the Primary and Secondary DNS server IP addresses. You can create internal, ISP, google or any other open source DNS service.

[Verify Config](#)[DNS Servers](#)

DNS Service

DNS Service Name *

Type

Eg: dns_service1

Static

Primary DNS *

Secondary DNS

Eg: a.b.c.d

Eg: a.b.c.d

Cancel

Save

Click **Verify Config** to validate any audit error.

Proxy Auto Config

With the increase in enterprise adoption of mission-critical SaaS applications and distributed workforce, it becomes highly critical to reduce latency and congestion. Latency and congestion are inherent in traditional methods of backhauling traffic through the Data Center. Citrix SD-WAN allows direct internet break out of SaaS applications such as Office 365. For more information, see [Office 365 Optimization](#).

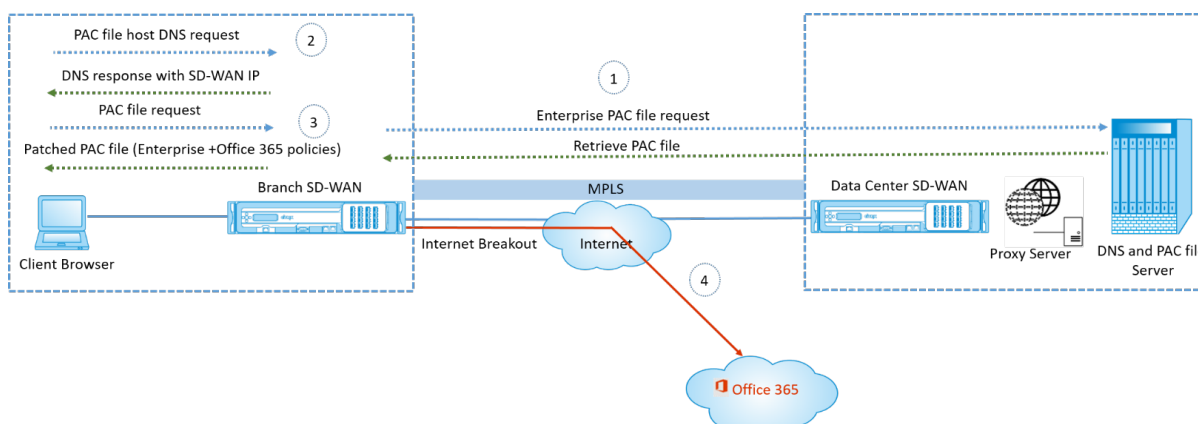
If there are explicit web proxies configured on the enterprise deployment all traffic are steered to the web proxy making it difficult for classification and direct internet breakout. The solution is to exclude SaaS application traffic from getting proxied by customizing the enterprise PAC (Proxy Auto-Config) file.

Citrix SD-WAN 11.0 allows proxy bypass and local Internet breakout for Office 365 application traffic by dynamically generating and serving a custom PAC file. PAC file is a JavaScript function that defines whether web browser requests go directly to the destination or to a web proxy server.

How PAC file customization works

Ideally, the enterprise network host PAC file on the internal web server, these proxy settings are distributed via group policy. The Client browser requests for PAC files from the enterprise web server.

The Citrix SD-WAN appliance serves the customized PAC files for sites where Office 365 breakout is enabled.



1. Citrix SD-WAN periodically requests and retrieves the latest copy of the enterprise PAC file from the enterprise web server. The Citrix SD-WAN appliance patches office 365 URLs to the enterprise PAC file. The enterprise PAC file is expected to have a placeholder (SD-WAN specific tag) where the Office 365 URLs are seamlessly patched.
2. The Client browser raises a DNS request for the enterprise PAC file host. Citrix SD-WAN intercepts the request for the proxy configuration file FQDN and responds with the Citrix SD-WAN VIP.
3. The Client browser requests for the PAC file. Citrix SD-WAN appliance serves the patched PAC file locally. The PAC file includes enterprise proxy configuration and Office 365 URL exclusion policies.
4. On receiving a request for the Office 365 application, the Citrix SD-WAN appliance performs a direct internet breakout.

Prerequisites

1. The enterprises must have a PAC file hosted.
2. The PAC file must have a placeholder *SDWAN_TAG* or one occurrence of the `findproxyforurl` function for patching Office 365 URLs.
3. The PAC file URL must be domain based and not IP based.
4. The PAC file is served only over the trusted identity VIPs.
5. Citrix SD-WAN appliance must be able to download the enterprise PAC file over its management interface.

Configure Proxy Auto Config

In the SD-WAN Orchestrator UI, at the network level, navigate to **Configuration > App and DNS Settings > Proxy Auto Config** and click **+ PAC file profile**.

Network Configuration : Proxy Auto Config

The screenshot displays the 'Proxy Auto Config' configuration page. At the top, there is a navigation bar with a home icon, a 'Verify Config' button, and the 'Proxy Auto Config' tab. Below this is a 'Profile Information' section with two input fields: 'Profile Name' (containing 'PAC1') and 'PAC File URL' (containing 'http://www.testpac.com/test.pac'). Below the 'Profile Information' section is a 'Select Site(s)' section. This section contains two columns: 'Select Region/Groups' and 'Select Sites'. The 'Select Region/Groups' column lists various regions and groups, all of which are selected. The 'Select Sites' column lists various sites, with Belgium, London, and San Francisco selected. At the bottom, there are 'Cancel' and 'Review' buttons, and a pagination bar showing 'Showing 1 - 7 of 7 items' and 'Page 1 of 1'.

Enter a name for the PAC file profile, provide the URL of the enterprise PAC file server. The Office 365 breakout rules are dynamically patched to the enterprise PAC file.

Select the sites to which the PAC file profile is applied. If there are different URLs for each site, create a different profile per site.

Limitations

- HTTPS PAC file server requests are not supported.
- Multiple PAC files in a network are not supported, including PAC files for routing domains or security zones.
- Generating a PAC file on Citrix SD-WAN from scratch is not supported.
- WPAD through DHCP is not supported.

Profiles and Templates

May 4, 2021

A profile is a live configuration template. A regular template aids the creation of a new entity. But once the template is created, subsequent changes in the template do not apply to the existing entities created using the base template. A profile serves as the live central master entity. The all child entities inherit from the profile, not only during creation but also throughout the life of a profile. All the child entities associated with the profile, automatically inherit any changes made in a profile.

For example, an admin creates a site configuration profile called the small retail store and applies it to all the small retail stores owned by a company. Now, any changes made to the small retail store profile at any given time would be applied automatically to all the stores inheriting this profile. Based on what's common across all the entities, and what's not, certain parameters in the profile configuration can be left unset. Such parameters would be customizable and can vary across the entities inheriting the same profile.

Site profile

Site profiles help you to easily and quickly configure sites. You can create a site profile once and reuse it multiple times while creating sites.

Network Configuration : Profiles & Templates

Home [Profiles](#) Templates

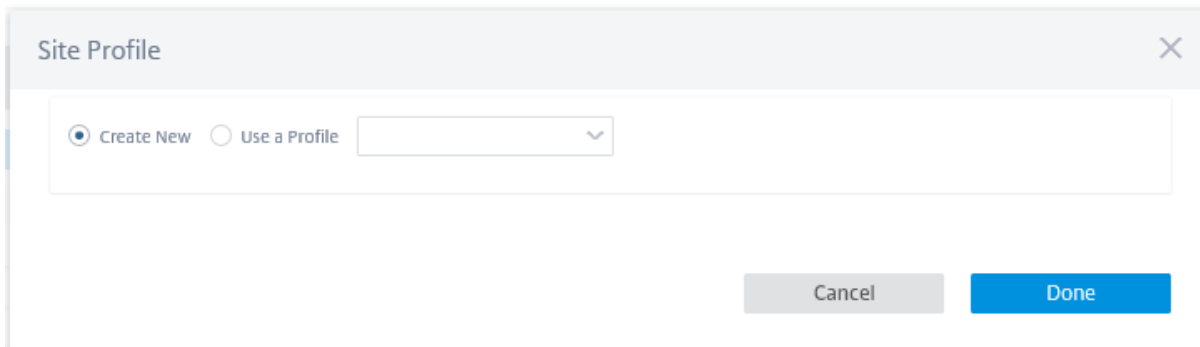
Site Profiles ?

[+ Site Profile](#)

Site Profile	Site Count	Actions
test	0 / 6	
Internetsite	0 / 6	
testdhcp	0 / 6	
Test_service	0 / 6	

To create a site profile, click **+ Site Profile**. You can create a profile from scratch or edit an existing site

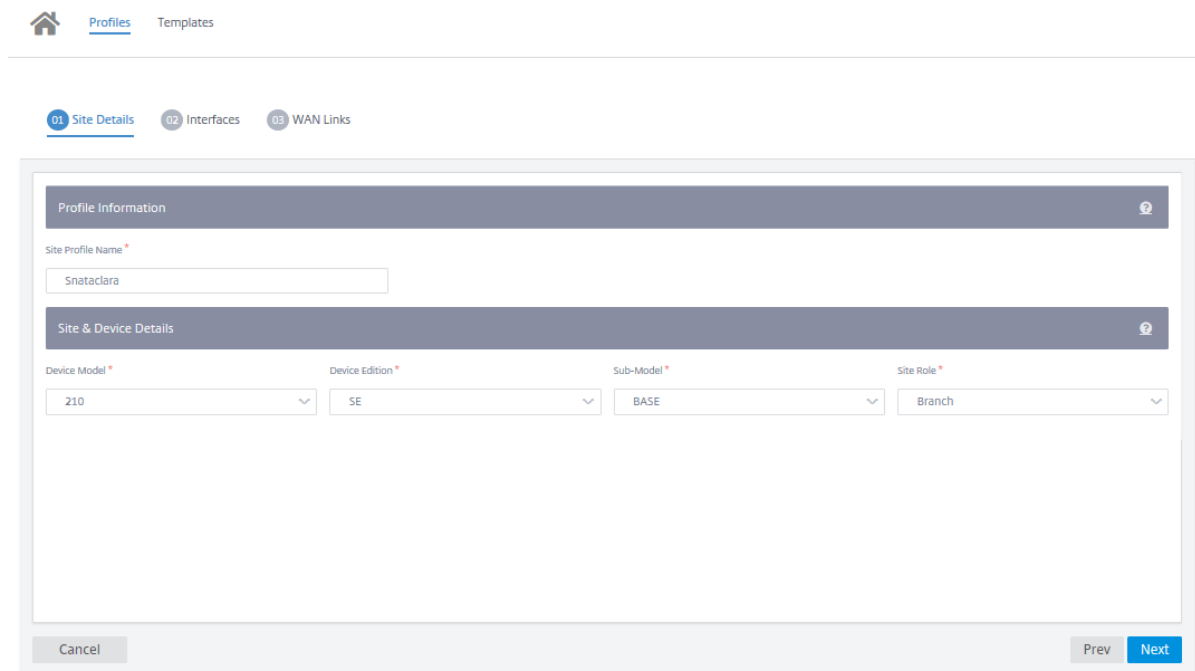
profile and save it as a new profile.

A dialog box titled "Site Profile" with a close button (X) in the top right corner. Inside the dialog, there are two radio buttons: "Create New" (which is selected) and "Use a Profile". To the right of the "Use a Profile" radio button is a dropdown menu. At the bottom right of the dialog, there are two buttons: "Cancel" and "Done".

To create a site profile, you need to configure the **Site Details**, **Interfaces**, and **WAN Links**. For detailed description of configuring sites, see [Site details](#).

Provide the device details.

Network Configuration : Profiles & Templates

A screenshot of the "Site Details" configuration page in the SD-WAN Orchestrator. The page has a breadcrumb trail: "Profiles" > "Templates". Below this, there are three tabs: "01 Site Details" (active), "02 Interfaces", and "03 WAN Links". The main content area is divided into two sections: "Profile Information" and "Site & Device Details". In the "Profile Information" section, there is a "Site Profile Name" field with the value "Snataclara". In the "Site & Device Details" section, there are four dropdown menus: "Device Model" (210), "Device Edition" (SE), "Sub-Model" (BASE), and "Site Role" (Branch). At the bottom of the page, there are three buttons: "Cancel", "Prev", and "Next".

Assign an interface for the site by clicking the **+ Interface** option. To add an interface, you need to fill the **Interface Attributes**, **Physical Interface**, and **Virtual Interfaces** fields. For detailed description of configuring interfaces, see [Interfaces](#).

01 Site Details

02 Interfaces

03 WAN Links

Interface Attributes

?

Deployment Mode *

Interface Type *

Security *

Interface Name

Edge (Gateway) ▾

LAN ▾

Trusted ▾

LAN-1

Physical Interface

?

Select Interface *

12345678

☐ LSP

Virtual Interfaces

?

VLAN ID *

Virtual Interface Name

0

VIF-2-LAN-1

Routing Domain *

Firewall Zones

Default_RoutingDomain ▾

<Default> ▾

Save

Cancel

Fill **WAN Link Attributes**, **Access Interfaces**, and **Services** with **Advanced Options**.

For detailed description of configuring WAN links, see [WAN links](#).

01 Site Details

02 Interfaces

03 WAN Links

WAN Link Attributes

Access Type *

ISP Name *

☐ Custom

Internet Category

Public Internet

Verizon

Select Internet Type

Link Name

Egress Speed *

Mbps

Ingress Speed *

Mbps

Internet-Verizon

100

100

☐ Public IP Address Auto Learn

Access Interfaces

Add Access Interface

Name	Virtual Interface	VIF Path Mode	Actions
Alf-1	VIF-Bridge-1-VLAN-0	Primary	

Advanced WAN Options

☐ Active MTU detect ☐ Enable Metering

Congestion Threshold (µs)

Provider ID

Frame Cost (Bytes)

Standby Mode

Tunnel Header Size

MTU (Bytes)

Priority

Active Heartbeat Interval

Standby Heartbeat Interval

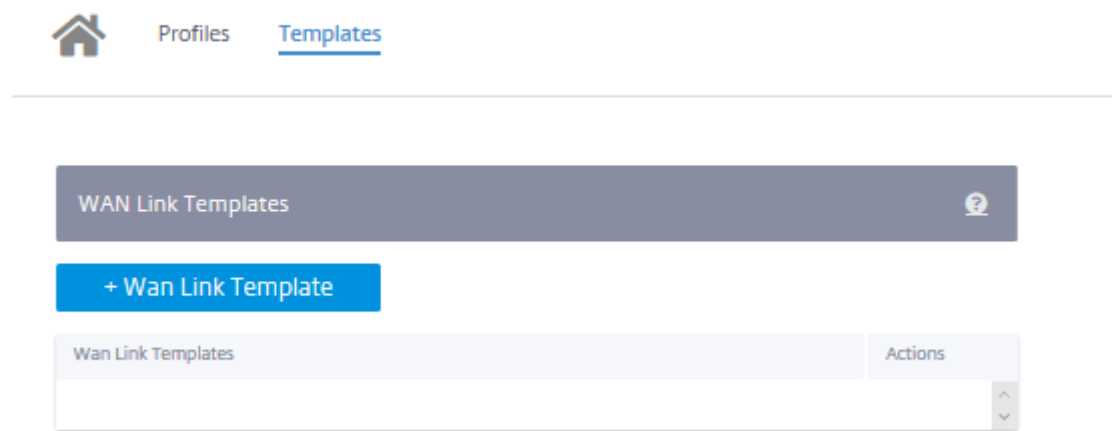
Cancel

Done

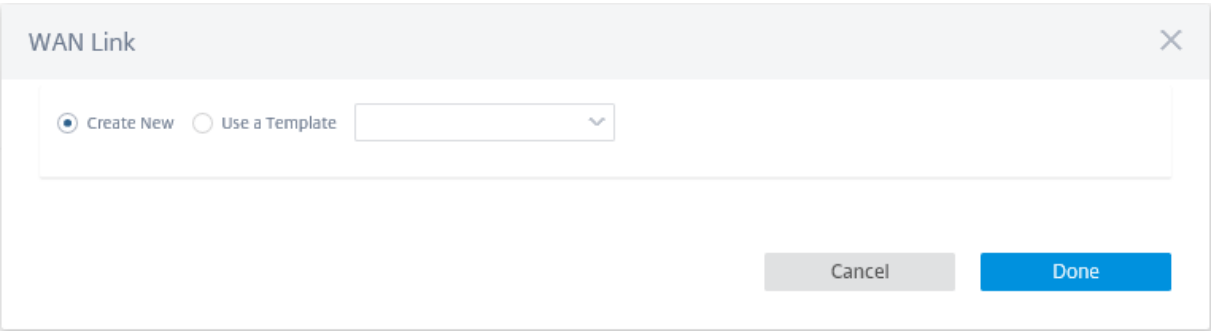
WAN link template

WAN link templates help you to easily and quickly configure WAN links. You can create a WAN link template once and reuse it multiple times while configuring WAN links.

Network Configuration : Profiles & Templates

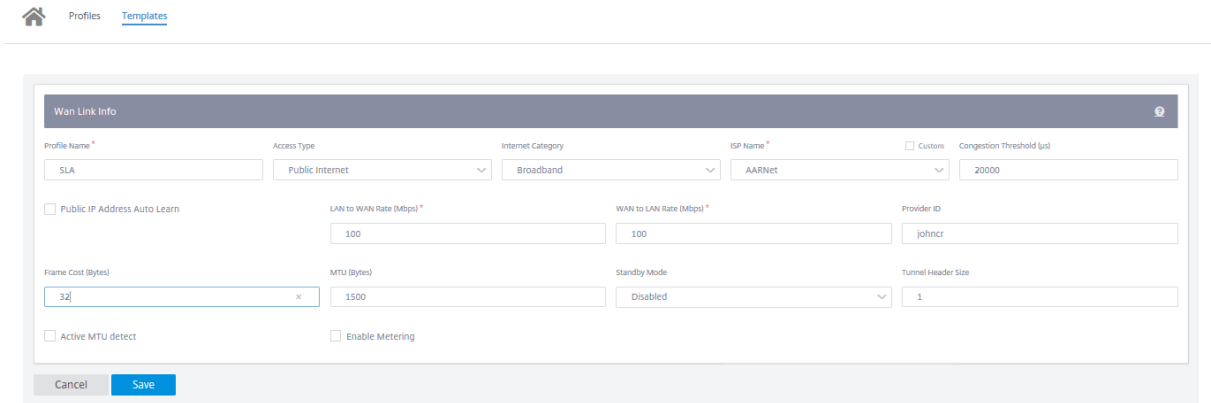


To create a WAN link template, click **+ WAN Link Template**. You can create a template from scratch or edit an existing WAN link template and save it as a new template.



Provide the WAN link information such as **Profile Name**, **Access Type**, **Internet Category**, **LAN to WAN Rate** (Mbps) and so on to create a WAN profile. For detailed description of configuring WAN links, see [WAN links](#).

Network Configuration : Profiles & Templates



Site configuration

April 28, 2021

You can add new sites from the Network Dashboard and configure your SD-WAN network.

To create a site, click **+ New site** on the Network Dashboard. Provide a name and location for the site.

The screenshot shows the 'New Site' configuration form. The form is titled 'New Site' and contains a section for 'Site Details'. Within this section, there are several input fields and options:

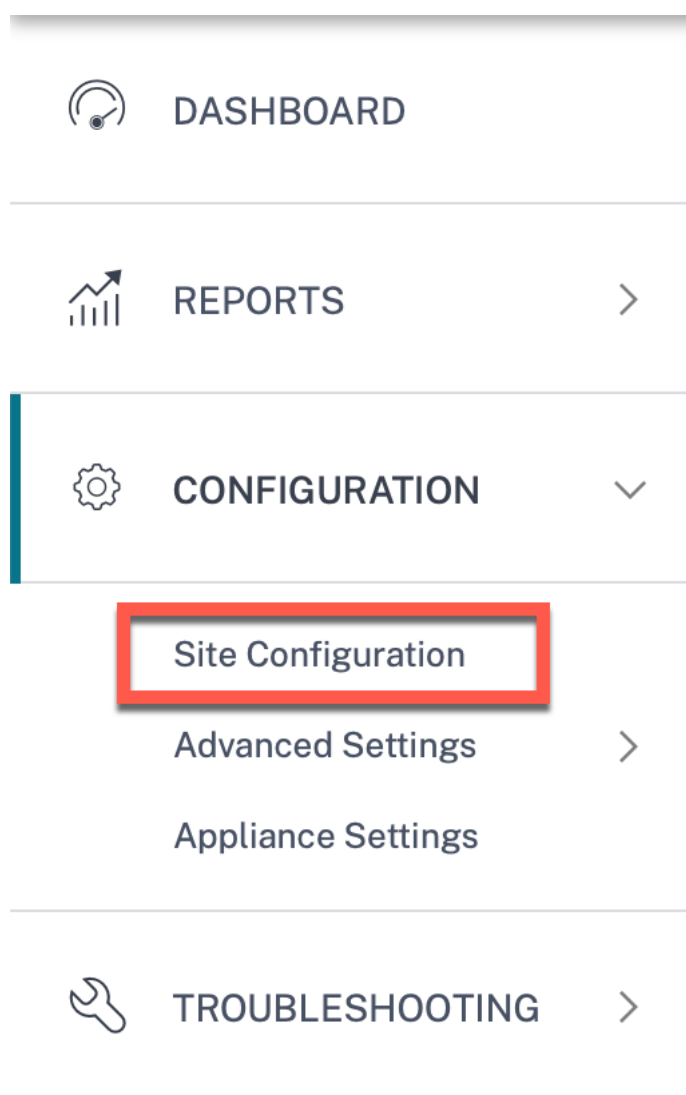
- Site Name ***: A text input field containing 'Bengaluru'.
- Site Type**: Two radio buttons, 'On-Premises' (selected) and 'Cloud Site'.
- Site Address ***: A text input field containing 'Bengaluru, Karnataka, India'. To the right of this field is a checkbox labeled 'Lat/Lng' which is checked.
- Latitude ***: A text input field containing '12.9715987'.
- Longitude ***: A text input field containing '77.5945627'.

At the bottom of the form, there are two buttons: 'Cancel' and 'Next'.

You can create a site from scratch, or use a [site profile](#) to configure a site quickly.

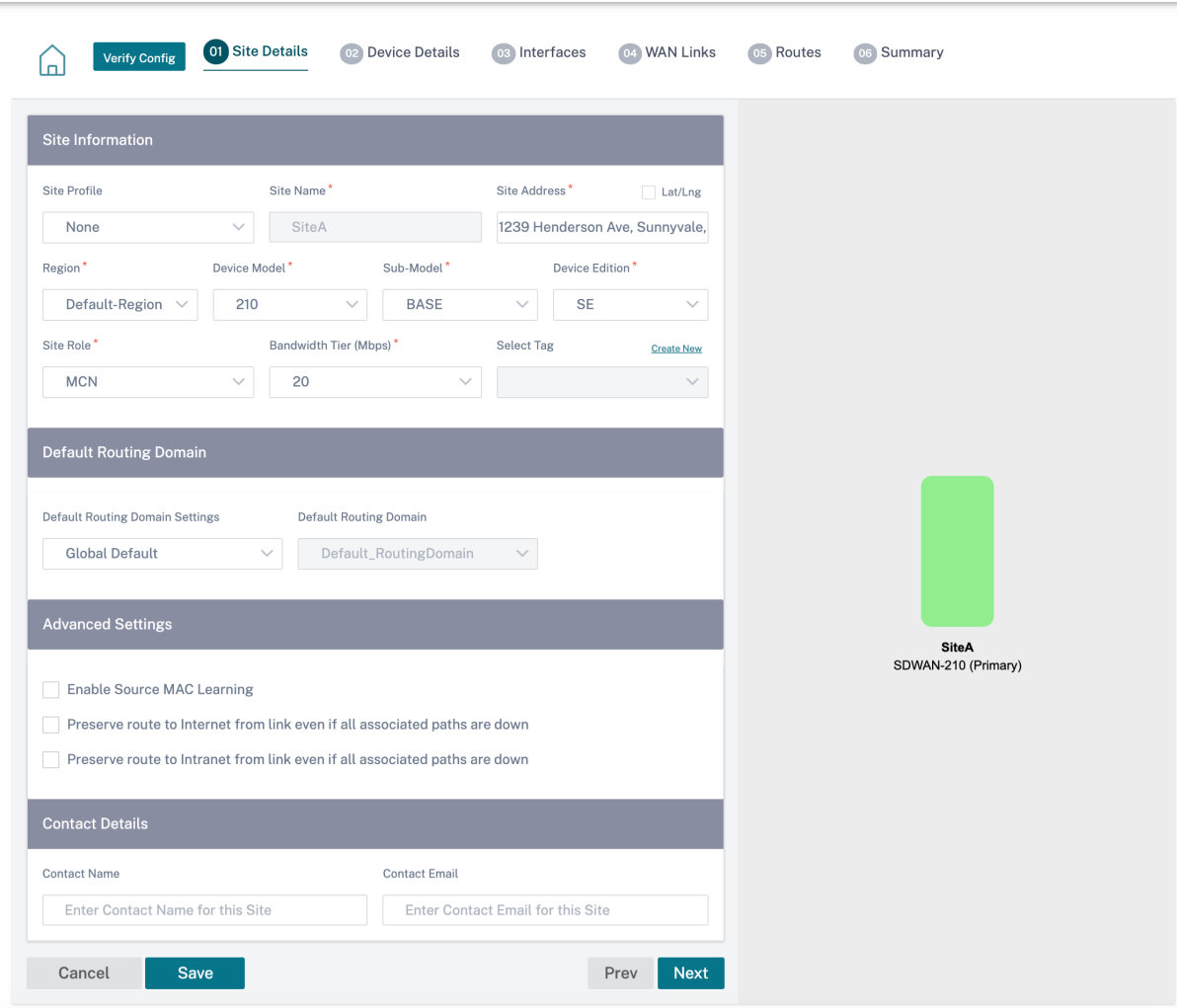
A graphical display to the right of the screen provides a dynamic topology diagram as you proceed with the configuration.

To view site configuration, select site and navigate to **Configuration > Site Configuration**.



Site details

The first step involves entering the site, device, advanced settings, and site contact details.



Site Information

Site Profile: None | Site Name: SiteA | Site Address: 1239 Henderson Ave, Sunnyvale, | ☐ Lat/Lng

Region: Default-Region | Device Model: 210 | Sub-Model: BASE | Device Edition: SE

Site Role: MCN | Bandwidth Tier (Mbps): 20 | Select Tag: [Create New](#)

Default Routing Domain

Default Routing Domain Settings: Global Default | Default Routing Domain: Default_RoutingDomain

Advanced Settings

- ☐ Enable Source MAC Learning
- ☐ Preserve route to Internet from link even if all associated paths are down
- ☐ Preserve route to Intranet from link even if all associated paths are down

Contact Details

Contact Name: Enter Contact Name for this Site | Contact Email: Enter Contact Email for this Site

Cancel Save Prev Next

SiteA
SDWAN-210 (Primary)

Site information

- Choosing a **Site Profile** auto-populates the site, interface, and WAN links parameters based on the site profile configuration.
- **Site Address** and **Site Name** are auto-populated based on the details provided in the previous step.
- Enable the **Lat/Lng** check box to get the latitude and longitude of a site.
- Select the **Region** from the drop-down list.
- **Device Model** and **Sub-Model** can be picked based on the hardware model or virtual appliance used at a given site.
- **Device Edition** reflects automatically based on the selected device model. Currently, Premium Edition (PE), Advanced Edition (AE), and Standard Edition (SE) are supported. The PE model is

only supported on 1100, 2100, 5100, and 6100 platforms. The AE model is supported on 210 and 1100 platforms.

Note

SD-WAN Orchestrator for On-premises does not support Advanced Edition and Premium Edition platforms.

- **Site Role** defines the role of the device. You can assign one of the following roles to a site:
 - **MCN**: Master Control Node (MCN) serves as the controller of the network, and only one active device in a network can be designated as the MCN.
 - **Branch**: Appliances at the branch sites that receive configuration from the MCN and participate in establishing virtual WAN functionalities to the branch offices. There can be multiple branch sites.
 - **RCN**: Regional Control Node (RCN) supports hierarchical network architecture, enabling multi-region network deployment. MCN controls multiple RCNs and each RCN, in turn, controls multiple branch sites.
 - **Geo-redundant MCN**: A site in a different location, that takes over the management functions of the MCN, if it is not available, ensuring disaster recovery. Note the geo-redundant MCN does not provide High Availability or failover capabilities for the MCN.
 - **Geo-Redundant RCN**: A site in a different location, that takes over the management functions of the RCN, if it is not available, ensuring disaster recovery. Note the geo-redundant RCN does not provide High Availability or failover capabilities for the RCN.
- **Bandwidth Tier** is the billable bandwidth capacity you can configure on any device, depending on the device model. For instance, the SD-WAN 410 Standard Edition (SE) appliance supports 20, 50, 100, 150, and 200 Mbps bandwidth tiers. Depending on your bandwidth needs for a given site, you can select the desired tier. Each site is billed for the configured bandwidth tier.

Routing domain

The **Routing Domain** section allows you to select the default routing domain for the site. **Routing Domain** settings can either be global or site specific. If you select **Global Defaults**, the default routing domain that is applicable globally is auto-selected. If you select **Site Specific**, you can select the default routing domain from the **Routing Domain** drop-down list.

Advanced settings

- **Enable Source MAC Learning**: Stores the source MAC address of received packets so that outgoing packets to the same destination can be sent to the same port.
- **Preserve route to Internet from link even if all associated paths are down**: When enabled, the packets destined for the internet service continue to choose the internet service even if all

WAN Links for the internet service are unavailable.

- **Preserve route to Intranet from link even if all associated paths are down:** When enabled, the packets destined for the intranet service continue to choose the intranet service even if all WAN Links for the intranet service are unavailable.
- Contact details of the admin available at the site.

A dynamic network diagram to the right of the configuration panel, provides visual feedback on an ongoing basis, as you go through the configuration process.

Device details

The device details section allows you to configure and enable High Availability (HA) at a site. With HA, two appliances can be deployed at a site as an active primary and a passive secondary. The secondary appliance takes over when the primary fails. For more information, see [High Availability](#).

Device Information

☒ Enable HA

Primary Device Serial Number: OGGPTUSRTW Short Name: Primary

Secondary HA Device Serial Number: OFTKNSTUXY HA Device Short Name (Optional): Secondary

Advanced HA Settings

Failover Time (ms): 1000 Shared Base MAC: AA:AA:AA:00:00:00

☐ Primary Reclaim

☐ HA Fail-to-Wire Mode

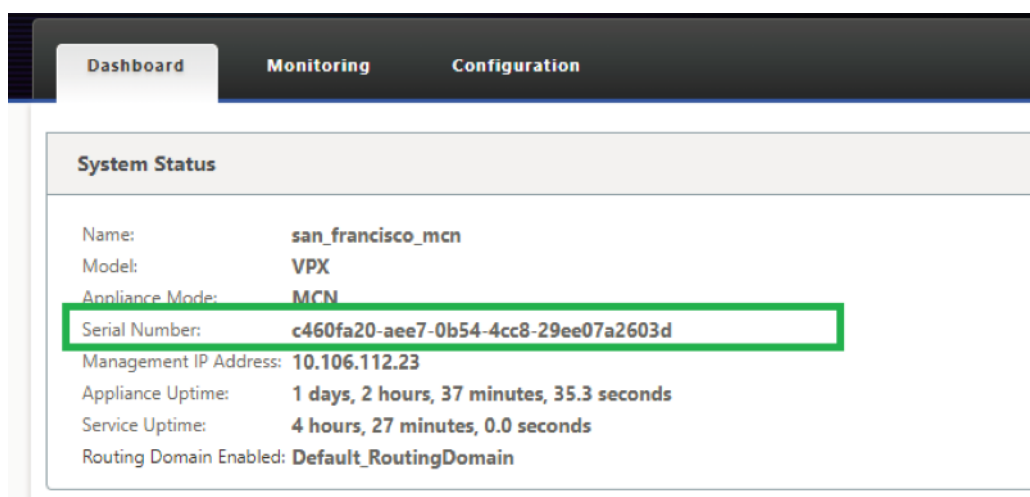
Cancel Save Prev Next

SiteA
SDWAN-210 (Primary)

Device information

Enable HA and enter the serial number and a short name for the primary and the secondary appliances.

- **Serial Number:** The **Serial Number** of a virtual SD-WAN instance (VPX) can be accessed from the VPX web console, as highlighted in the following screen-shot. A serial number of a hardware appliance can be found on the device label too.



- **Short Name:** The **Short Name** field is used to specify an easily identifiable short name for a site or to tag a site if desired.

Advanced HA settings

- **Failover Time (ms):** The wait time after contact with the primary appliance is lost, before the standby appliance becomes active.
- **Shared base MAC:** The shared MAC address for the high availability pair appliances. When a failover occurs, the secondary appliance has the same virtual MAC addresses as the failed primary appliance.
- **Disable Shared Base MAC:** This option is available on hypervisor and cloud based platforms only. Choose this option to disable the shared virtual MAC address.
- **Primary Reclaim:** The designated primary appliance reclaims control upon restart after a failover event.
- **HA Fail-to-Wire Mode:** The HA Fail-to-wire mode is enabled. For more details, see [HA deployment modes](#).
- **Enable Y-Cable Support:** The Small Form-factor Pluggable (SFP) ports can be used with a fiber optic Y-Cable to enable the high availability feature for Edge Mode deployment. This option is available on Citrix SD-WAN 1100 SE/PE appliances only. For more information, see [Enable Edge Mode High Availability Using Fiber Optic Y-Cable](#).

Wi-Fi details

You can configure a Citrix SD-WAN appliance that supports Wi-Fi as a Wi-Fi Access Point.

The following two variants of Citrix SD-WAN 110 platform support Wi-Fi and can be configured as a Wi-Fi access point:

- Citrix SD-WAN 110-WiFi-SE

- Citrix SD-WAN 110-LTE-WiFi

For more details on Wi-Fi configuration, see [Wi-Fi Access Point](#)

Interfaces

The next step is to add and configure the interfaces. Click **+ Interface** to start configuring the interface. Click **+ HA Interface** to start configuring HA interface. The **+ HA Interface** option is available only if you have configured a secondary appliance for high availability.

Interface configuration involves selecting the deployment mode and setting the interface level attributes. This configuration is applicable to both LAN and WAN links.

In-band management

In-band management allows you to use the SD-WAN data ports for management. It carries both data and management traffic, without having to configure an extra management path. In-band manage-

ment allows virtual IP addresses to connect to management services such as web UI and SSH. You can access the web UI and SSH using the management IP and in-band virtual IPs.

To enable in-band management, choose an IPv4 address from the **InBand Management IP** drop-down list or an IPv6 address from the **InBand Management IPv6** drop-down list. Select the DNS proxy to which all DNS requests over the in-band and backup management plane is forwarded to from the **InBand Management DNS** or **InBand Management DNS V6** drop-down list.

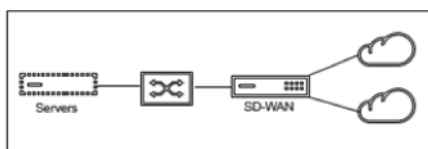
For more information on in-band management, see [In-band management](#).

The IP addresses configured for interfaces get listed under the **InBand Management IP** drop-down list. The DNS proxy services configured under **Advanced Settings > DNS** get listed in the **InBand Management DNS** drop-down list.

Interface attributes

The following deployment modes are supported:

1. Edge (Gateway)
 2. Inline – Fail-to-wire, Fail-to-block, and Virtual inline.
- **Deployment Mode:** Select one of the following deployment modes.
 - **Edge (Gateway):**



Gateway Mode implies SD-WAN serves as the “gateway” to the WAN for all the LAN traffic. The **Gateway Mode** is the default mode. You can deploy the appliance as a gateway on the LAN side or the WAN side.

- **Inline:**

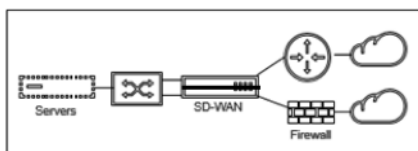
When SD-WAN is deployed in-line between a LAN switch and a WAN router, SD-WAN is expected to “bridge” LAN and WAN.

All the Citrix SD-WAN appliances have pre-defined bridge-paired interfaces. With “Bridge” option enabled, selection of any interface on the LAN end automatically highlights the paired interface that is reserved for the WAN end of the bridge. For example, physical interfaces 1 and 2 are a bridged pair.

- **Fail-To-Wire:** Enables a physical connection between the bridged pair of interfaces, allowing traffic to bypass SD-WAN and flow directly across the bridge in the event of appliance restart or failure.

Note

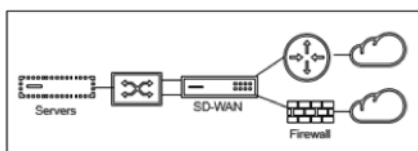
Inline (Fail-to-Wire) option is available only on hardware appliances and not on virtual appliances (VPX / VPXL).



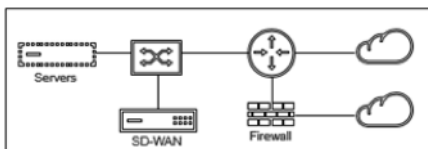
- ★ **Fail-to-Block:** This option disables the physical connection between the bridged pair of interfaces on hardware appliances, preventing traffic from flowing across the bridge in the event of appliance restart or failure.

Note

Inline (Fail-to-Block) is the only bridge mode option available on virtual appliances (VPX / VPXL).



- ★ **Virtual Inline (One-Arm):**



When SD-WAN is deployed in this mode, it has a **single arm** connecting it to the WAN router, LAN, and WAN sharing the same interface on SD-WAN. Therefore, the interface settings are shared between the LAN and WAN links.

- **Interface Type:** Select the interface type from the drop-down list.
- **Security (Trusted / Untrusted):** Specifies the security level of the interface. Trusted segments are protected by a Firewall.
- **Interface Name:** Based on the selected deployment mode, the **Interface Name** field is auto filled.

Physical interface

- **Select Interface:** Select the configurable Ethernet port that is available on the appliance.

Virtual interface

- **VLAN ID:** The ID for identifying and marking traffic to and from the interface.
- **Virtual Interface Name:** Based on the selected deployment mode, the **Virtual Interface Name** field is auto filled.
- **Enable HA Heartbeat:** Enable syncing of HA heartbeats over this interface. This option is enabled if you have configured a secondary appliance for HA. Select this option to allow primary and secondary appliances to synchronize the HA heartbeats over this interface. Specify the IP address of the primary and secondary appliance.
- **Routing Domain:** The routing domain that provides a single point of administration of the branch office network, or a data center network.
- **Firewall Zones:** The firewall zone to which the interface belongs. Firewall zones secure and control the interfaces in the logical zone.
- **Client Mode:** Select **Client Mode** from the drop-down list. On selection of PPPoE Static displays more settings.

Note:

When the Site mode (under Site Details tab) is selected as **Branch** and the **Security field** (under **Interface** tab) is selected as **Untrusted**, the **PPPoE Dynamic** option is available under **Client Mode**.

Citrix SD-WAN act as a PPPoE client. It authenticates with the PPPoE server and obtains dynamic IP address, or uses static IP address to establish PPPoE connections.

- **DHCP Client:** When enabled on the virtual interfaces, the DHCP Server assigns dynamically IPv4 addresses to the connected client.
- **DHCP IPv6 Client:** When enabled on the virtual interfaces, the DHCP Server dynamically assigns IPv6 addresses to the connected client.
- **SLAAC:** This option is available only for IPv6 addresses. When selected, the interface obtains IPv6 addresses through Stateless Address Auto-configuration (SLAAC).
- **Directed Broadcast:** When the **Directed Broadcast** check box is selected, the directed broadcasts are sent to the virtual IP subnets on the virtual interface.
- **Enabled:** By default, the **Enabled** check box is selected for all virtual interfaces. If you want to disable the virtual interface, clear the **Enabled** check box.

Note

- The **Enabled** check box is available only from Citrix SD-WAN release 11.3.1 onwards.
- The option to disable a virtual interface is only available when it is not used by a WAN

Link Access Interface. If the virtual interface is used by a WAN Link Access Interface, then the check box is read-only and selected by default.

- While configuring other features, along with enabled virtual interfaces, the disabled virtual interfaces also get listed, except under **Access Interfaces** for a **WAN Link**. Even if you select a disabled virtual interface, the virtual interface is not considered and does not impact the network configuration.

- **+ IPv4 Address:** The virtual IPv4 address and netmask of the interface.
- **+ IPv6 Address:** The virtual IPv6 address and prefix of the interface.
- **Identity:** Choose an identity to be used for IP services. For example, **Identity** is used as the Source IP Address to communicate with BGP neighbors.
- **Private:** When enabled, the Virtual IP Address is only routable on the local appliance.

Note

- LTE ports do not support static IP addresses (IPv4 and IPv6).
- LTE ports support both DHCP and SLAAC. Configuring DHCPv4 or DHCPv6 is mandatory. SLAAC is optional.
- In LTE ports, Link-Local addresses can be configured for IPv6 or SLAAC.

PPPoE credentials

Point-to-Point Protocol over Ethernet (PPPoE) connects multiple computer users on an Ethernet LAN to a remote site through common customer premises appliances.

Citrix SD-WAN appliances use PPPoE to provide support to the ISP to have ongoing and continuous DSL and cable modem connections unlike dialup connections. For more information, see [PPPoE configuration](#).

Virtual Interfaces

VLAN ID *	Virtual Interface Name *	
<input type="text" value="0"/>	<input type="text" value="VIF-1-LAN-1"/>	<input type="checkbox"/> Enable HA Heartbeat
Routing Domain *	Firewall Zones	Client Mode
<input type="text" value="Default_RoutingDomain"/>	<input type="text" value="Internet_Zone"/>	<input type="text" value="PPPoE Static"/>
AC Name	Service Name	Reconnect Hold Off (s)
<input type="text" value="test-ac-name"/>	<input type="text" value="test-service-name"/>	<input type="text" value="0"/>
Username *	Password *	Auth
<input type="text" value="test-username"/>	<input type="password" value="....."/>	<input type="text" value="Auto"/>

Note : Converting Virtual Interface to PPPoE will clear any Gateway IP Address and Virtual IP. Address (in case of PPPoE Dynamic only) associate with it under access interfaces

☐ DHCP Client
 ☐ SLAAC
 ☐ Directed Broadcast

- **AC Name:** Provide the Access Concentrator (AC) name for the PPPoE configuration.
- **Service Name:** Enter a service name.
- **Reconnect Hold Off (s):** Enter the reconnect attempt hold off time.
- **User Name:** Enter the user name for the PPPoE configuration.
- **Password:** Enter the password for the PPPoE configuration.
- **Auth:** Select the authorization protocol from the drop-down list.
 - When the **Auth** option is set to Auto, the SD-WAN appliance honors the supported authentication protocol request received from the server.
 - When the **Auth** option is set to PAP/CHAP/EAP, then only specific authentication protocols are honored. If PAP is in the configuration and the server sends an authentication request with CHAP, the connection request is rejected. If the server does not negotiate with PAP, an authentication failure occurs.

Tip

Optionally, create subinterfaces to add multiple VLANs.

Continue to add interfaces as per your network requirement.

Wired 802.1X configuration

Wired 802.1X is an authentication mechanism that requires clients to authenticate before being able to access the LAN resources. Citrix SD-WAN Orchestrator service supports configuring wired 802.1X

authentication on LAN interfaces.

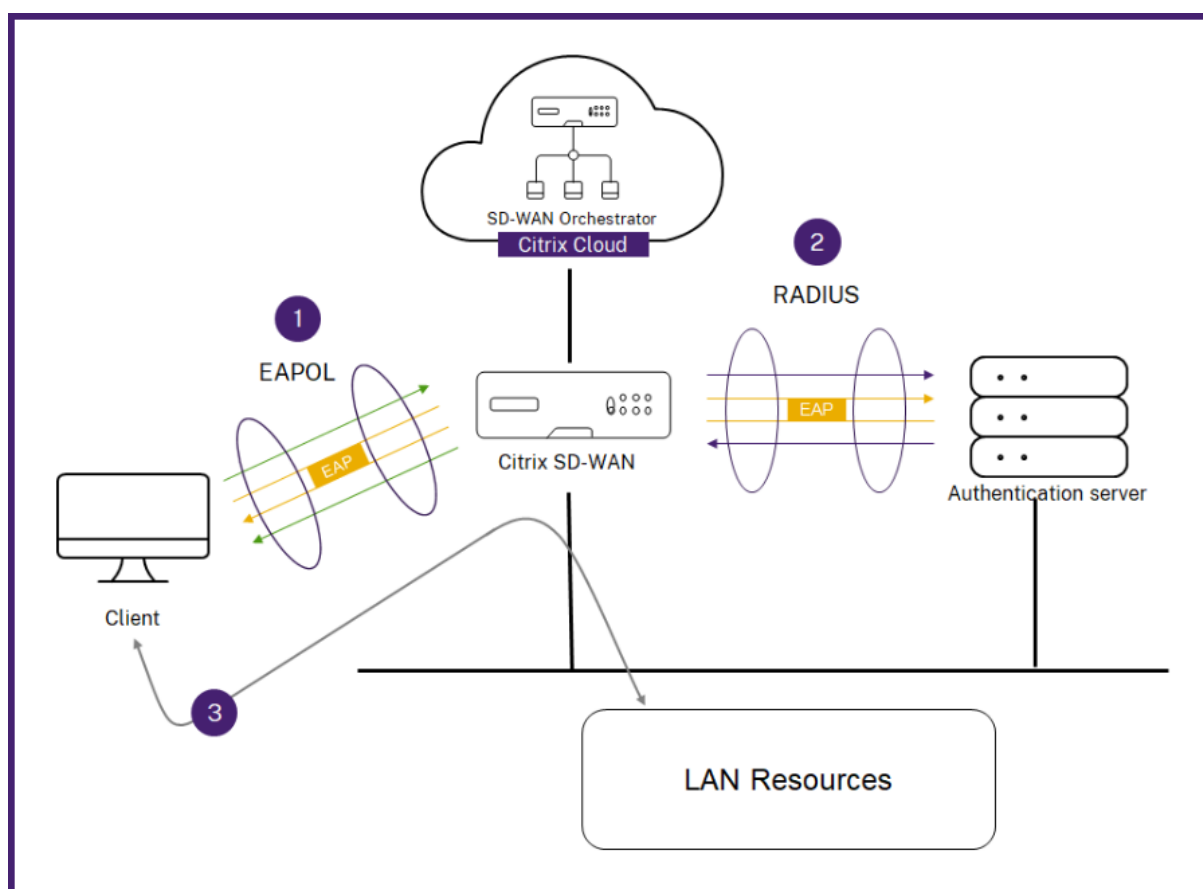
In the Citrix SD-WAN network, the clients send authentication requests to the Citrix SD-WAN appliance to access the LAN resources. The Citrix SD-WAN appliance acts as an authenticator and sends the authentication requests to the authentication server. Citrix SD-WAN Orchestrator service supports only RADIUS servers to be configured as authentication servers.

When authenticating for the first time, only EAPOL packets can be processed or DHCP packets that can initialize the 802.1X authentication from the default virtual LAN. A newly connected client must be authenticated within 90 seconds. If the authentication is successful, it gets access to the LAN resources.

If the authentication fails, the client is not granted network access and all packets are dropped. The clients that are directly connected to the Citrix SD-WAN appliance can retry authentication by unplugging the Ethernet cable and reinserting it. Optionally, you can define a specific virtual LAN to grant access to limited LAN resources for the failed authentication requests. In such cases, the failed authentication requests get access to the specified virtual LAN. You can restrict access to the authenticated traffic using different routing domains or firewall zones while creating the virtual LAN.

Note

- The default virtual LAN must always have 802.1X enabled.
- Dynamic virtual LANs are not supported.



The Citrix SD-WAN appliance expects to receive packets without an 802.1Q tag (untagged packets). If the Citrix SD-WAN appliance receives a packet with an 802.1Q tag set to the assigned virtual LAN, then all the packets originated from the MAC must be tagged. If a packet is received with no 802.1Q tag in the header or with a tag other than the virtual LAN that the MAC address belongs to, then the packet is dropped.

When multiple clients connected to a switch try to authenticate at the same time over a single port, each client is authenticated individually, before it can gain access to the LAN resources. The clients that fail to authenticate can retry authentication by unplugging the Ethernet cable, waiting for 3 minutes, and reinserting the Ethernet cable. Citrix SD-WAN 110, 210, and 400 platforms support a maximum of 32 clients (both authenticated and unauthenticated). All other platforms support a maximum of 64 clients (both authenticated and unauthenticated).

To configure 802.1X authentication, navigate to **Site Configuration > Interfaces** and turn on the **Enable 802.1x** toggle button. Select an existing RADIUS profile or click **Create RADIUS Profile** to create a RADIUS profile. For details on creating a RADIUS profile, see [RADIUS server profiles](#). You can use the same RADIUS profile(s) for wired 802.1x and wireless WPA2-enterprise authentication, provided your appliance supports wireless WPA2-enterprise.

Select a virtual interface from the **Authenticated VIF** drop-down list. The selected virtual interface grants access to the LAN resources for successful authentication requests.

Optionally, you can select an interface from the **Unauthenticated VIF** drop-down list. The selected virtual interface grants access to a specific LAN resource for the failed authenticated requests.

You can add a list of MAC addresses which bypasses the authentication process. Traffic from these MAC addresses will be implicitly treated as authenticated. These MAC addresses are susceptible to malicious attacks. So, use this capability only in physically secure environments and for legacy hardware that does not support wired 802.1x authentication.

The screenshot shows the 'Wired 802.1X Configuration' page. At the top, there is a toggle switch for 'Enable 802.1x' which is turned on. Below this is an information box stating: 'When enabled 802.1x Configuration will be applied to supported ports only.' The page is divided into three main sections: 'RADIUS Profiles', 'Virtual Interfaces', and 'MAC Address Bypass'. The 'RADIUS Profiles' section has two columns: 'Primary RADIUS Profile' with a dropdown menu showing 'PiFreeRADIUS' and a 'Create Radius Profile' link, and 'Secondary RADIUS Profile' with a dropdown menu showing 'Select Radius Profile' and a 'Create Radius Profile' link. The 'Virtual Interfaces' section has two columns: 'Authenticated VIF' with a dropdown menu showing '101' and 'Unauthenticated VIF' with a dropdown menu showing '100'. The 'MAC Address Bypass' section has a text input field labeled 'Enter a MAC Address to byapss' (note the typo) and an 'Add' button. Below this is a table with two columns: 'MAC Address Bypass Value' and 'Actions'.

MAC Address Bypass Value	Actions
--------------------------	---------

You can view the alerts associated with wired 802.1x authentication requests under **Reports > Alerts**. For more information, see [Alerts](#).

WAN links

The next step is to configure WAN links. Click **+ WAN Link** to start configuring a WAN link.

WAN link configuration involves setting up the WAN link access type and access interface attributes.

You can configure the **WAN link** attribute from scratch, or use a [WAN link profile](#) to configure WAN link attributes quickly. If you have already used a site profile, the **WAN link** attributes auto-populate.

WAN link attributes

Home

Verify Config

01 Site Details

02 Device Details

03 Interfaces

04 WAN Links

05 Routes

06 Summary

WAN Link Attributes

Access Type *

Public Internet

ISP Name *

Captive Audience

☐ Custom

Internet Category

Broadband

Link Name *

Broadband-Captive_Audience-

Tracking IP Address

Public IPv4 Address

☐ Auto Detect

E.g. a.b.c.d

Public IPv6 Address

E.g. 2001:0db8:85a3:0000:0000:8a2e:0370:7334

Egress

Speed *

100

Mbps

Permitted Rate

☐ Auto Learn

☒ Physical Rate

100

Ingress

Speed *

100

Mbps

Permitted Rate

☐ Auto Learn

☒ Physical Rate

100

Access Interfaces

Access Interface Name

AIF-1

Virtual Interface *

Select Virtual Interface

Virtual Path Mode *

Primary

IP Address *

E.g. a.b.c.d

☒ V4

☐ V6

Gateway IP Address *

E.g. a.b.c.d

☒ Bind Access Interface to Gateway MAC

☐ Enable Proxy ARP

Enable Internet Access on Routing Domain(s)

None

Done

Services

Service Bandwidth Settings :

Global Defaults

Virtual Path Settings for the Link

Relative Bandwidth Provisioning across Virtual Paths :

Global Defaults

Advanced WAN Options

☐ Enable Metering

☐ Adaptive Bandwidth Detection

Congestion Threshold (µs)

20000

Provider ID

Frame Cost (Bytes)

1

Standby Mode

Disabled

MTU (Bytes)

1350

Eligibility

	LAN to WAN	WAN to LAN
Real Time	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Interactive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Bulk	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Cancel

SiteA

SDWAN-210 (Primary)

- **Access Type:** Specifies the WAN connection type of the link.
 - **Public Internet:** Indicates the link is connected to the Internet through an ISP.
 - **Private Intranet:** Indicates the link is connected to one or more sites within the SD-WAN network and cannot connect to locations outside the SD-WAN network.
 - **MPLS:** Specialized variant of Private Intranet. Indicates the link uses one or more DSCP tags to control the Quality of Service between two or more points on an Intranet and cannot connect to locations outside of the SD-WAN network.
- **ISP Name:** The name of the service provider.
- **Link Name:** Auto-populated based on the previous inputs.
- **Tracking IP Address:** The Virtual IP Address on the Virtual Path that can be pinged to determine the state of the path.
- **Public IPv4 Address** and **Public IPv6 Address:** The IP address of the NAT or DNS Server. This address is applicable and exposed, only when the WAN link access type is Public Internet or Private Intranet in Serial HA deployment. Public IP can either be manually configured or auto-learned using the Auto Learn option.
- **Auto Detect:** When enabled, the SD-WAN appliance automatically detects the public IP address. This option is available only when the device role is a **branch** and not the **Master Control Node (MCN)**.
- **Egress Speed:** The WAN to LAN speed.
 - **Speed:** The available or allowed speed of the WAN to LAN traffic in Kbps or Mbps.
 - **Permitted Rate:** In cases where the entire WAN link capacity is not supposed to be used by the SD-WAN appliance, change the permitted rate accordingly.
 - **Auto Learn:** When you are unsure of the bandwidth and if the links are non-reliable, you can enable the Auto Learn feature. The Auto Learn feature learns the underlying link capacity only, and uses the same value in the future.
 - **Physical Rate:** The actual bandwidth capacity of the WAN link.
- **Ingress Speed:** The LAN to WAN speed.
 - **Speed:** The available or allowed speed of the LAN to WAN traffic in Kbps or Mbps.
 - **Permitted Rate:** In cases where the entire LAN link capacity is not supposed to be used by the SD-WAN appliance, change the permitted rate accordingly.
 - **Auto Learn:** When you are unsure of the bandwidth and if the links are non-reliable, you can enable the Auto Learn feature. The Auto Learn feature learns the underlying link capacity only, and uses the same value in the future.
 - **Physical Rate:** The actual bandwidth capacity of the LAN link.

MPLS Queues

The **MPLS queue** settings are available for WAN link access type MPLS only. This option is meant to enable definition of queues corresponding to the Service Provider MPLS queues, on the MPLS WAN Link. For more information, see [MPLS Queues](#).

MPLS Queues

Queue Name: MPLS-Captive_Audience-QUEUE-1

DSCP Tag *

default
▼

LAN to WAN (%) *

50

WAN to LAN (%) *

50

Tracking IP Address

a.b.c.d

Congestion Threshold (μs)

20000

☒ Unmatched ☐ No Retag

Eligibility :

	LAN to WAN	WAN to LAN
Real Time	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Interactive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Bulk	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Cancel

Save

Following are the queue parameters:

- **Queue Name:** The name of the MPLS queue.
- **DSCP Tag:** The unique **Differentiated Services Code Point(DSCP)** tag of the MPLS queue.
- **LAN to WAN (%):** The proportion (%) of bandwidth used for upload cannot exceed the defined physical upload rate.
- **WAN to LAN (%):** The proportion (%) of bandwidth used for download cannot exceed the defined physical download rate.
- **Tracking IP Address:** The Virtual IP Address on the Virtual Path that can be pinged to determine the state of the path.
- **Congestion Threshold:** The amount of congestion (in microseconds) after which the MPLS Queue throttles packet transmission to avoid further congestion.
- **Unmatched option:** If enabled, DSCP tags not matched by other MPLS Queues would use this Class. Only one MPLS Queue can be marked for use by unmatched tags.
- **No retag option:** If enabled, the LAN to WAN intranet traffic retains the original tag and no retag with the default DSCP tag.
- **Eligibility:** The eligibility settings for an MPLS Queue allow the user to add an extra penalty for using the MPLS Queue for certain Classes of traffic. When a Class of traffic is marked as not-eligible for the MPLS Queue, a penalty is added that makes the WAN Link unlikely to be used unless network conditions require it.

Access Interface

An Access Interface defines the IP Address and Gateway IP Address for a WAN Link. At least one Access Interface is required for each WAN Link. The following are the access interface parameters:

- **Access Interface Name:** The name by which Access interface is referenced. The default uses the following naming convention: WAN_link_name-AI-number: Where WAN_link_name is the name of the WAN link you are associating with this interface, and number is the number of Access Interfaces currently configured for this link, incremented by 1.
- **Virtual Interface:** The Virtual Interface that the Access Interface uses. Select an entry from the drop-down menu of Virtual Interfaces configured for the current branch site.
- **Virtual Path Mode:** Specifies the priority for Virtual Path traffic on the current WAN link. The options are: Primary, Secondary, or Exclude. If set to Exclude, the Access Interface is used for Internet and Intranet traffic, only.
- **IP Address:** The IP Address for the Access Interface endpoint from the appliance to the WAN. Select V4 (IPv4) or V6 (IPv6) as required.
- **Gateway IP Address:** The IP Address for the gateway router.
- **Bind Access Interface to Gateway MAC:** If enabled, the source MAC address of packets received on Internet or Intranet services must match the gateway MAC address. [WAN Links > Advances WAN Options](#).
- **Enable Proxy ARP:** If enabled, the Virtual WAN Appliance replies to ARP requests for the Gateway IP Address, when the gateway is unreachable.
- **Enable Internet Access on Routing Domain(s):** Auto-creates a DEFAULT route (0.0.0.0/0) in all the routing tables of the respective routing domains. You can enable for ALL routing domains or NONE. It avoids the need for creating exclusive static route across all the routing domains if they needed internet access.

Services

The **Services** section allows you to add service types and allocate the percentage of bandwidth to be used for each service type. You can define the service types and configure attributes for it from the [Delivery services](#) section. You can choose to use these global defaults or configure link specific service bandwidth settings from the **Service Bandwidth Settings** drop-down list. If you choose link specific, enter the following details:

- **Service Name:** The name of the WAN link service.
- **Allocation %:** The guaranteed fair share of bandwidth allocated to the service from the link's total capacity.
- **Mode:** The operation mode of the WAN Link, based on the service selected. For Internet, there is one of Primary, Secondary, and Balance and for Intranet there is Primary and Secondary.
- **LAN to WAN Tag:** The DHCP tag to apply to LAN to WAN packets on the service.
- **WAN to LAN Tag:** The DHCP tag to apply to WAN to LAN packets on the service.

- **WAN to LAN Match:** The match criteria for Internet WAN to LAN packets to get assigned to the service.
- **LAN to WAN Delay:** The maximum time, to buffer packets when the WAN Links bandwidth is exceeded.
- **Tunnel Header Size:** The size of the tunnel header, in bytes.
- **WAN to LAN Grooming:** If enabled, packets are randomly discarded to prevent WAN to LAN traffic from exceeded the Service's provisioned bandwidth.

Services

Service Bandwidth Settings : Link Specific ▾

Service Name

Allocation %

Mode

internet ▾

50

primary ▾

Tunnel Header Size (bytes)

0

☒ Access Inteface Failover

LAN to WAN

Tagging

Max Delay (ms)

None ▾

500

WAN to LAN

Tagging

Matching

Default ▾

Default ▾

☒ Grooming

Cancel

Done

Virtual Path settings for the link

Select the relative bandwidth provisioning across virtual paths as **Global Default** or **Link Specific** as required. On selecting **Link Specific**, when you enable the auto-bandwidth provisioning, the share of the bandwidth for the virtual path service is automatically calculated and applied accordingly to the magnitude of bandwidth that might be consumed by remote sites.

- **Max to Min Virtual Path Bandwidth Ratio for the Link:** You can set the maximum to minimum virtual path ratio that can be applied to the selected WAN link.

- **Minimum Reserved Bandwidth for each Virtual Path (Kbps):** You can set the minimum reserved bandwidth value in Kbps for each virtual path.

Virtual Path Settings for the Link

Relative Bandwidth Provisioning across Virtual Paths : Link Specific ▾

☒ Enable Auto-Bandwidth Provisioning across all Virtual paths associated with the link

Max to Min Virtual Path Bandwidth Ratio for the Link *

10

Minimum Reserved Bandwidth for each Virtual Path (Kbps) *

80

Advanced WAN options

The WAN Link Advanced Settings allows the configuration of the **ISP specific** attributes.

- **Congestion Threshold:** The amount of congestion after which the WAN link throttles packet transmission to avoid further congestion.
- **Provider ID:** Unique Identifier for the provider to differentiate paths when sending duplicate packets.
- **Frame Cost (Bytes):** Extra header/trailer bytes added to every packet, such as for Ethernet IPG or AAL5 trailers.
- **MTU (Bytes):** The largest raw packet size in bytes, not including the Frame Cost.
- **Standby Mode:** A standby link is not used to carry user traffic unless it becomes active.
 - **Disabled:** The standby mode of a WAN link is disabled by default.
 - **On-Demand:** An on-demand standby WAN link will also become active if all non-standby WAN links are dead or disabled.
 - **Last-Resort:** A last-resort standby WAN link becomes active only when all non-standby WAN links and all on-demand standby WAN links are dead or disabled.

1 ! [Advanced wan option] (/en-us/citrix-sd-wan-orchestrator/media/advanced-wan-option.png)

- **Enable Metering:** Tracks usage on a WAN link and alerts the user when the link usage exceeds the configured data cap.

- **Data Cap (MB):** The maximum data threshold in MB.
- **Billing Cycle:** The billing frequency, weekly or monthly.
- **Starting From:** The date from which the billing cycle starts.
- **Approximate Data Already Used:** The approximate data already used in MB for the metered link. This is applicable only for the first cycle. To track the proper metered link usage, specify the approximate metered link usage, if the link has already been used for few days in the current billing cycle.
- **Disable link if Data Cap Reached:** If the data usage reaches the specified data cap, the metered link and all its related paths are disabled until the next billing cycle. If this option is not selected, the metered link remains in the current state, after the data cap is reached, until the next billing cycle.

For more information, see [Metering and Standby WAN Links](#).

- **Adaptive Bandwidth Detection:** Uses the WAN link at a reduced bandwidth rate when a loss is detected. When the available bandwidth is below the configured **Minimum Acceptable Bandwidth**, then the path marked as BAD. Use Custom Bad Loss Sensitivity under Path or Autopath group with Adaptive Bandwidth Detection.

Note

Adaptive Bandwidth Detection is available only for Client and not for MCN.

- **Minimum Acceptable Bandwidth:** When there is varying bandwidth rate, the percentage of WAN to LAN permitted rate below which the path is marked as BAD. The minimum kbps is different on each side of a virtual path. The value can be in the range 10%-50% and the default being 30%.

Routes

The next step in the site configuration workflow is to create routes. You can create application and IP routes based on your site requirements.

NOTE

The routes that were added before introducing the **Application Route** and **IP Route** tabs are listed under the **IP Routes** tab with **Delivery Service** as Internet.

The global routes and site-specific routes that are created at the network level automatically get listed under **Routes > Application Routes** and **Routes > IP routes** tabs. You can only view the global routes at the site level. To edit or delete a global route, navigate to network level configurations.

You can also create, edit, or delete routes at the site level.

Cost Ranges: Custom Application (1-20) Application (21-40) Application Group (41-60) IP (1-65535)

+ Application Route Search for Route

No	Match Type	Name	Delivery Service	Routing Domain	Sites	Cost	Actions
1	Application	EzTravel.com.tw	Internet Breakout	Any	Global	21	
2	Application Group	Default Cloud Dir...	Cloud Direct Service	Any	Global	45	
3	Application Group	Default SIA App ...	Secure Internet Access ...	Any	Global	45	
4	Application Group	O365Optimize_In...	Internet Breakout	Any	SiteA	50	
5	Application Group	O365Optimize_In...	Internet Breakout	Any	Global	50	

Application routes

Click **+ Application Route** to create an application route.

- **Custom Application Match Criteria:**
 - **Match Type:** Select the match type as **Application/Custom Application/Application Group** from the drop-down list.
 - **Application:** Choose one application from the drop-down list.
 - **Routing Domain:** Select a routing domain.
- **Traffic Steering**
 - **Delivery Service:** Choose one delivery service from the list.
 - **Cost:** Reflects the relative priority of each route. Lower the cost, the higher the priority.
- **Eligibility Based on Path:**

- **Add Path:** Choose a site and WAN links, both to and from. If the added path goes down, then the application route does not receive any traffic.

If a new application route gets added, then the route cost must be in the following range:

- Custom application: 1–20
- Application: 21–40
- Application group: 41–60

IP routes

Go to **IP Routes** tab and click **+ IP Route** to create the IP Route policy to steer traffic.

- **IP Protocol Match Criteria:**
 - **Destination Network:** Add the destination network that helps to forward the packets.
 - **Use IP Group:** You can add a destination network or enable the Use IP Group check box to select any IP group from the drop-down list.
 - **Routing Domain:** Select a routing domain from the drop-down list.
- **Traffic Steering**
 - **Delivery Service:** Choose one delivery service from the drop-down list.
 - **Cost:** Reflects the relative priority of each route. Lower the cost, the higher the priority.
- **Eligibility Criteria:**

- **Export Route:** If the Export Route check box is selected and if the route is a local route, then the route is eligible to be exported by default. If the route is an INTRANET/INTERNET based route, then for the export to work, WAN to WAN forwarding has to be enabled. If the Export Route check box is cleared, then the local route is not eligible to be exported to other SD-WAN and has local significance.
- **Eligibility based on Path:**
 - **Add Path:** Choose a site and WAN links, both to and from. If the added path goes down, then the IP route does not receive any traffic.

If a new IP route gets added, then the route cost must be in the 1–20 range.

Navigation: [Verify Config](#) | [01 Site Details](#) | [02 Device Details](#) | [03 Interfaces](#) | [04 WAN Links](#) | **[05 Routes](#)** | [06 Summary](#)

Application Routes | **IP Routes**

Cost Ranges: [Custom Application \(1-20\)](#) | [Application \(21-40\)](#) | [Application Group \(41-60\)](#) | [IP \(1-65535\)](#)

IP Protocol Match Criteria

Destination Network * ☒ Use IP Group Routing Domain

Traffic Steering

Delivery Service Cost *

Eligibility Criteria

☒ Export Route

Eligibility Based on Path

Add Path

Site Name	From Wan Link	To Wan Link	Actions
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Summary

This section provides a summary of the site configuration to enable a quick review before submitting the same.

[Verify Config](#)
01 Site Details
02 Device Details
03 Interfaces
04 WAN Links
05 Routes
06 **Summary**

Site & Device Details

Site Name	Device Model	Site Role	Serial Number	Bandwidth Tier
mymcn	VPX	MCN	3065cea3-f6b8...	1000 Mbps

Interfaces

LAN-1-1

- VLAN0-VIF-1-LAN-1-Default_RoutingDomain-192.168.1.1/24

WAN-1-2

- VLAN0-VIF-2-WAN-1-Default_RoutingDomain-172.16.1.2/24

WAN Links

Broadband-OTE-1-1000 Mbps

- 1000 Mbps↑ 1000 Mbps↓
- AlF-1-VIF-2-WAN-1-172.16.1.2-172.16.1.1-primary

Cancel Save Save as Profile Prev Done

Use the **Save as Template** option to save the site configuration as a template for reuse across other sites. Clicking **Done** marks completion of site configuration, and takes you to the **Network Configuration – Home** page to review all the sites configured. For more information, see [Network Configuration](#).

LTE firmware upgrade

December 16, 2020

SD-WAN Orchestrator for On-premises allows you to configure and manage all the LTE sites in your network. It includes appliances connected through an internal LTE modem or external USB LTE modem.

To configure the LTE sites in your network:

1. At the site level, navigate to **Configuration > Site Configuration**.

The screenshot shows the 'Site Details' configuration page. The 'Sub-Model' dropdown is highlighted with a red box and set to 'LTE'. Other fields include Site Name 'Site_210', Site Address 'Kolkata, West Bengal, India', Region 'Default-Region', Device Model '210', Device Edition 'SE', Site Role 'Branch', and Bandwidth Tier '200'.

2. Select the submodel as **LTE** along with other necessary details and click Save. For more information on site configuration, see [Site configuration](#).
3. Once the site is created, navigate to the **Network Configuration Home** page and click **Deploy Config/Software** button.

Network Configuration: Home

Software Version : 11.2.2.1005

Site Group: All

[+ Add Site](#)
[Batch Add Sites](#)
[Deploy Config/Software](#)
[Back Up/Review Checkpoints](#)
[More Actions ...](#)
[Deployment Tracker](#)

Availability	Cloud Connectivity	Site Name	Site Role	Device Model	Serial No	Bandwidth Tier	Management IP	Actions
●	● Inactive	Branch_Azure_VPXL	Branch	VPXL-SE		200	Unknown	Edit Copy More
●	● Inactive	RajanCube_210	Branch	210-SE		200	Unknown	Edit Copy More
●	● Inactive	Siva_1100_Branch	Branch	1100-SE		300	Unknown	Edit Copy More
●	● Inactive	Siva_2100_Branch	Branch	2100-SE		1000	Unknown	Edit Copy More
●	● Online	Site_210	Branch	210-SE		200	Unknown	Edit Copy More
●	● Online	Branch_VPX_Azure	Branch	VPX-SE	2867ACC5-DDFD-4105...	50	10.105.173.229	Edit Copy More
●	● Online	MCN_Azure	MCN	VPX-SE	0000-0017-0293-3041...	1000	172.20.0.4	Edit Copy More
●	● Online	Azure VPX Branch test	Branch	VPX-SE	0000-0015-9237-3615...	500	172.18.0.4	Edit Copy More
●	● Online	Site_210	Branch	210-SE	✓ GF04KD3EGW	100	10.140.3.67	Edit Copy More

Page Size: 200 Showing 1-9 of 9 items Page 1 of 1

C

Note

Currently, the LTE support is available on Citrix SD-WAN 210 appliances.

4. The **Software Version** field is auto filled with the latest software version package and the field is non-editable. Once you click **Stage**, it downloads all the appropriate LTE firmware for the selected software version.

Software Version : 11.2.2.1005

Stage ✓ **Activate** ✓ ☐ Ignore Incomplete

Staged Appliances 4/4

Activated Appliances 4/4

Total Appliances	Staged	Activated	Failed
4	4	4	0

Online	Site	Status	HA State	Software Version
Yes	MCN_Azure	Activation Complete	Not Configured	11.2.2.1005.888881
Yes	Azure_VPX_Branch_test	Activation Complete	Not Configured	11.2.2.1005.888881
Yes	Branch_VPX_Azure	Activation Complete	Not Configured	11.2.2.1005.888881
Yes	Site_210	Activation Complete	Not Configured	11.2.2.1005.888881

Page Size: 200 Showing 1-4 of 4 items Page 1 of 1

It takes few minutes to complete the staging. You can view the status to track the staging progress. Initially the status shows **Staging Pending**, then **Downloading Appliance Software**, and finally **Staging Complete**. You can cancel the staging anytime by clicking **Cancel Stage** button.

- Once the staging is completed, click **Activate** button to activate the software.
- The LTE software activation is part of the scheduling window. To upgrade the LTE software, navigate to **Change Management Settings** tab. You can see a list of site names with scheduling information and an action option.

Scheduling Information

Site Name	HA State	Scheduling Information	Maintenance Mode	Actions
Azure_VPX_Branch_test	Not Configured	2021-01-04 at 21:20:00 (Maintenance window of 1 hours and repeated every 1...	<input type="checkbox"/>	
Site_110	Not Configured	2021-01-04 at 21:20:00 (Maintenance window of 1 hours and repeated every 1...	<input type="checkbox"/>	
MCN_Azure	Not Configured	2021-01-04 at 21:20:00 (Maintenance window of 1 hours and repeated every 1...	<input type="checkbox"/>	
Branch_VPX_Azure	Not Configured	2021-01-04 at 21:20:00 (Maintenance window of 1 hours and repeated every 1...	<input type="checkbox"/>	

In the scheduling window, a specific time frame is specified to complete the LTE software upgrade.

- Click the action symbol and provide the scheduling information - date with time, maintenance window duration in hours, repeat window with unit as days/weeks/months. Click **Save**.

Scheduling Info

Site Name

Azure_VPX_Branch_test

Date:

2021-01-04 21:20:00

Maintenance Window (hours):

1

Repeat Window:

1

Unit:

Days

Save

Cancel

Once the timing is set, it propagates the information to the appliance. LTE firmware upgrades when the time in the appliance matches with the time set in the schedule window. The schedule window lets you configure a specific time to upgrade LTE firmware. LTE firmware upgrade will not start immediately when you set the schedule window.

Note

For all the appliances, the following are the default scheduling information that is already set:

- **Schedule window** - 21:20:00
- **Maintenance window** - 1 hour
- **Repeated window** - 1 day

So if you don't configure the change management settings, the scheduling window processes the update automatically. Also, when you set the value of **Maintenance Window (hours)** to **0**, the LTE firmware upgrade happens immediately.

Starting 11.1.0, a new configuration knob is added for in-band management configuration on the site interface group page. This is a mandatory configuration for any appliance that needs to be managed through an inband IP. Missing this configuration in the SD-WAN Orchestrator for On-premises can cause the appliance to go offline (especially important when the 210 s and 110 s that were managed over LTE upgrade to 11.1.0).

Address resolution protocol

March 8, 2021

In Citrix SD-WAN deployments such as Gateway and One-arm, when the Address Resolution Protocol (ARP) requests are received frequently, the access points become overloaded affecting traffic flow. To overcome the traffic overload, you can configure the following ARP timers to send the ARP requests with specific interval times.

- **Gateway ARP Timer (ms):** The time, (range: 100–20000 milliseconds), between ARP requests for configured Gateway IP addresses.
- **Host ARP Timer (ms):** The time, (range: 1000–180000 milliseconds), between ARP requests for configured Host IP addresses.

Configuration / Advanced Settings / ARP

ARP ⓘ

Gateway ARP Timer (ms)

Host ARP Timer (ms)

Save

Virtual paths

October 21, 2020

A virtual path is a logical link between two WAN links. It comprises of a collection of WAN paths combined to provide high service-level communication between two SD-WAN nodes. This is done by constantly measuring and adapting to changing application demand and WAN conditions. The SD-WAN appliances measure the network on a per-path basis. A virtual path can be static (always exists) or dynamic (exists only when traffic between two SD-WAN appliances reaches a configured threshold).

Static virtual paths

The virtual path settings are inherited from the global wan link auto-path settings. You can override these configurations and add or remove the member path. You can also filter the virtual paths based on the site and the applied QoS profile. Specify a tracking IP address for the WAN Link that can be pinged to determine the state of the WAN Link. You can also specify a reverse tracking IP for the reverse path that can be pinged to determine the state of the reverse path.

To configure static virtual paths, from the site level, navigate to **Configuration > Advanced Settings > Virtual Paths > Static Virtual Paths**.

Virtual Paths ⓘ

Static Virtual Paths Dynamic Virtual Paths

Static Virtual Paths

Remote Site ^{*}
Branch_Azure_VPXL

QOS Profile
Standard

Branch_VPX_Azure Tracking IP

Branch_Azure_VPXL Reverse Tracking IP

Route Cost
Default

Active Member Paths

Restore Default Member Paths

<input type="checkbox"/>	Path	Actions
<input checked="" type="checkbox"/>	Branch_VPX_Azure -Broadband-ACT-1 -Branch_Azure_VPXL -Broadband-Verizon_Comm-1	

WAN Link Properties

Name	UDP Port	Alternate Port	Port Switching Interval (min)	Tunnel Header Size	Action
Branch_VPX_Azure-Broadband-ACT-1	4980		1440	0	
Branch_Azure_VPXL-Broadband-Verizon...	4980		1440	0	

Cancel
Save

The active member paths are listed in the **Active Member Paths** section, you can view or edit the member path settings.

- **IP DSCP Tagging:** A tag for the external IP header of the Virtual Path Control Protocol (VPCP) frame.
- **Loss Sensitive:** If enabled, a path might be marked as BAD due to loss and incurs a latency penalty in a path score. Set the percentage of loss over the time required to mark the path as BAD. Disable this option if loss of bandwidth is intolerable.
- **Percent Loss:** If packet loss exceeds the set percentage over the configured time, the GOOD Path state changes to BAD.
- **Over Time:** If packet loss exceeds the set percentage over this configured time, the path state is marked as BAD.
- **Silence Period:** The path state transitions from GOOD to BAD when no packets are received within the specified amount of time.
- **Path Probation Period:** The period to wait before changing the path state from BAD to GOOD.
- **Instability Sensitive:** Latency penalties due to BAD state and other spikes in latency are considered.

Member Path Info

IP DSCP Tagging

Any

Bad Loss Sensitive

Enable

Percent Loss (%)

DEFAULT

Over Time (ms)

1000

Silence Period (ms)

DEFAULT

Path Probation Period (ms)

10000

☒ Instability Sensitive

Cancel

Done

The WAN link details for the selected active member paths are listed, you can change the settings as required. The **UDP port** settings can be configured for both IPv4 and IPv6.

- **UDP Port:** The port used for LAN to WAN and WAN to LAN packet transfer. You can also specify.
- **Alternate Port:** The alternate UDP Port to be used when UDP port switching is enabled.
- **Port Switch Interval:** The interval, in minutes, that the WAN Link alternates its UDP Port.
- **Tunnel Header Size in Bytes:** The size of the tunnel header, in bytes, if applicable.
- **Active MTU Detect:** The LAN to WAN paths for dynamic virtual paths is actively probed for MTU.
- **Enable UDP Hole Punching:** The MCN assists UDP connectivity between compatible NAT-protected client sites.

Branch_VPX_Azure-Broadband-ACT-1

UDP Port	UDP Port V6
<input type="text" value="4980"/>	<input type="text" value="4980"/>
Alternate Port	Alternate Port V6
<input type="text"/>	<input type="text"/>
Port Switch Interval (min)	Port Switch Interval V6 (min)
<input type="text" value="1440"/>	<input type="text" value="1440"/>
Tunnel Header Size in Bytes	<input type="checkbox"/> Active MTU Detect
<input type="text" value="0"/>	<input type="checkbox"/> Enable UDP Hole Punching V6
<input type="checkbox"/> Enable UDP Hole Punching	

Cancel Done

Dynamic virtual paths

With demand for VoIP and video conferencing, the traffic between offices has increased. Setting up full mesh connections through data centers is time consuming and inefficient. With Citrix SD-WAN, you can automatically create paths between offices on demand using the Dynamic Virtual Path feature. The session initially uses an existing fixed path. As the bandwidth and time threshold is met, a new path is created dynamically if that new path has better performance characteristics than the fixed path. The session traffic is transmitted through the new path resulting in efficient usage of resources. The dynamic virtual paths exist only when they are needed and reduce the amount of traffic transmitted to and from the data center.

To configure dynamic virtual paths, from the site level, navigate to **Configuration > Advanced Settings > Virtual Paths > Dynamic Virtual Paths**.

Select **Override Global Defaults** to override the virtual path settings inherited from the global wan link auto-path settings. Select **Enable Dynamic Virtual Paths** to allow dynamic virtual paths between this site and other sites connected through an intermediate node. Set the maximum allowable dynamic virtual paths for the site.

Virtual Paths ⓘ

Static Virtual Paths Dynamic Virtual Paths

- ☐ Override Global Defaults
- ☒ Enable Dynamic Virtual Paths

Max limit for Number of dynamic virtual paths

Active Member Paths

<input type="checkbox"/>	Link	UDP Port	Alternate Port	Interval (min)	Actions
<input checked="" type="checkbox"/>	MPLS-ATMNet-1	4980	0	1440	
<input checked="" type="checkbox"/>	Internet-Jio-2	4980	0	1440	
<input type="checkbox"/>	Broadband-Airespring-3	4980	0	1440	

Save

Set the UDP port and dynamic virtual path threshold. Specify the throughput threshold, in kbps or packets per second, on the intermediate site at which the dynamic virtual paths are triggered on LAN to WAN or WAN to LAN.

Member Path Info

UDP Port

UDP Port V6

Alternate Port

Alternate Port V6

Interval (min)

Interval V6

LAN to WAN

Throughput (Kbps)

Throughput (pps)

WAN to LAN

Throughput (Kbps)

Throughput (pps)

Cancel

Done

Dynamic routing

March 25, 2021

After configuration and deployment of SD-WAN appliances in the network and once the connections are established, it is important to ensure that the traffic is properly redirected through the overlay SD-WAN network. You can check traffic redirection by using ping and traceroute diagnostic tools. If the ping and traceroute tests indicate that connectivity is established through the underlay paths, traffic redirection can be achieved by using the following dynamic routing protocols.

- **Open Shortest Path First (OSPF):** It is an interior gateway protocol, used to redirect traffic within an autonomous system, like the enterprise network. OSPF uses a link state routing algorithm to detect changes in the network topology and reroute packets by computing the shortest path free for each route. Use this protocol to redirect MPLS traffic. For more information, see **OSPF** section.
- **Border Gateway Protocol (BGP):** It is an exterior gateway protocol designed to redirect traffic routing and reachability information among different autonomous systems on the internet. It is capable of making routing decisions based on paths determined by ISPs. Use this protocol to redirect Internet traffic. For more information, see **Configure BGP** section.

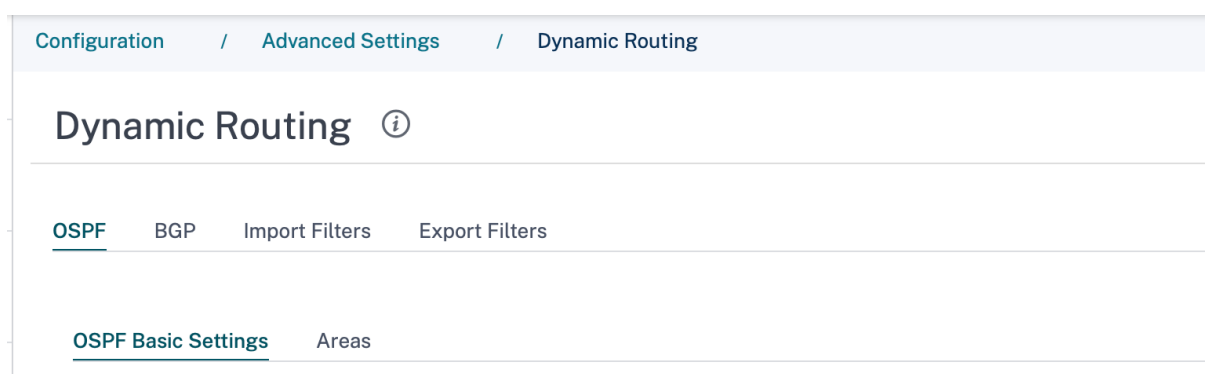
Earlier, the dynamic routing capability was available only for a single router ID. You were able configure a unique router ID either globally for the entire protocol (one for OSPF and BGP) or provide no router ID. From Citrix SD-WAN 11.3.1 release onwards, you can not only configure a router ID for the entire protocol but also configure a router ID for each routing domain. With this enhancement, you can enable stable dynamic routing across multiple instances with different router ID's converging in a stable manner.

If you configure a router ID for a specific routing domain, the specific router ID overrides the protocol level routing domain.

The screenshot shows a configuration window titled "Router ID Settings". It contains two main input fields: "Routing Domain" and "Router ID". The "Routing Domain" field is a dropdown menu currently showing "Default_RoutingDomain". The "Router ID" field is an empty text box. Below these fields are two buttons: "Save Router ID Settings" (in a teal box) and "Cancel" (in a light blue box).

OSPF

To configure OSFF, navigate to **Configuration > Advanced Settings > Dynamic Routing > OSPF**.



OSPF basic settings

Here are the parameters to be configured:

- **Enable:** Allow the OSPF routing protocol on the SD-WAN appliance to start exchanging Hello packets between neighboring routers.
- **Router ID:** An IPv4 address used for OSPF advertisements. This is optional, if not specified the lowest virtual IP of the virtual interfaces participating in routing is chosen.
- **Export OSPF Route Type:** Advertise the SD-WAN route to OSPF neighbors as type 1 Intra-area route or type 5 External route.
- **Export OSPF Route Weight:** The cost advertised to OSPF neighbors is the original route cost and the weight configured here.
- **Advertise SD-WAN Routes:** To advertise SD-WAN routes to the peer network elements.
- **Advertise BGP Routes:** To enable redistribution of BGP routes into the OSPF domain.

Configuration / Advanced Settings / Dynamic Routing

Dynamic Routing ⓘ

OSPF BGP Import Filters Export Filters

OSPF Basic Settings Areas

☐ Enable

Export OSPF Route Type

Type 5 AS External

Export OSPF Route Weight

0

☐ Advertise Citrix SD-WAN Routes

Tag Value

0

☐ Advertise BGP Routes

Tag Value

0

Protocol Preference *

150

Router ID Settings

Routing Domain *

Default_RoutingDomain

Router ID *

Save Router ID Settings Cancel

Areas

Click **+ Area** and provide the Area ID of the network that OSPF will learn routes from and advertise routes. Stub area ensures that this area will not receive route advertisements from outside of the designated Autonomous System. Configure the virtual interface settings.

Dynamic Routing ?

[OSPF](#) [BGP](#) [Import Filters](#) [Export Filters](#)

Area Information

Area ID *

☐ Stub Area

Virtual Interfaces

Name *

Routing Domain *

Authentication Type

Password

Interface Cost *

Network Type

Hello Interval *

Dead Interval *

BGP

To configure BGP, navigate to **Configuration > Advanced Settings > Dynamic Routing > BGP**.

[Configuration](#) / [Advanced Settings](#) / [Dynamic Routing](#)

Dynamic Routing ?

[OSPF](#) [BGP](#) [Import Filters](#) [Export Filters](#)

[BGP Basic Settings](#) [Communities](#) [Policies](#) [Neighbors](#)

BGP basic settings

Here are the parameters to be configured:

- **Enable:** Allow the BGP routing protocol on the SD-WAN appliance to start sending an open message as part of BGP peering.
- **Router ID:** (Optional) IPv4 address used for BGP advertisements. If the router ID is not specified the lowest virtual IP of the virtual interfaces participating in routing is chosen.
- **Local Autonomous System:** Autonomous system number the BGP protocol is running in.

- **Advertise SD-WAN Routes:** To advertise SD-WAN routes to the peer network elements.
- **Advertise OSPF Routes:** To enable redistribution of OSPF routes into the BGP domain.

The screenshot shows the 'Dynamic Routing' configuration page in the SD-WAN Orchestrator. The breadcrumb trail at the top is 'Configuration / Advanced Settings / Dynamic Routing'. The main heading is 'Dynamic Routing' with an information icon. Below this, there are tabs for 'OSPF', 'BGP' (which is selected), 'Import Filters', and 'Export Filters'. Under the 'BGP' tab, there are sub-tabs: 'BGP Basic Settings' (selected), 'Communities', 'Policies', and 'Neighbors'. In the 'BGP Basic Settings' section, there is an 'Enable' checkbox which is unchecked. Below it is the 'Local Autonomous System' field with the value '1'. There are two checkboxes: 'Advertise Citrix SD-WAN Routes' (unchecked) and 'Advertise OSPF Routes' (unchecked). The 'Protocol Preference' field has the value '100'. A dark grey bar separates the settings from the 'Router ID Settings' section. In this section, there is a 'Routing Domain' dropdown menu with the text 'Select a Routing Domain' and a 'Router ID' text input field. At the bottom, there are two buttons: 'Save Router ID Settings' and 'Cancel'.

Communities

Click **+ Community** to add a community. A collection of BGP communities that can be used for route filtering. The community list can also be used to set or modify the communities of a matching route.

For each policy, users can configure multiple community strings, AS-PATH-PREPEND, **MED** attribute. Users can configure up to 10 attributes for each policy.

Specify the name for the community and enter a community string to be advertised.

Dynamic Routing ⓘ

OSPF **BGP** Import Filters Export Filters

Community Information

Community Name ^{*}

Community Strings

Manual/Well Known

☒ New Format(AA:NN)

ASN ^{*}

Value ^{*}

Manual

Cancel

Done

- **Community Name:** Enter a community name.
- **Manual/Well Known:** Configure BGP community manually or select a standard well known BGP community from the list.
- **New Format (AA:NN):** Select the check box to use the new format for configuring the BGP community.
- **ASN:** The first 16 digit of the BGP community when using the new format for configuration.
- **Value:** Enter the BGP community value.

Policies

A collection of BGP attributes which can be used to set or modify route attributes for each BGP Peer. Create BGP policies to be applied selectively to a set of networks on a per-neighbor basis, in either direction (import or export). An SD-WAN appliance supports eight policies per site, with up to eight network objects (or eight networks) associated with a policy.

Dynamic Routing

OSPF BGP Import Filters Export Filters

Policy Information

BGP Policy Name ^{*}

Route Policy Attributes

BGP Attribute

Med

MED Value ^{*}

☐ Copy Route Cost to MED

Cancel

Done

- **BGP Policy Name:** Enter the BGP policy name.
- **BGP Attributes:** Select the BGP attributes from the list and provide the necessary information.

Neighbors

Neighbors are all of the configured BGP peer routers that are checked to find the shortest paths for routing. All the neighbors must be part of the same Autonomous System.

Click **+ Neighbor** to add a configured BGP policy for neighboring routers. You can specify the direction to indicate if this policy is applied for incoming or outgoing routes.

Dynamic Routing ⓘ

OSPF **BGP** Import Filters Export Filters

Neighbor Information

Routing Domain *

Default_RoutingDomain

Virtual Interface *

Neighbor IP *

Neighbor AS *

1

Hold Time *

180

Local Preference *

100

Password

☒ IGP Metric

☒ Multi Hop

Neighbor Policies

Order

100

Network Address

*

☐ Use IP Group

Community String list

Manual

BGP Community(AA:NN)

*

*

AS Path

*

BGP Policy *

Direction *

Cancel

Done

Import filters

You can configure Filters to fine-tune how route-learning takes place.

Import filter rules are rules that have to be met before importing dynamic routes into the SD-WAN route database. By default, no routes are imported.

Click **+ Import Rule**.

Dynamic Routing ⓘ

OSPF BGP Import Filters Export Filters

Import Filter Rule Attributes

Protocol

Routing Domain

Source Router

Destination IP

☐ Use IP Group

Prefix

Next Hop

Route Tag

Any

Default_RoutingDomain

*

*

eq

*

*

*

AS Path Length

Citrix SD-WAN Cost

☒ Export Route to Citrix Appliances

☒ Include

eq

*

6

☐ Eligibility Based on Gateway

☐ Eligibility Based On Path

Service Type

Service Name

Path

Local

Select Name

Select Path

Local

Internet

Intranet

GRE Tunnel

Passthrough

Cancel

Done

Export filters

Define the rules that have to meet when advertising SD-WAN routes over dynamic routing protocols. By default, all routes are advertised to peers.

Dynamic Routing ⓘ

OSPF BGP Import Filters Export Filters

+ Export Rule

☒ Top of List

☐ Bottom of List

☐ Specify Row Number

Row number

Local Export Filters

No	Routing Domain	Network Address	Prefix	Cost	Service Type	Service Name	Gateway IP
----	----------------	-----------------	--------	------	--------------	--------------	------------

Global Export Filters

Routing Domain	Network Address	Prefix	Cost	Service Type	Service Name	Gateway IP
Default_RoutingDom...	*	eq *	eq *	Local	Any	*

Save

Network address translation

December 16, 2020

Network Address Translation (NAT) on the SD-WAN appliances translates the private IP addresses within your local branch or data center enterprise network to a single Public IP address. The public IP address is used for communication over the internet.

For more information about configuring NAT, see [Network Address Translation](#).

To configure NAT for a site using the SD-WAN Orchestrator for On-premises, from site level, navigate to **Configuration > Advanced Settings > NAT**.

NAT ⓘ

Dynamic Source NAT Static Source NAT Destination NAT

+ Dynamic Source NAT

☒ Top of List ☐ Bottom of List ☐ Specify Row Number

Row number

No	Type	Name	Inside Zone	Routing Domain	Inside IP	Actions
----	------	------	-------------	----------------	-----------	---------

You can configure the following types of NAT:

- Dynamic source NAT
- Static NAT
- Destination NAT

Dynamic source NAT

Dynamic Source NAT allows multiple hosts to have their source IP addresses translated to the same public IP address with different port numbers. Port restricted NAT uses the same outside port for all translations related to an Inside IP address and port pair. For more information, see [Configure Dynamic NAT](#).

NAT ⓘ

Dynamic Source NAT

Type	Routing Domain	IP Type	
Internet	Default_RoutingDomain	ipv4	
Destination Service *	Inside Zone	Inside IP/Prefix	Outside IP
Internet	Default_LAN_Zone	Any	

— Advanced Options

<input type="checkbox"/> Port Parity	<input type="checkbox"/> Bind Responder Route	<input type="checkbox"/> Allow Related	<input type="checkbox"/> IPSec Passthrough	<input type="checkbox"/> GRE/PPTP Passthrough	<input type="checkbox"/> On Recieve	<input type="checkbox"/> Symmetric
--------------------------------------	---	--	--	---	-------------------------------------	------------------------------------

Port Forwarding Rules

Routing Domain	Protocol	Outside Port	Inside IP *	Inside Port
Default_RoutingDomain	Both			
Cancel	Done			

Static NAT

In **Static NAT**, a permanent 1–1 mapping between an internal private address and a public address is done. This type of NAT can be used for allowing traffic into a mail server or web server. For more information, see [Configure Static NAT](#).

NAT ⓘ

Static Source NAT

Type	Destination Service *	Inside Zone	Outside Zone
Internet	Internet	Default_LAN_Zone	Default_LAN_Zone
Routing Domain	IP Type	Inside IP/Prefix *	Outside IP/Prefix
Default_RoutingDomain	ipv4		
<input type="checkbox"/> Bind Responder Route	<input type="checkbox"/> Proxy ARP	<input type="checkbox"/> On Recieve	
Cancel	Save		

Destination NAT

Destination NAT is performed on incoming packets when the SD-WAN appliance translates a public destination address to a private address. It also allows port forwarding.

NAT ⓘ

Destination NAT

Type
Service Name *
IP Type

Internet
Internet
ipv4

Inside IP/ Prefix *
Inside Port
Outside IP *
Outside Port
Routing Domain

Default_RoutingDomain

Cancel
Save

Dynamic host configuration protocol

April 14, 2021

You can configure your SD-WAN appliances as either **DHCP Servers** or **DHCP Relay agent**. The DHCP server feature allows devices on the same network as the SD-WAN appliance's LAN/WAN interface to obtain their IP configuration from the SD-WAN appliance. The DHCP relay feature allows your SD-WAN appliances to forward DHCP packets between DHCP client and server.

DHCP ⓘ

Server Subnets
Relays
DHCP Options Set (Global)

+ Server Subnet

Virtual Interface	Domain Name	Primary DNS	Secondary DNS	Enabled	Actions

DHCP server

Citrix SD-WAN appliances can be configured as a DHCP server. It can assign and manage IP addresses from specified address pools within the network to DHCP clients.

The DHCP server can be configured to assign other parameters such as the DNS IP address and default gateway. DHCP server accepts address assignment requests and renewals. The DHCP server also accepts broadcasts from locally attached LAN segments or from DHCP requests forwarded by other DHCP relay agents within the network.

To configure the DHCP server, in the Site configuration page, from site level, navigate to **Configuration > Advanced Settings > DHCP > Server Subnets** > click **+ Server Subnet**.

Select the **Virtual interface** to be used to receive the DHCP requests. The IP Subnet to which the DHCP server provides the IP addresses is auto-populated.

DHCP ⓘ

Server Subnet

Virtual Interface: VIF-5-LAN-2
 IP Subnet: 10.146.110.1/23
 Domain Name: uk.bgroup.bz

Primary DNS: 172.27.0.3
 Secondary DNS: 172.27.0.4 ☒ Enable

IP Address Ranges

+ IP Address Range

Range Start IP	Range End IP	Gateway IP	DHCP Options Set	Actions
10.146.110.21	10.146.110.32	10.146.110.1	CHDigital	

Reserved IP Addresses

Fixed IP Address*: 10.146.110.21
 MAC Address*: 58:e6:ba:2b:30:b1

DHCP Options Set*: [DHCP Options Set](#)
 CHDigital

Cancel Done

Enter the **Domain Name**, **Primary DNS**, and **Secondary DNS**. The DHCP Server forwards this information to the DHCP clients.

Configure dynamic IP address pools that is used to allocate IP addresses to clients. Specify the range starting and ending IP address and select the **DHCP Option Set**.

Note

The DHCP Option Set are groups of DHCP settings that can be applied to individual IP address ranges. For more information, see DHCP Option Set.

Set the reserved IP address by mapping individual hosts that require a fixed IP address to its MAC address. Enter the **Fixed IP Address**, **MAC Address**, and select a **DHCP Option Set**.

Note

For reserved IP addresses, the **Gateway IP** is set by configuring the **Router** option in the **DHCP Option Set**.

DHCP relay

Citrix SD-WAN appliance can be configured as a DHCP relay. It relays DHCP requests and replies between the local DHCP Clients and a remote DHCP Server.

It allows local hosts to acquire dynamic IP addresses from the remote DHCP Server. Relay agent receives DHCP messages and generates a new DHCP message to send out on another interface.

To configure the DHCP server, in the Site configuration page, navigate to **Configuration > Advanced Settings > DHCP > Relays** > click **+ DHCP Relay**.

DHCP ⓘ

Server Subnets Relays DHCP Options Set (Global)

+ DHCP Relay

Virtual Interface	IP Address
<input type="text" value="Virtual Interface"/>	<input type="text" value="Server IP"/>

Save

Select a **Virtual Interface** that communicates to a remote DHCP Server. Enter the **DHCP Server IP** that the relay uses to forward the request and response from the clients.

You can configure a single **DHCP Relay** using a common Virtual Network Interface and point it to multiple DHCP Servers.

DHCP options set

DHCP Options are a group of DHCP configurations that can be applied to individual IP address ranges or a single host.

Set a name for the DHCP option profile and choose the **IP Address Type**. Click **+ DHCP Options Set** and select a DHCP option name from the list. The option number is pre-configured. For custom options, the range is 224–254. Select a **Data Type** and enter a **Value** for the option.

DHCP ⓘ

Server Subnets Relays DHCP Options Set (Global)

Set Name *

IP Address Type ☒ V4 ☐ V6

+ DHCP Options

DHCP Option Name	Option Number	Data Type	DHCP Option Value	Actions
<input type="text"/>				

Cancel

Save

Multicast routing

April 8, 2021

Multicast routing enables efficient distribution of one-to-many traffic. A multicast source, sends multicast traffic in a single stream to a multicast group. The multicast group contains receivers such as hosts and adjacent routers that use the IGMP protocol for multicast communication. Voice over IP, Video on demand, IP television, and Video conferencing are some of the common technologies that use multicast routing. When you enable multicast routing on the Citrix SD-WAN appliance, the appliance acts as a multicast router.

Source specific multicast

Multicast protocols typically allow multicast receivers to receive multicast traffic from any source.

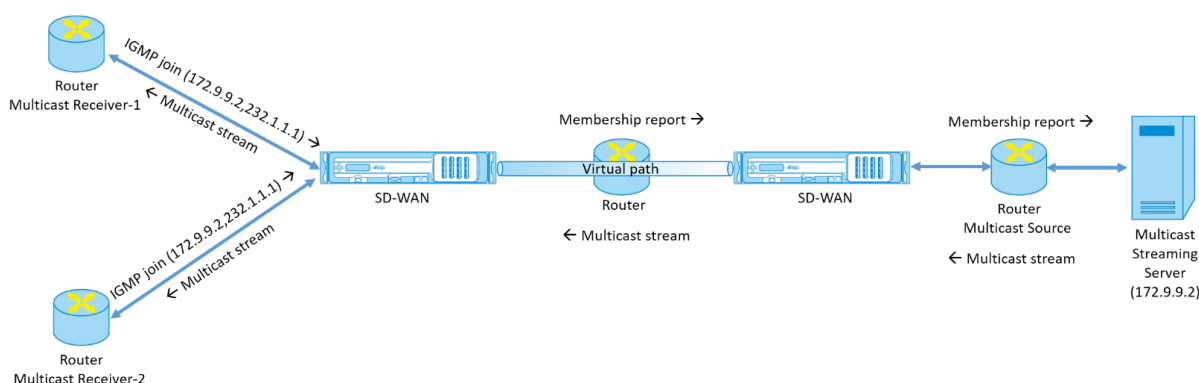
With the source specific multicast (SSM), you can specify the source from which the receivers receive the multicast traffic. It ensures that the receivers are not open listeners to every source that is sending multicast streams but rather listen to a particular multicast source.

The SSM reduces the cost of resources used in consuming traffic from every possible source. The SSM also provides a layer of security by ensuring that the receivers receive traffic from a known sender.

The following topology shows two multicast receivers at a branch site and a multicast server (172.9.9.2) at the Data Center. The multicast server streams traffic over a particular group (232.1.1.1), the receivers join the group. Any traffic streamed on the multicast group is relayed to all the receivers that joined the group.

Note

For SSM to work, the multicast group IP must fall within the range 232.0.0.0/8.



1. The multicast receivers send an IP IGMP join request indicating that the receivers want to join the multicast group and want to receive the multicast stream from the source.

The IGMP join includes 2 attributes the multicast source and group (S, G). IGMP Version 3 is used for SSM on the multicast source and the receiver to relay some INCLUDE specific source addresses.

The SSM allows the receivers to explicitly receive streams from specific Multicast servers, whose source address is explicitly provided by the receivers as part of the JOIN request. In this example, an IGMP v3 join request is triggered with an explicit include source list, which contains the source 172.9.9.2, to be the address that sends the multicast stream over the group 232.1.1.1.

2. The Citrix SD-WAN at the branch listens to all the IGMP requests from these receivers and converts it into a membership report and sends it over the Virtual Path to the SD-WAN appliance at the data center.
3. The Citrix SD-WAN appliance at the data center receives the membership report over the Virtual Path and forwards it to the Multicast Source, establishing a control channel.
4. The Multicast source transmits the multicast stream over the Virtual path to the multicast receivers.

The control channel traffic and the multicast stream flow through the established virtual path between the branch and the data center. The Citrix SD-WAN overlay path insures and insulates multicast traffic from WAN degradation or link brownouts.

Configure multicast

To configure multicast, perform the following on the SD-WAN appliance at both the source and destination.

1. Create a multicast group - Provide a name and IP address for the multicast group. The multicast group IP must fall within the range 232.0.0.0/8 for source specific multicast.
2. Enable IGMP proxy – You can configure the Citrix SD-WAN appliance as an IGMP proxy to carry the IGMP control channel information for multicast routing. IGMP V3 is required for single source

multicast.

3. Define the upstream and downstream services - An upstream interface enables the IGMP PROXY to connect to the SD-WAN appliance closer to the actual multicast source that streams the traffic. A downstream interface enables the IGMP Proxy to connect to the hosts that are farther away from the actual multicast source that streams the traffic.

The upstream and downstream services are different for the appliance at the source and the appliance at the destination

To configure multicast, at the site level, navigate to **Configuration > Advanced Settings > Multicast Groups**. Create a multicast group by providing a name and IP address for the multicast group. Click **Enable IGMP Proxy**.

Configure the upstream and downstream paths for the Branch and data center appliances.

For the appliance closer to the multicast receiver (Branch), the appliance receives the multicast traffic on the Virtual Path Interface and sends the traffic on the Local Interface towards the receiver.

Multicast Groups ⓘ

Multicast Group

Group Name *

Group IP *

Routing Domain *

☒ Enable IGMP Proxy

Grp2

232.1.1.1

Default_RoutingDomain

Service

+ Service

Service Type	Service Instance	Direction	Upstream	Actions
Local	VIF-1-LAN-1	Send	No	
Virtual Path	orch_mcn	Receive	Yes	

Cancel

Save

For the appliance closer to the multicast source (Data center), the appliance receives the multicast traffic on the Local Interface and sends the traffic on the Virtual Path Interface.

Multicast Groups ⓘ

Multicast Group

Group Name *

Group IP *

Routing Domain *

iDC1_Grp

232.1.1.1

Default_RoutingDomain

☒ Enable IGMP Proxy

Service

+ Service

Service Type	Service Instance	Direction	Upstream	Actions
Local	VIF-2-WAN-1	Receive	Yes	
Virtual Path	orch_mc	Send	No	

Cancel

Save

Monitoring

Flows statistics

After the multicast control channel is established and the multicast source begins streaming, you can view the multicast flows statistics. You can see that Multicast UDP traffic was sent on the virtual path service from a receiver to the multicast group 232.1.1.1.

Note:

If SSM is enabled and if the traffic is received from a different server that is not part of the expected list of source senders the SD-WAN appliance will not have any reporting data.

Site Reports:Real Time Flows

Maximum number of flows to display

Retrieve latest data

Search

☒ Upload ☒ Download

Customize Columns

Info	No	Application	Direction	Throughput (Kbps)	Routing Domain	Source IP Addr	Dest IP Addr	Source Port	Dest Port	Proto	Service Type	Packets	PPS	Class	Service Name	Age (mS)	Bytes
ⓘ	1	isakmp	Upload	1068.459	Default_RoutingDomain	10.3.2.4	232.1.1.1	44250	5001	UDP(17)	VPath	7212	89.157	N/A	zscalerService_1	3934	0

Showing

Showing 1-1 of 1 items

Page 1 of 1

Firewall statistics

The firewall table shows the multicast traffic coming over the LAN interface over the Multicast group IP address and is sent over the virtual path.

Site Reports: Real Time Firewall Connections

Maximum number of Connections to display Retrieve latest data Search

Customize Columns

Application	Family	Routing Domain	IP Addr	Source Service Type	Destination IP Addr	Destination Service Type	State	Is NAT	Bytes	Sent Kbps
Internet Security ...	Encrypted	Default_RoutingD...	10.56.2.4	IPHost	165.225.218.38	Intranet	ESTABLISHED	NO	6429631	0.025
Internet Security ...	Encrypted	Default_RoutingD...	10.56.2.4	IPHost	165.225.216.38	Intranet	ESTABLISHED	NO	6430975	0.025

1 to 2 of 2 < < Page 1 of 1 > >

Multicast group statistics

The multicast group table provides details about multicast traffic such as packets sent and received over source, destination, and the aggregation of both.

DASHBOARD

REPORTS

- Alerts
- Usage
- Quality
- QoS
- Historical Statistics
- Real Time
 - Statistics
 - Flows
 - Firewall Connections
- Cloud Direct
- O365 Metrics
- Appliance Reports (preview)

CONFIGURATION

Site Report : Real Time Statistics

ARP Routes Virtual Path Services Classes Ethernet Observed Protocols Wan Path Application QoS Multicast Group

Retrieve latest data

Multicast Group Destination Services

Multicast Group	Service Type	Service Name	Packets	Kbps
ATGDC1_Grp	IPHOST		1071	1068.503

Multicast Group Source Services

Multicast Group	Service Type	Service Name	Packets	Kbps
ATGDC1_Grp	VPath	Ombud1	1071	1068.503

Multicast Group Statistics

Multicast Group	Packets Received	Kbps Received	Packets Sent	Kbps Sent
ATGDC1_Grp	1071	1068.503	1071	1068.503

Virtual router redundancy protocol

January 4, 2021

Virtual Router Redundancy Protocol (VRRP) is a widely used protocol that provides device redundancy to eliminate the single point of failure inherent in the static default-routed environment. VRRP allows you to configure two or more routers to form a group. This group appears as a single default gateway with one virtual IP address and one virtual MAC address.

Citrix SD-WAN supports VRRP version 2 and version 3 to inter-operate with any third party routers. The SD-WAN appliance acts as a master router and direct the traffic to use the Virtual Path Service between sites. You can configure the SD-WAN appliance as the VRRP master by configuring the Virtual Interface IP as the VRRP IP and by manually setting the priority to a higher value than the peer routers. You can configure the advertisement interval and the preempt options.

To configure VRRP, in the Site configuration page, navigate to **Configuration > Advanced Settings > VRRP** > click **+ Add VRRP**.

VRRP ⓘ

VRRP Settings

VRRP Group ID * 1 Version V3 Priority * 100 Advertisement Interval * 1000

Authentication Type Authentication Text ☒ Reclaim ☒ Use V2 Checksum

Virtual Router IPs

Virtual Interface * VIF-1-One-Arm-1 Virtual IP Address * 1.1.1.1/1 VRRP Router IP * 1.2.3.4

Cancel Done

You can edit the following member path parameters:

- **VRRP group ID:** The VRRP group ID. The group ID must be a value range is 1–255. The same group ID must be configured on the back-up routers too.
- **Version:** The VRRP protocol version. You can choose between VRRP protocol V2 and V3.
- **Priority:** The priority of the Citrix SD-WAN appliance for the VRRP group. The priority range is 1–254. Set this value to maximum (254) to make the SD-WAN appliance the master.

Note

If the router is the owner of the VRRP IP address, the priority is set to 255 by default.

- **Advertisement Interval:** The frequency in milliseconds, with which the VRRP advertisements are sent when the SD-WAN appliance is the master. The default advertisement interval is one second.
- **Authentication Type:** You can choose **Plain Text** to enter an authentication string. The authentication string is sent as a plain text without any encryption in the VRRP Advertisements. Choose **None**, if you do not want to set up authentication.
- **Authentication Text:** The authentication string to be sent in the VRRP Advertisement. This option is enabled if the **Authentication Type** is **Plain Text**.

Note

The **Authentication Type** and **Authentication Text** parameters are enabled only for VRRP protocol version 2.

- **Use V2 Checksum:** Enables compatibility with third party network devices for VRRPv3. By default, VRRPv3 uses the v3 checksum computation method. Certain third party devices might only support VRRPv2 checksum computation. In such cases, enable this option.

- **Virtual Interface:** The virtual interface to be used for VRRP. Choose one of the configured virtual interfaces.
- **Virtual IP Address:** The virtual IP address assigned to the virtual interface. Choose one of the configured virtual IP addresses for the virtual interface.
- **VRRP Router IP:** The virtual router IP address for the VRRP group. By default, the Virtual IP address of the SD-WAN appliance is assigned as the virtual router IP address.

Domain Name System settings

April 7, 2021

Domain Name System (DNS) translates human readable domain names to machine-readable IP addresses, and the opposite way. Citrix SD-WAN provides the following DNS features:

- DNS Proxy
- DNS Transparent Forwarding

To configure DNS settings, in the Site configuration page, navigate to **Configuration > Advanced Settings > DNS Settings**.

DNS ⓘ

Site Specific DNS Services DNS Proxies DNS Transparent Forwarders

+ DNS Service

No	DNS Service Name	Primary DNS	Secondary DNS	Actions

Site specific DNS servers

On the **Site specific DNS servers** tab, click **+ DNS Server** to configure site-specific DNS servers to which the DNS requests are routed. Provide a name for the DNS server. Choose one of the following service types:

- **Static:** Intercepts the DNS requests destined to the Citrix SD-WAN IP address and forwards it to the specified IPv4 DNS servers. You can create internal, ISP, google or any other open source DNS service.
- **Dynamic:** Intercepts the DNS requests destined to the Citrix SD-WAN IP address and redirects it to one of the IPv4 DNS servers learned from the DHCP based WAN links. If the WAN link goes

down, another DHCP based WAN links DNS server is chosen. This feature is useful in the deployment where ISPs allow DNS requests only to DNS servers hosted by them. Dynamic DNS service can be configured at site level only. Only one dynamic DNS service is permitted per site.

- **StaticV6:** Intercepts the DNS requests destined to the Citrix SD-WAN IP address and forwards it to the specified IPv6 DNS servers. You can create internal, ISP, google or any other open source DNS service.
- **DynamicV6:** Intercepts the DNS requests destined to the Citrix SD-WAN IP address and redirects it to one of the IPv6 DNS servers learned from the DHCP based WAN links. If the WAN link goes down, another DHCP based WAN links DNS server is chosen. This feature is useful in the deployment where ISPs allow DNS requests only to DNS servers hosted by them. Dynamic DNS service can be configured at site level only. Only one dynamic DNS service is permitted per site.

To configure the Static DNS service, select the **Type** as **Static** (for IPv4 address) or **StaticV6** (for IPv6 address) and enter a pair of **Primary DNS** and **Secondary DNS** server IP addresses.

To configure Dynamic DNS service, select the **Type** as **Dynamic** (for IPv4 address) or **DynamicV6** (for IPv6 address) and select **Internet** for **Service Type** and **Service Instance**.

The corresponding DNS proxy services get listed in the **InBand Management DNS** drop-down list under **Site Configuration > Interfaces**.

DNS ⓘ

DNS Service for the Site

<p><small>DNS Service Name *</small></p> <input style="width: 90%;" type="text" value="Eg: dns_service1"/>	<p><small>Type</small></p> <div style="border: 1px solid #ccc; padding: 2px; text-align: center;">Static ▼</div>
<p><small>Service Type</small></p> <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div>	<p><small>Service Instance</small></p> <div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div>
<p><small>Primary DNS *</small></p> <input style="width: 90%;" type="text" value="Eg: a.b.c.d"/>	<p><small>Secondary DNS</small></p> <input style="width: 90%;" type="text" value="Eg: a.b.c.d"/>
<div style="display: inline-block; border: 1px solid #ccc; padding: 5px 10px; margin-right: 10px;">Cancel</div> <div style="display: inline-block; background-color: #0070c0; color: white; padding: 5px 10px;">Save</div>	

DNS proxy

DNS proxy intercepts the DNS requests destined to the SD-WAN IP address and forwards it to the selected DNS servers. You can configure a proxy with multiple forwarders that helps steering DNS re-

quests based on application domain names.

DNS ⓘ

DNS Proxy

DNS Proxy Name *

DNS-proxy-1

Interfaces to intercept DNS requests

<input type="checkbox"/>	Virtual Interface
<input checked="" type="checkbox"/>	VIF-1-LAN-1
<input checked="" type="checkbox"/>	VIF-2-WAN-1
<input type="checkbox"/>	VIF-3-WAN-2
<input type="checkbox"/>	VIF-4-LAN-2

IPv4 Default DNS Service

IPv6 Default DNS Service

App Specific DNS Forwarding Rule

Application * IPv4 DNS Service * IPv6 DNS Service

Cancel

Done

- DNS proxy settings:
 - **DNS Proxy Name:** Name of the DNS Proxy.
 - **Interfaces to intercept DNS requests:** The interfaces on which the DNS requests are intercepted. Only trusted interfaces are allowed.
 - **Default DNS Server for all traffic:** The default DNS server to which the DNS requests is forwarded, if none of the applications match in the DNS forwarder look-up.
 - **IPv4 Default DNS Service:** The IPv4 default DNS service to which the DNS requests are forwarded, if none of the applications match in the DNS forwarder look-up.
 - **IPv6 Default DNS Service:** The IPv6 default DNS service to which the DNS requests are forwarded, if none of the applications match in the DNS forwarder look-up.
- App specific DNS Forwarding rules:
 - **Application:** Applications for which DNS requests have to be forwarded to the selected DNS server.

- **IPv4 DNS Service:** The IPv4 DNS service that the DNS request is forwarded to for the specified application.
- **IPv6 DNS Service:** The IPv6 DNS service that the DNS request is forwarded to for the specified application.

DNS transparent forwarders

Citrix SD-WAN can be configured as a transparent DNS forwarder. In this mode, SD-WAN can intercept DNS requests that are not destined to its IP address and forward them to the specified DNS servers. Only the DNS requests coming from the local service on trusted interfaces are intercepted. If the DNS requests match any applications in the DNS forwarder list, then it is forwarded to the configured DNS service.

DNS ⓘ

DNS Transparent Forwarder

Application *

IPv4 DNS Service * IPv6 DNS Service

Cancel

Save

- **Application:** Applications for which DNS requests have to be forwarded to the selected DNS server.
- **IPv4 DNS Service:** The IPv4 DNS service that the DNS request is forwarded to for the specified application.
- **IPv6 DNS Service:** The IPv6 DNS service that the DNS request is forwarded to for the specified application.

March 8, 2021

Link aggregation groups

The Link Aggregation Groups (LAG) functionality allows you to group two or more ports on your SD-WAN appliance to work together as a single port. This ensures increased availability, link redundancy, and enhanced performance.

SD-WAN Orchestrator for On-premises supports simple Link Aggregation Group (ACTIVE-BACKUP). The 802.3ad LACP protocol based negotiations are not supported in the current release. At any time only one port is active and the other ports are in backup mode. The active and backup supports rely on the Data Plane Development Kit (DPDK) package for LAG functionality. The LAG functionality is available only on the following DPDK supported platforms:

- Citrix SD-WAN 110 SE
- Citrix SD-WAN 210 SE
- Citrix SD-WAN 410 SE
- Citrix SD-WAN 1100 SE/PE
- Citrix SD-WAN 4000, 4100, and 5100 SE
- Citrix SD-WAN 6100 SE

Note

The LAG functionality is not supported on VPX/VPXL platforms.

To configure link aggregation groups, at the site level, navigate to **Configuration > Advanced Settings > LAG** and select the member Ethernet interfaces to form a link aggregation group.

You can create a maximum of 4 LAGs with a maximum of 4 ports grouped in each LAG on the Citrix SD-WAN appliances.


For the Citrix SD-WAN 210 and 410 appliances, a maximum of 3 LAGs and for the Citrix SD-WAN 110 appliance, a maximum of 2 LAGs can be created.

LAG ⓘ

Name	Ethernet Interfaces					
LAG0	1/1	1/2	1/3	1/4	1/7	1/8
LAG1	1/1	1/2	1/3	1/4	1/7	1/8
LAG2	1/1	1/2	1/3	1/4	1/7	1/8
LAG3	1/1	1/2	1/3	1/4	1/7	1/8

Save

Once the ports are added to the LAG, you can select the LAGs to configure interfaces under **Site Configuration**. These interfaces are further used to configure LAN/WAN links and HA. You cannot change settings for individual member ports, any configuration changes made to the LAG, is automatically pushed to the member ports.


Verify Config
01 Site Details
02 Device Details
03 Interfaces
04 WAN Links
05 Routes
06 Summary

Interface Attributes

Deployment Mode *	Interface Type *	Security *	Interface Name
Edge (Gateway) ▾	LAN ▾	Trusted ▾	LAN-2

Physical Interface

Select Interface *

LAG0
1/1
1/2
1/5
1/6
1/7
1/8
LTE-E1

[Link Aggregation Group](#)

In the **Interfaces** section, click **Link Aggregation Group** to quickly change the LAG configuration if necessary.

Link Aggregation Groups

Name	Ethernet Interfaces
LAG0	1/1 1/2 1/3 1/4 1/7 1/8
LAG1	1/1 1/2 1/3 1/4 1/7 1/8
LAG2	1/1 1/2 1/3 1/4 1/7 1/8
LAG3	1/1 1/2 1/3 1/4 1/7 1/8

Done

Appliance settings

May 4, 2021

SD-WAN Orchestrator for On-premises allows you to configure the appliance settings, at the site level and push it to the remote appliances.

You can configure the user, network adapters, NetFlow, AppFlow, SNMP, Fallback configuration, and Purge flow settings.

If HA is configured, select the primary or secondary appliance for which you want to change the appliance settings.

Device Information

Select Device

Primary

Primary

Secondary

Administrative interface

The administrative interface allows you to add and manage the local and remote user accounts. The remote user accounts are authenticated through the RADIUS or TACACS+ authentication servers.

Manage users

You can add new user accounts for the site. To add a new user, navigate to **Configuration > Appliance Settings > Administrator Interface > Manage Users**, and click **+User**.

Manage Users

+ User

Note: Deleting a user will also delete local files for that user.

User Name

▼

Delete Selected User

Provide the following details:

- **User Name:** The user name for the user account.
- **New Password:** The password for the user account.
- **Confirm Password:** Reenter the password to confirm it.
- **User level:** Select one of the following account privileges:
 - **Admin:** An Admin account has read-write access to all the settings. An admin can perform configuration and software update to the network.
 - **Viewer:** A Viewer account is a read-only account with access to Dashboard, Reporting, and Monitoring sections.
 - **Network Admin:** A Network Administrator has read-write access to the Network setting and read-only access for other settings.
 - **Security Admin:** A Security Administrator has read-write access for the Firewall / Security related settings read-only access for other settings.

Note

Security administrator has the authority to disable the write access to the firewall for other users (Admin/Viewer).

Manage Users

User Name *

admin

New Password *

.....

Confirm Password *

.....

User Level *

admin

Cancel

Save

To delete a user, select a user name and click **Delete Selected User**. The user account and the local files are deleted.

Change local user password

To change the local user password, navigate to **Configuration > Appliance Settings > Administrative Interface > User Accounts > Change Local User Password** and provide the following values:

- **User Name:** Select a user name for which you want to change the password from the list of users configured at the site.
- **Current Password:** Enter the current password. This field is optional for admin users.
- **New Password:** Enter a new password of your choice.
- **Confirm Password:** Reenter the password to confirm it.

User Accounts**RADIUS****TACACS+**

Change Local User Password

User Name *

admin

Current Password

.....

New Password *

.....

Confirm Password *

.....

Save

RADIUS authentication server

RADIUS enables remote user authentication on the appliance. To use RADIUS authentication, you must specify and configure at least one RADIUS server. Optionally, you can configure redundant backup RADIUS servers, up to a maximum of three. The servers are checked sequentially. Ensure that the required user accounts are created on the RADIUS authentication server.

To configure RADIUS authentication, navigate to **Configuration > Appliance Settings > Administrative Interface > RADIUS**, and click **Enable RADIUS**.

Note

You can either enable RADIUS or TACACS+ authentication on a site. You cannot enable both at the same time.

Provide the host IP address of the RADIUS server and the authentication port number. The default port number is 1812. Enter a Server key and confirm it, it is a secret key used to connect to the RADIUS server. Specify the time interval to wait for an authentication response from the RADIUS server. The timeout value must be less than or equal to 60 seconds.

Note

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

The screenshot shows the 'RADIUS Settings' configuration page. At the top, there's a navigation bar with 'Administrator Interface' selected, and sub-headers for 'User Accounts', 'RADIUS', and 'TACACS+'. The 'RADIUS Settings' section has a checkbox 'Enable RADIUS' which is checked. Below this, there are three rows for 'Server 1', 'Server 2', and 'Server 3'. Each row has 'IP Address' and 'Authentication Port' fields. 'Server 1' has IP 10.102.72.41 and port 1812; 'Server 2' has IP 10.102.72.56 and port 1812; 'Server 3' fields are empty. There are also fields for 'Server Key', 'Confirm Server Key', and 'Timeout' (set to 10). A 'Save' button is at the bottom left.

TACACS+ authentication server

TACACS+ enables remote user authentication on the appliance. To use TACACS+ authentication, you must specify and configure at least one TACACS+ server. Optionally, you can configure redundant backup TACACS+ servers, up to a maximum of three. The servers are checked sequentially. Ensure that the required user accounts are created on the TACACS+ authentication server.

To configure TACACS+ authentication, navigate to **Configuration > Appliance Settings > Administrative Interface > TACACS+** and click **Enable TACACS+**.

Note

You can either enable RADIUS or TACACS+ authentication on a site. You cannot enable both at the same time.

1. Select the encryption method to send the user name and password to the TACACS+ server.
2. Provide the host IP address of the TACACS+ server and the authentication port number. The default port number is 49.
3. Enter a Server key and confirm it, it is a secret key used to connect to the TACACS+ server.
4. Specify the time interval to wait for an authentication response from the TACACS+ server. The timeout value must be less than or equal to 60 seconds.

Note

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

User Accounts RADIUS **TACACS+**

Tacacs Settings

☒ Enable TACACS

Server 1:	IP Address* 10.102.75.41	Authentication Port* 49
Server 2:	IP Address 10.102.75.46	Authentication Port 49
Server 3:	IP Address	Authentication Port

Authentication Type: ☒ PAP ☐ ASCII

Server Key:

Confirm Server Key:

Timeout:

Save

NetFlow host settings

NetFlow Collectors collect IP network traffic as it enters or exits an SD-WAN interface. You can determine the source and destination of traffic, class of service, and the causes for traffic congestion using NetFlow data. For more information, see [Multiple NetFlow Collector](#).

You can configure up to three NetFlow hosts. To configure NetFlow host settings, navigate to **Configuration > Appliance Settings > NetFlow Host Settings**. Select **Enable NetFlow** and provide the IP Address, and Port number of the NetFlow host.

NetFlow Host Settings

☒ Enable NetFlow

NetFlow Host 1:	IP Address* 10.102.72.41	Port* 2055
NetFlow Host 2:	IP Address	Port
NetFlow Host 3:	IP Address	Port

Save

Network adapters

For Citrix SD-WAN appliances, you can manually change the management IP address and other network parameters. You can change the IPv4 address, subnet mask, gateway IP address, IPv6 address, and prefix of the appliance or obtain the IP address automatically by enabling DHCP or SLAAC (only for IPv6 addresses). For more information, see [Dynamic host configuration protocol](#).

Note

You cannot change the IP address, if the interface is used for in-band management. For more information on in-band management, see [In-band management](#).

To configure the network adapter settings, navigate to **Configuration > Appliance Settings > Network Adapter**.

The screenshot shows the 'Network Adapters' configuration page. At the top, there is a navigation bar with links: Administrator Interface, NetFlow Host, **Network Adapters** (selected), AppFlow Host, SNMP, Fallback, DateTime, Syslog, and Flows. Below the navigation bar, the page is divided into sections: Device Information, IP Address, and DNS Settings. In the 'Device Information' section, there is a 'Select Device' dropdown menu with 'Primary' selected. The 'IP Address' section contains two sub-sections: 'IPv4 Protocol' and 'IPv6 Protocol'. The 'IPv4 Protocol' section has checkboxes for 'Enable IPv4' (checked), 'Enable DHCP' (unchecked), and 'Enable SLAAC' (unchecked). Below these are input fields for 'IP Address', 'Subnet Mask', and 'Gateway IP Address'. The 'IPv6 Protocol' section has checkboxes for 'Enable IPv6' (checked), 'Enable SLAAC' (unchecked), and 'Enable DHCP' (unchecked). Below these are input fields for 'IPv6 Address' and 'Prefix'. The 'DNS Settings' section has input fields for 'Primary DNS' and 'Secondary DNS'. At the bottom of the page, there is a 'Save' button.

Administrator Interface NetFlow Host **Network Adapters** AppFlow Host SNMP Fallback DateTime Syslog Flows

Mobile Broadband Status

Device Information

Select Device

Primary

IP Address

IPv4 Protocol

☒ Enable IPv4

☐ Enable DHCP

☐ Enable SLAAC

IP Address * Subnet Mask * Gateway IP Address *

IPv6 Protocol

☒ Enable IPv6

☐ Enable SLAAC

☐ Enable DHCP

IPv6 Address * Prefix *

DNS Settings

Primary DNS Secondary DNS

Save

AppFlow host settings

AppFlow and IPFIX are flow export standards used to identify and collect application and transaction data in the network infrastructure. This data gives better visibility into application traffic utilization and performance.

The collected data, called flow records are transmitted to one or more IPv4 collectors. The collectors aggregate the flow records and generate real-time or historical reports. For more information, see [AppFlow and IPFIX](#).

To configure AppFlow Host Settings, navigate to **Configuration > Appliance Settings > AppFlow Host Settings** and click **Enable**. Specify the data update interval, in minutes, at which the AppFlow reports are exported to the AppFlow / IPFIX collector.

Choose one of the following AppFlow dataset templates:

- **TCP only for HDX:** Collects and sends multi-hop data of ICA connections to the AppFlow collector.
- **HDX:** Collects and sends HDX insight data of ICA connections to the AppFlow collector.

You can configure up to four AppFlow / IPFIX collectors. For each collector specify the following parameters:

- **IP Address:** The IP address of the external AppFlow / IPFIX collector system.
- **Port:** The port number on which the external AppFlow / IPFIX collector system listens. The default value is 4739. You can change the port number depending on the collector used.
- **AppFlow:** Sends flow records, as per IPFIX template 613, to IPFIX collectors.
- **Application Flow Info:** Sends flow records, as per IPFIX templates 611 and 612, to IPFIX collectors.
- **Citrix ADM:** Use Citrix ADM as the AppFlow collector. Provide the user name and password to seamlessly log in into Citrix ADM and store flow data.

Note

Citrix ADM currently does not support IPFIX collection.

AppFlow Host Settings

☒ Enable

Data Update Interval (minutes) :

5

Appflow Data Set:
☐ TCP only for HDX
☐ HDX

AppFlow / IPFIX Collector 1

IP Address

10.102.76.35

Port

4730

Data Set:
☐ Appflow
☒ Application Flow Info (IPFIX)
☐ Basic Properties (IPFIX)

☐ Citrix ADM

Citrix ADM user*

Password*

AppFlow / IPFIX Collector 2

IP Address

10.102.36.89

Port

4736

Data Set:
☐ Appflow
☐ Application Flow Info (IPFIX)
☐ Basic Properties (IPFIX)

☒ Citrix ADM

Citrix ADM

admin

Password

AppFlow / IPFIX Collector 3

IP Address

10.29.30.45

Port

4735

Data Set:
☒ Appflow
☒ Application Flow Info (IPFIX)
☐ Basic Properties (IPFIX)

☐ Citrix ADM

Citrix ADM

Password

AppFlow / IPFIX Collector 4

IP Address

10.102.89.46

Port

4732

Data Set:
☐ Appflow
☐ Application Flow Info (IPFIX)
☒ Basic Properties (IPFIX)

☐ Citrix ADM

Citrix ADM

Password

Save

SNMP

SNMP is used for exchanging management information between network devices. SNMPv1 is the first version of the SNMP protocol. SNMPv2 is the revised protocol, which includes enhancements in protocol packet types, transport mappings and MIB structure elements. SNMPv3 defines the secure version

of the SNMP. SNMPv3 protocol also facilitates remote configuration of the SNMP entities.

The SNMP agent collects the management information from the appliance locally and sends it to the SNMP manager whenever it is queried. If the agent detects an emergency event on the appliance, it sends out a warning message to the manager without waiting to be queried for data. This emergency message is called a trap. Enable the required SNMP version agents, the corresponding traps, and provide the required information. For more details see, SNMP.

To configure SNMP settings, navigate to **Configuration > Appliance Settings > SNMP**

SNMP

UDP Port:

System Description:

System Contact:

System Location:

SNMP v1/v2

☐ Enable v1/v2 Agent

Community String:

☐ Enable v1/v2 Traps

Destination IP Address(es):

Port:

SNMP v3

☐ Enable v3 Agent

User Name:

Password:

Verify Password:

Authentication:

Encryption:

☐ Enable v3 Traps

Destination IP Address(es):

Port:

User Name:

Password:

Verify Password:

Authentication:

Encryption:

Fallback configuration

Fallback configuration ensures that the appliance remains connected to the zero-touch deployment service if there is a link failure, configuration mismatch, or software mismatch. Fallback configuration is enabled by default on the appliances that have a default configuration profile. You can also edit the fallback configuration as per your existing LAN network settings. For more information, see [Fallback configuration](#).

Flows

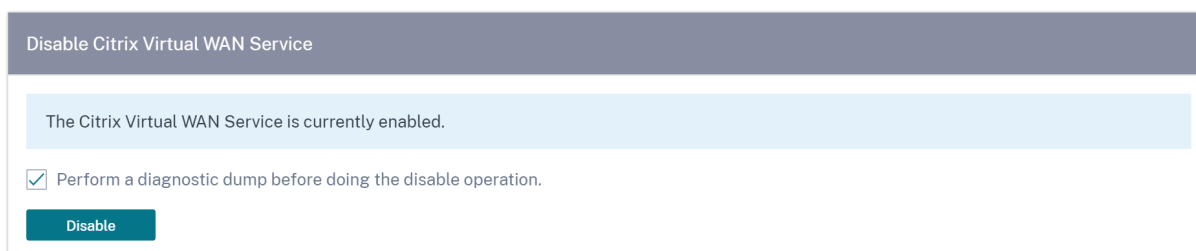
The flows section allows you to enable or disable Citrix Virtual WAN service on the appliance. Enabling the service enables and starts the Virtual WAN daemon. An option to enable Citrix Virtual Wan Service is available if the service is disabled.



Disable Citrix Virtual WAN service

The **Disable Citrix Virtual WAN Service** option is available if the service is enabled. Disabling the service stops the Virtual WAN daemon on the appliance.

You can choose to collect a diagnostic dump of the Virtual WAN network before disabling the Citrix Virtual WAN service.



Restart dynamic routing

You can restart the dynamic route learning process through OSPF and BGP routing protocols. The restart dynamic routing option is provided for troubleshooting only.

Warning

Restarting dynamic routing might result in network outage.

Restart Dynamic Routing

Restarting routing process may result in network outage. It is provided only for trouble shooting and can result in undesired behavior if performed when service is enabled.

Restart

Virtual paths

You can choose to enable or disable the virtual path between 2 sites. You can either choose the underlying individual paths, in either directions, or the overlay virtual path. Disabling individual paths, disables the entire virtual path.

Note

All paths are re-enabled after restarting the Citrix Virtual WAN Service.

Virtual Paths and Paths

Enable ▾

Virtual Path: London-Germany ▾

Notes:

Disabling all paths in either direction will cause the entire virtual path to be disabled.

Disabling a path or virtual path is not persistent across Citrix Virtual WAN Service restart operations. All paths will be re-enabled after a restart.

Submit

All paths on WAN link

You can choose to enable or disable WAN links between 2 sites. Disabling all WAN links, disables the Virtual path.

Note

All the WAN links are re-enabled after restarting the Citrix Virtual WAN Service.

All Paths on WAN Link

Enable ▾

WAN Link: London-Internet-AOL-1 ▾

Notes:

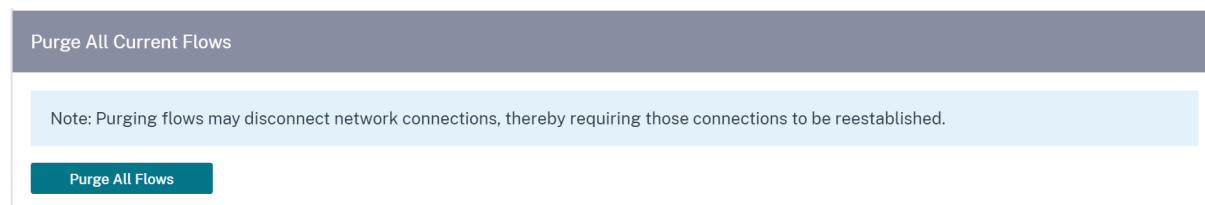
Disabling all paths in either direction will cause the entire virtual path to be disabled.

Disabling paths for a WAN Link is not persistent across Citrix Virtual WAN Service restart operations. All paths will be re-enabled after a restart.

Submit

Purge all current flows

Purging flows ends all the current flows, clears the flow tables, re-establishes flow connections, and repopulates the flow table.



Date and time

You can change the date and time of the appliance either manually or by using an NTP server. To configure date and time manually, ensure that the **Use NTP server** option is not selected and provide the date and time.

Date/Time Settings

NTP Settings

☐ Use NTP Server

NTP Server 1

time.nist.gov

NTP Server 2

NTP Server 2

NTP Server 3

NTP Server 3

NTP Server 4

NTP Server 4

Date/Time Settings

Date

01/03/2021

Time

6:51 AM

Save

If you select the **Use NTP server** option, then you cannot manually enter a current date and time. You can specify up to 4 NTP servers, but you must specify at least one. These act as backup NTP servers, if one server is down the appliance 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.

Date/Time Settings

NTP Settings

☒ Use NTP Server

NTP Server 1

time.nist.gov

NTP Server 2

NTP Server 2

NTP Server 3

NTP Server 3

NTP Server 4

NTP Server 4

Date/Time Settings

Date

01/03/2021

Time

6:23 AM

Save

If the time zone has to be changed, change it before setting the date and time, or else your settings do not persist. Reboot the appliance after changing the time zone.

Timezone Settings

After changing the timezone setting, a reboot will be necessary for the timezone changes to take full effect.

Until then, some logs will continue to use the actual timezone setting in effect at the time of the last reboot, even though events timestamps may reflect the new setting.

Timezone

UTC

Save

In-band management

April 7, 2021

SD-WAN Orchestrator for On-premises allows you to manage the SD-WAN appliance in two ways, out-of-band management and in-band management. Out-of-band management allows you to create a management IP using a port reserved for management, which carries management traffic only. In-band management allows you to use the SD-WAN data ports for management. It carries both data and management traffic, without having to configure an addition management path.

In-band management allows virtual IP addresses to connect to management services such as web UI and SSH. You can enable in-band management on a trusted interface that is enabled to be used for IP services. You can access the web UI and SSH using the management IP and in-band virtual IPs.

Note

In-band management in SD-WAN Orchestrator for On-premises is supported for Citrix SD-WAN 11.1.1 and higher.

To enable in-band management on a virtual IP, at the site level, navigate to **Configuration > Site Configuration > Interfaces**. Select the virtual IP to be used as the In-band management port. You can use the **InBand Management IP** or **InBand Management IPv6** to access the web UI and SSH.

Note

In-band management is supported on LAN ports only.

For detailed procedure on configuring a virtual IP address, see [Interfaces](#).

The In-band management IP also acts as a back-up management IP. It is used as the management IP address if the management port is not configured with a default gateway. Select the DNS proxy to which all DNS requests over the in-band management plane is forwarded to. For information on configuring DNS, see [DNS settings](#).

For use cases where the appliance connectivity to SD-WAN Orchestrator for On-premises toggles between management and in-band ports, configure **InBand Management DNS** or **InBand Management DNS V6** to ensure uninterrupted SD-WAN Orchestrator for On-premises connectivity.

In-band provisioning

The need to deploy SD-WAN appliances in simpler environments like home or small branches has increased significantly. Configuring separate management access for simpler deployments is an added overhead. Zero-touch deployment along with the in-band management feature enables provisioning

and configuration management through designated data ports. Zero-touch deployment is supported on the designated data ports and there is no need to use a separate management port for Zero-touch deployment.

You can provision an appliance in the factory shipped state, that supports in-band provisioning by connecting the data or management port to the internet. The appliances that support in-band provisioning have specific ports for LAN and WAN. The appliance in the factory reset state has a default configuration that allows to establish a connection with the zero-touch deployment service. The LAN port acts as the DHCP server and assigns a dynamic IP to the WAN port that acts as a DHCP client. The WAN links monitor the Quad 9 DNS service to determine WAN connectivity.

Once the IP address is obtained and a connection is established with the zero-touch deployment service the configuration packages are downloaded and installed on the appliance. For information on zero-touch deployment through the SD-WAN Orchestrator for On-premises, see [Zero Touch Deployment](#).

Note

- In-band provisioning is applicable to all the platforms. However, default configuration is enabled only on Citrix SD-WAN 110 and VPX platforms because the other platforms are shipped with an older software version.
- For day-0 provisioning of SD-WAN appliances through the data ports, the appliance software version must be Citrix SD-WAN 11.1.1 or higher.

The default configuration of an appliance in factory reset state includes the following configurations:

- DHCP Server on LAN port
- DHCP client on WAN port
- QUAD9 configuration for DNS
- Default LAN IP is 192.168.101.1/24 for Citrix SD-WAN appliances with factory image 11.1.1.39.
- Default LAN IP is 192.168.0.1/24 for Citrix SD-WAN 110 appliance with factory image 11.0.4.
- Grace License of 35 days.
- Interface 1/1 as LAN port.
- Interface 1/2 and LTE as WAN port

Once the appliance is provisioned, the default configuration is disabled and overridden by the configuration received from the zero-touch deployment service. If an appliance license or grace license expires, the default configuration is activated, ensuring that the appliance remains connected to the zero-touch deployment service and receives the license managed service.

Fallback configuration

Fallback configuration ensures that the appliance remains connected to the zero-touch deployment service if there is a link failure, configuration mismatch, or software mismatch. Fallback configuration

is enabled by default on the appliances that have a default configuration profile. You can also edit the fallback configuration as per your existing LAN network settings.

Note

After the initial appliance provisioning, ensure that the fallback configuration is enabled for zero-touch deployment service connectivity.

If the fallback configuration is disabled, you can enable it through Citrix SD-WAN Orchestrator service at the site level by navigating to **Configuration > Appliance Settings > Fallback** and click **Enable Fallback Configuration**.

The screenshot displays the 'Day 0' Default / 'Day N' Fallback Config page in the Citrix SD-WAN Orchestrator interface. The left sidebar shows the navigation menu with 'CONFIGURATION' expanded. The main content area has a breadcrumb trail: Administrator Interface > NetFlow Host Settings > Network Adapters > AppFlow Host Settings > SNMP > Fallback. The page title is 'Day 0' Default / 'Day N' Fallback Config. A blue banner states: 'The fallback configuration provides basic network functionality when a critical failure occurs and the system can no longer function.' Below this, a toggle switch for 'Enable Fallback Configuration' is highlighted with a red box. To the right of the toggle is a 'Reset' button. The 'LAN Settings' section contains the following fields:

- VLAN ID: 0
- IP Address: 192.168.101.1/24
- Enable DHCP Server: ☐
- DHCP Start: 192.168.101.50
- DHCP End: 192.168.101.250
- Dynamic DNS Servers: ☒
- DNS Server: (empty field)
- Alt DNS Server: (empty field)
- Internet Access: ☐

To customize the fallback configuration as per your LAN network, edit the values for the following LAN settings as per your network requirements. This is the minimum configuration required to establish a connection with the zero-touch deployment service.

- **VLAN ID:** The VLAN ID to which the LAN port must be grouped.
- **IP Address:** The virtual IP address assigned to the LAN port.
- **Enable DHCP Server:** Enables the LAN port as the DHCP server. The DHCP server assigns dynamic IP addresses to the WAN port.
- **DHCP Start and DHCP End:** The range of IP addresses which DHCP uses to assign an IP to the WAN port dynamically.
- **Dynamic DNS Server:** Enables the LAN port as the domain name server.
- **DNS Server:** The IP address of the primary DNS server.
- **Alt DNS Server:** The IP address of the secondary DNS server.
- **Internet Access:** Permit internet access to all LAN clients without other filtering.

'Day 0' Default / 'Day N' Fallback Config

The fallback configuration provides basic network functionality when a critical failure occurs and the system can no longer function.

☒ Enable Fallback Configuration

Reset

LAN Settings

VLAN ID

0

IP Address

192.168.101.1/24

☒ Enable DHCP Server

DHCP Start

192.168.101.50

DHCP End

192.168.101.250

☐ Dynamic DNS Servers

DNS Server

Alt DNS Server

☒ Internet Access

Configure the mode for each port. The port can be a LAN port or a WAN port or can be disabled. The ports displayed depend on the appliance model. Also, set the port bypass mode to **Fail-to-Block** or **Fail-to-wire**.

The following table provides the details of pre-designated WAN and LAN ports for fallback configuration on different platforms:

Platform	WAN Ports	LAN Ports
110	1/2	1/1
110-LTE	1/2, LTE-1	1/1
210	1/4, 1/5	1/3
210-LTE	1/4, 1/5, LTE-1	1/3
VPX	2	1
410	1/4, 1/5, 1/6	1/3 (FTB)
1100	1/4, 1/5, 1/6	1/3 (FTB)

Port Settings

Port	Mode		
1	<input type="radio"/> WAN	<input checked="" type="radio"/> LAN	<input type="radio"/> Disabled
2	<input checked="" type="radio"/> WAN	<input type="radio"/> LAN	<input type="radio"/> Disabled
3	<input type="radio"/> WAN	<input type="radio"/> LAN	<input checked="" type="radio"/> Disabled
4	<input type="radio"/> WAN	<input type="radio"/> LAN	<input checked="" type="radio"/> Disabled
5	<input type="radio"/> WAN	<input type="radio"/> LAN	<input checked="" type="radio"/> Disabled
6	<input type="radio"/> WAN	<input type="radio"/> LAN	<input checked="" type="radio"/> Disabled
7	<input type="radio"/> WAN	<input type="radio"/> LAN	<input checked="" type="radio"/> Disabled
8	<input type="radio"/> WAN	<input type="radio"/> LAN	<input checked="" type="radio"/> Disabled
MGT	<input type="radio"/> WAN	<input type="radio"/> LAN	<input checked="" type="radio"/> Disabled

Unassigned Port Bypass Mode

Fail to Block ▼

The WAN ports can be configured as independent WAN Links using the DHCP client and monitor the Quad9 DNS service to determine WAN connectivity. You can configure WAN IPs/static IPs for the WAN ports in the absence of DHCP to use In-band management for initial provisioning.

Note

You can only configure the Ethernet ports with the static IPs. The static IPs are not configurable with LTE-1 and LTE-E1 ports. Though you can add the LTE-1 and LTE-E1 port as WAN, the configuration fields remain non-editable.

When you add a WAN port, it is added under the **WAN Settings (Port: 2)** section with the **Enable DHCP** check box selected by default. If the **DHCP Mode** check box is selected, the **IP Address**, **Gateway IP Address**, **IP Address**, and the **VLAN ID** text fields are grayed out. Clear the **Enable DHCP** check box, if you want to configure static IP.

WAN Settings

Port	DHCP Mode	IP Address	Gateway IP Address	Vlan ID	WAN Tracking IP
2	<input checked="" type="checkbox"/> Enable DHCP			0	9.9.9.9

Save

By default, the **WAN Tracking IP Address** field is auto filled with the 9.9.9.9. You can change the address as needed.

Note

If you are selecting the **Dynamic DNS Servers** check box, ensure to add/configure at least one WAN port with the **DHCP Mode** selected.

To reset the fallback configuration to default configuration at any time, click **Reset**.

Note

It is recommended to enable fallback configuration on all appliances that are connected to Orchestrator through the In-band/Management Port connected to LAN subnet. Ensure that the default fall-back configuration is set up as per your network subnet requirements.

Port failover

SD-WAN Orchestrator for On-premises also allows to fail over management traffic seamlessly to the management port when the data port goes down and conversely. If an appliance can connect to the internet through both the management and in-band ports, the management port is chosen for zero-touch deployment.

On rebooting the appliance, if internet is available over the in-band port and not the management port, the appliance is connected to the SD-WAN Orchestrator for On-premises immediately.

Once the connection is established, a service agent running on the appliance sends the heartbeat information to the SD-WAN Orchestrator for On-premises every 10 seconds. If the SD-WAN Orchestrator for On-premises does not receive the heartbeat for 5 minutes, the In-band port failover is activated. SD-WAN Orchestrator for On-premises reports the appliance as offline during this period.

On rebooting the appliance, if internet is not available over both the management and in-band port and once internet connection is re-established, the service agent takes about 5 minutes to restart and establish a connection.

Ensure that the **Preserve route to internet from link even if all associated paths are down** option is enabled at the network level, **Configuration > Delivery Services > Internet**. Ensuring that the connectivity to the SD-WAN Orchestrator for On-premises is maintained even if the virtual path is down.

[Verify Config](#)[Service & Bandwidth](#)

Internet Service

Service Name	Cost
<input type="text" value="Internet"/>	<input type="text" value="5"/>

Advance Settings

☒ Preserve route to Internet from link even if all associated paths are down

Configurable management or data port

In-band management allows the data ports to carry both data and management traffic, eliminating the need for a dedicated management port. It leaves the management port unused on the low end appliances, which already have low port density. Citrix SD-WAN allows you to configure the management port to operate as either a data port or a management port.

Note

You can convert the management port to data port only on the following platforms.

- Citrix SD-WAN 110 SE/LTE
- Citrix SD-WAN 210 SE/LTE

While configuring a site, use the management port in your configuration. After the configuration is activated, the management port is converted to a data port.

Note

You can configure a management port only when in-band management is enabled on other trusted interfaces on the appliance.

To configure a management interface, at the site level, navigate to **Configuration > Site Configuration > Interfaces** and select the MGMT interface. For more information on configuring interface groups, see [Interfaces](#).

The screenshot displays the 'Interfaces' configuration page in the Citrix SD-WAN Orchestrator. The top navigation bar includes a home icon, a 'Verify Config' button, and tabs for '01 Site Details', '02 Device Details', '03 Interfaces' (selected), '04 WAN Links', '05 Routes', and '06 Summary'. The main content area is divided into three sections: 'Interface Attributes', 'Physical Interface', and 'Virtual Interfaces'. In the 'Interface Attributes' section, the 'Deployment Mode' is set to 'Edge (Gateway)', 'Interface Type' is 'LAN', 'Security' is 'Trusted', and 'Interface Name' is 'LAN-1'. The 'Physical Interface' section contains a 'Select Interface' dropdown with options 'LAG1', '1/1', 'LTE-E1', and 'MGMT'. The 'MGMT' option is highlighted with a red box. A link for 'Link Aggregation Group' is also present. The 'Virtual Interfaces' section is partially visible at the bottom.

To reconfigure the management port to perform management functionality, remove the configuration. Create a configuration without using the management port and activate it.

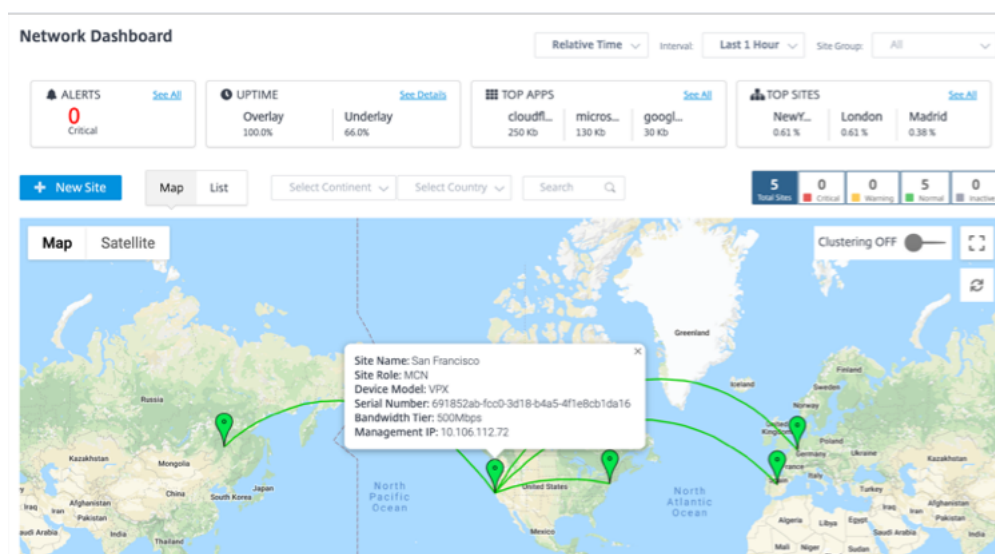
Customer/Network dashboard

January 11, 2021

The Network Dashboard provides a bird's eye view of an organization's SD-WAN network in terms of health and usage across all the sites. The dashboard captures a summary of the network-wide alerts, uptime of the overlay and underlay paths, highlights usage trends, and provides a global view of the network.

The dashboard summarizes the following aspects of a network, with a provision to drill down for more details.

- **Critical Alerts:** Running count of the critical health alerts, if any, popping up on the network.
- **Uptime:** Side-by-side comparison of the average uptime offered by the SD-WAN virtual overlay network v/s the physical underlay network
- **Usage Trends:** Top Apps - based on traffic volume and Top Sites - based on capacity utilization.
- **Network View:** A visual representation of all the sites across a network, available in both Map View and List View.



The map provides a real-time view of the global network with all the organization's sites depicted on a world map, based on their locations. The color of each site reflects its current health.

Following are the color-coding criteria used for each site:

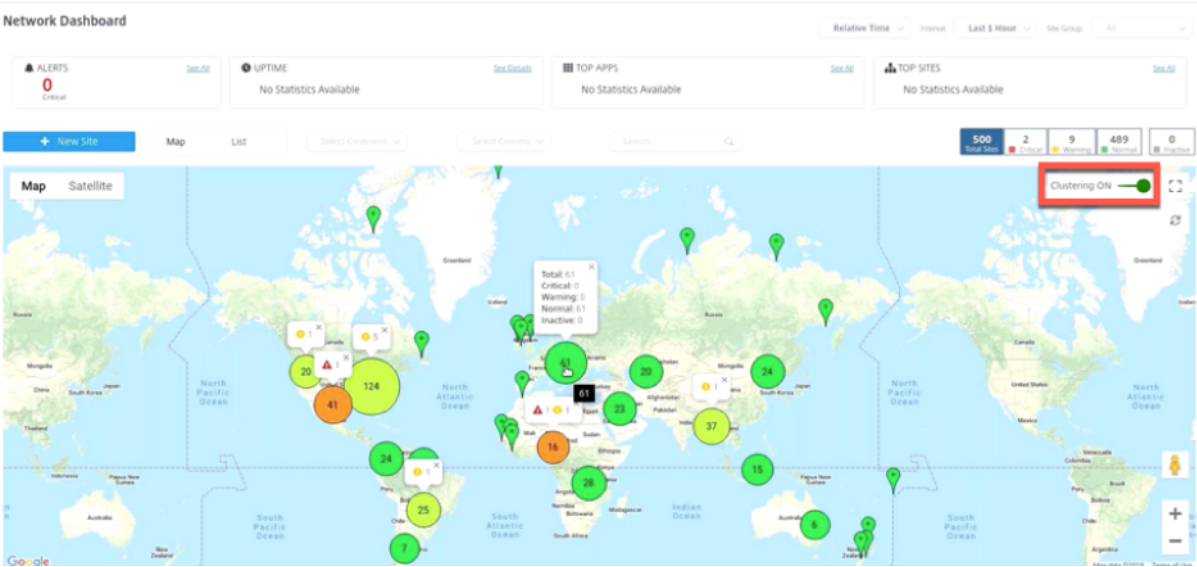
- **Critical (Red):** At least one overlay **virtual path** associated with a site is DOWN.
- **Warning (Orange):** At least one underlay member path is DOWN, but all the overlay virtual paths are UP.
- **Normal (Green):** All overlay virtual paths and the associated underlay member paths are UP.
- **Inactive (Grey):** Site is under-configuration and has not been deployed yet.

On hovering over any site, some of the key site-specific details such as the site role, device model, bandwidth tier is displayed. The virtual paths associated with a site show up with suitable color codes that reflect their health. The **List View** provides the same details for each site, summarized as entries in a table.




Clustering



The **Clustering ON** feature monitors the consistency, status, and health of various sites of a cluster or a combination of clusters. The Clustering ON service provides a real-time view of sites that help to monitor the failover and the current state of the site.

This **Clustering ON** feature is introduced to manage the high density of sites. It is not recommended to use the clustering off option when there are thousands of sites and it also brings down the performance.



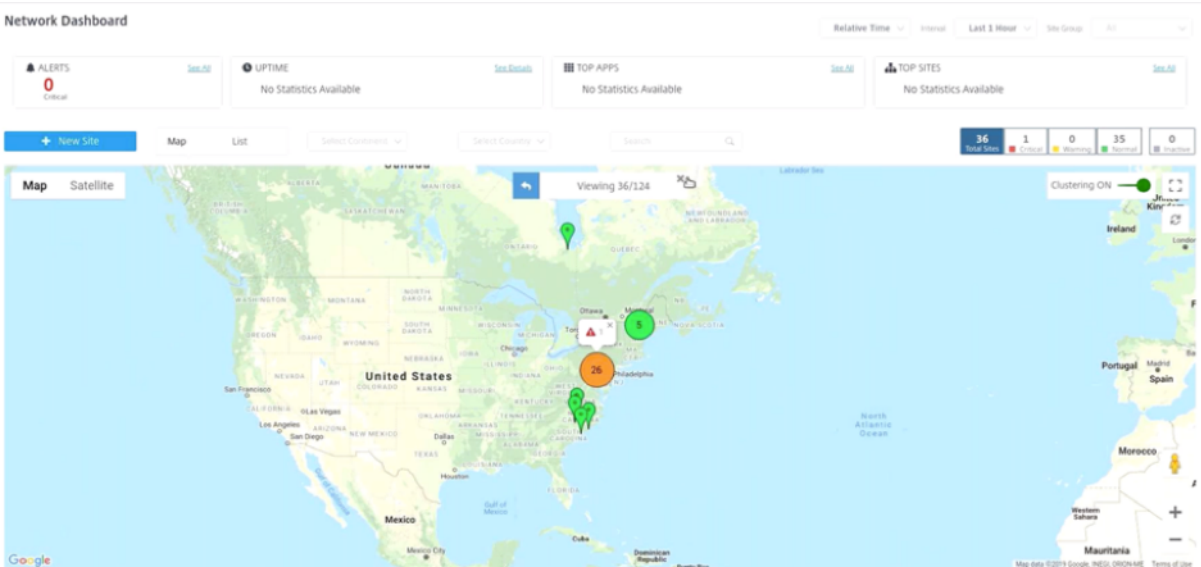
The following table describes the five colors shade that is used for clusters to represent the health of sites:

Color Legends	Description
	All sites in the cluster are green. That means each site has all the virtual paths, and the associated member paths UP
	All sites in the cluster are orange. That means each site has at least one member path DOWN, but all virtual paths UP
	All sites in the cluster are red. That means each site has at least one virtual path DOWN

Color Legends	Description
	The cluster has a combination of green and orange sites
	The cluster has a combination of red and non-red sites

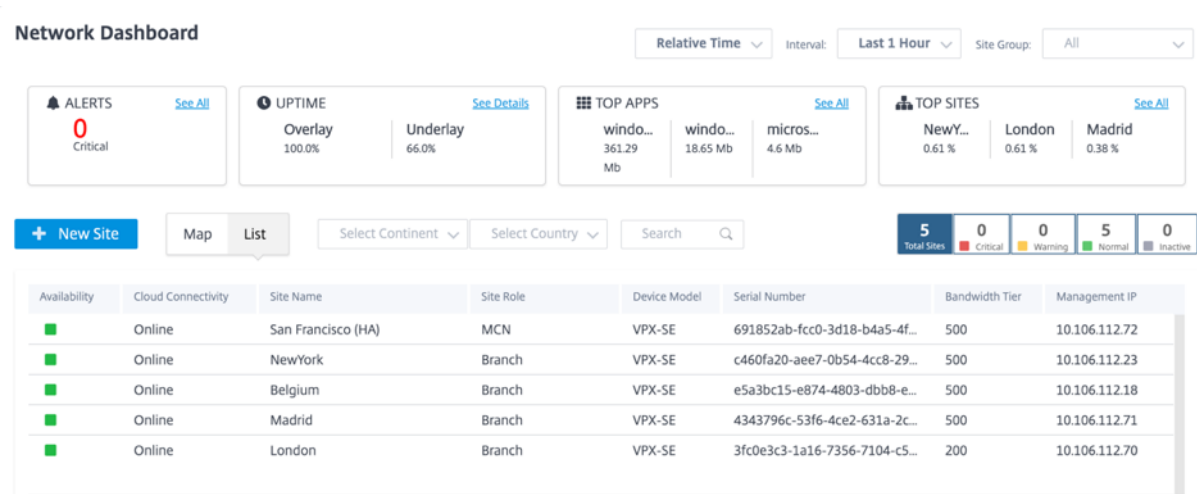
You can also verify the network aspect by hovering your mouse on any cluster. The critical or warning alerts are visible on top of the cluster as a pop-up.

If you click the cluster, it zooms into that cluster and shows other clusters. You can see a view bar with the number of clusters. The arrow option helps to bring you back one step. Click the **Close (X)** button to resume to the original page.



The **+ New Site** option is used to add a new site to the network. For information on site configuration workflow, see [Site configuration](#).

Alternatively, you can view the network summary in **List View**.



- Clicking any inactive “under-configuration” site that is yet to be deployed, would take you to the site configuration workflow.
- Clicking any active site, which has already been deployed, would take you to the **Site Dashboard**.

Note

Citrix SD-WAN overlay tunnels are called Virtual Paths. You would typically have one virtual path tunnel between each site and the Master Control Node (MCN), and extra site-site virtual paths as needed. Virtual paths are formed by bonding together the underlay WAN links / paths. So, each virtual path comprises multiple member paths.

This can be shown when a user hovers over the term virtual path or member path.

You can drag the **Pegman** onto the map to open the street view.



Site dashboard

October 21, 2020

The Site Dashboard provides an overview of a site's health and usage trends.

The dashboard summarizes the following aspects of a site, with a provision to drill down for more details.

- **Critical Alerts:** Running count of the critical health alerts, if any, popping up on the site.
- **Uptime:** Side-by-side comparison of the average uptime offered by the SD-WAN virtual overlay paths v/s the physical underlay paths, associated with a site
- **Usage Trends:** Top Apps and App Categories associated with a site, based on traffic volume
- **Site Details:** WAN Connections, and Devices associated with a site



Tip

Click **See All** or **See Details** to view statistics that are more detailed.

All the overlay virtual path connections associated with a site are displayed with suitable color-coding to reflect the health of each connection.

You can select any virtual path connection, to review the corresponding health metrics and trends.

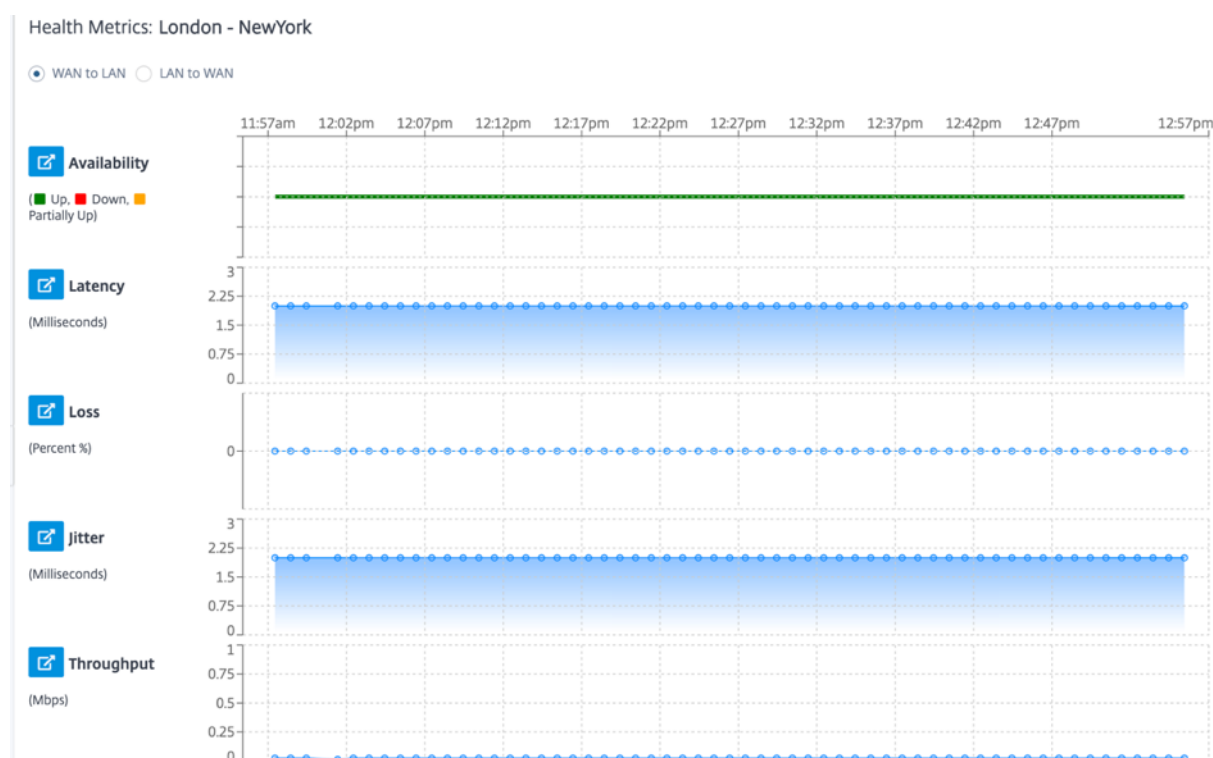
The color-coding criteria used for virtual path connections are:

- **Critical (Red):** Virtual path is DOWN.
- **Warning (Orange):** Virtual path is UP, but at least one member path is DOWN.
- **Normal (Green):** Virtual path and all member paths are UP.

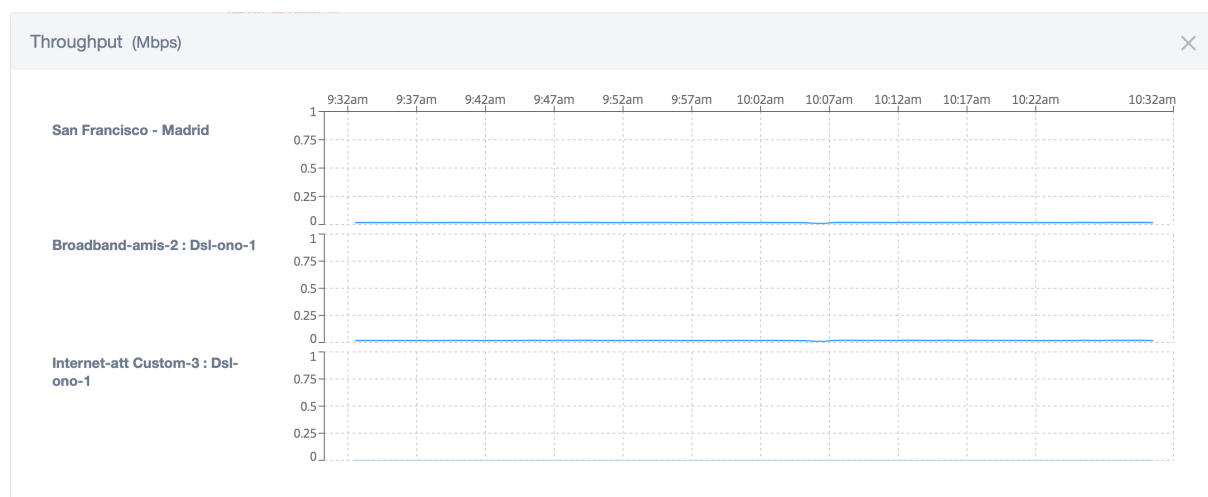
Health metrics

Health metrics and graphical trends around availability, latency, loss, jitter, and throughput are displayed for the selected virtual path connection. These statistics are available in both the directions:

WAN to LAN and **LAN to WAN**. All the metrics can be reviewed against a common timeline, to help quickly narrow down the problem domain while troubleshooting.



You can further drill down into each health metric to get a comparative view of the overlay virtual path and the underlay member paths for the same metric. This would aid in troubleshooting overlay versus underlay issues.



Devices

The **Devices** section displays details associated with the site's devices and interfaces. You can also reboot the appliance, reset the appliance configuration or download device logs.

WAN

DEVICES

Device Info

Availability	Cloud Connectivity	Uptime	Short Name	Device Model	Device Edition	Serial No.	Bandwidth	Management IP	Actions
<div>Up</div>	Yes	10 days 22 h...	Primary	CBVPX	SE	4343796c-5...	500 Mbps	10.106.112.71	<div></div> <div></div>

Interfaces (Primary)

STATUS	Interface Port	Bytes Sent	Bytes Received	Errors
<div>Up</div>	1	0	0	0
<div>Up</div>	2	4513	2136	0
<div>Up</div>	3	32	0	0
<div>Up</div>	4	3945	2023	0

March 8, 2021

Network Troubleshooting

Customers can view logs of all the network appliances from a single pane of glass, enabling quick troubleshooting. You can view audit and device logs.

Audit logs

Audit logs capture the action, time, and result of the action performed by users in the customer network.

Network Troubleshooting : Audit Logs

Search

Time	User	Action	Result
September 19, 2019 5:37 PM	sandeepmanohar.nirikhi@citrix.com	Update USER: sandeepmanohar.nirikhi@citrix.com	OK(200)
September 19, 2019 5:37 PM	sandeepmanohar.nirikhi@citrix.com	Create USER: sandeepmanohar.nirikhi@citrix.com	OK(200)
September 19, 2019 3:54 PM	sandeepmanohar.nirikhi@citrix.com	Create USER: sandeepmanohar.nirikhi@citrix.com	OK(200)
September 19, 2019 3:53 PM	sandeepmanohar.nirikhi@citrix.com	Create USER: sandeepmanohar.nirikhi@citrix.com	OK(200)
September 19, 2019 3:53 PM	sandeepmanohar.nirikhi@citrix.com	Create USER: sandeepmanohar.nirikhi@citrix.com	OK(200)
September 19, 2019 3:52 PM	sandeepmanohar.nirikhi@citrix.com	Create USER: sandeepmanohar.nirikhi@citrix.com	OK(200)
September 19, 2019 3:51 PM	sandeepmanohar.nirikhi@citrix.com	Create USER: sandeepmanohar.nirikhi@citrix.com	OK(200)
September 19, 2019 3:36 PM	abhishek.kumar5@citrix.com	Create USER: abhishek.kumar5@citrix.com	OK(200)
September 19, 2019 3:33 PM	sandeepmanohar.nirikhi@citrix.com	Update SITE: San Francisco	OK(200)
September 19, 2019 3:33 PM	sandeepmanohar.nirikhi@citrix.com	Update DEVICE: 691852ab-fcc0-3d18-b4a5-...	OK(200)
September 19, 2019 3:33 PM	sandeepmanohar.nirikhi@citrix.com	Update DEVICE: 4ffa8122-3baa-5d43-315c-...	OK(200)
September 19, 2019 3:33 PM	sandeepmanohar.nirikhi@citrix.com	Update CONFIG: Abycare Hospitals	OK(200)

Device logs

Customers can view the device logs that are specific to sites.

You can select specific device logs, download it, and share it with site admins if necessary.

Network Troubleshooting : Device Logs

Select Site
San Francisco

Download (0 Bytes / 1 GB)

Search Device Logs

<input type="checkbox"/>	Name	Last Modified	Size
<input type="checkbox"/>	init.log	September 20, 2019 11:10 AM	2.76 MB
<input type="checkbox"/>	SDWAN_filetransfer.log	September 20, 2019 11:10 AM	1.66 MB
<input type="checkbox"/>	SDWAN_ip_learned.log	September 20, 2019 11:10 AM	1.21 MB
<input type="checkbox"/>	SDWAN_snmp_poll.log	September 20, 2019 11:10 AM	1.66 MB
<input type="checkbox"/>	SDWAN_config_update.old.log	September 20, 2019 11:10 AM	1.91 MB
<input type="checkbox"/>	SDWAN_snmp_poll.old.log	September 20, 2019 11:10 AM	1.91 MB
<input type="checkbox"/>	SDWAN_dynamic_virtual_path.old.log	September 20, 2019 11:10 AM	7.63 MB
<input type="checkbox"/>	SDWAN_management.log	September 20, 2019 11:10 AM	1.51 MB
<input type="checkbox"/>	SDWAN_filetransfer.old.log	September 20, 2019 11:10 AM	1.91 MB
<input type="checkbox"/>	SDWAN_common.old.log	September 20, 2019 11:10 AM	3.81 MB
<input type="checkbox"/>	SDWAN_dynamic_virtual_path.log	September 20, 2019 11:10 AM	1.66 MB
<input type="checkbox"/>	SDWAN_igmp_proxy.old.log	September 20, 2019 11:10 AM	1.91 MB
<input type="checkbox"/>	SDWAN_security.old.log	September 20, 2019 11:10 AM	1.91 MB
<input type="checkbox"/>	dynamic_routing.log	September 20, 2019 11:10 AM	123.47 KB

Site troubleshooting

October 21, 2020

Device logs

Logs are useful to troubleshoot issues. The site administrator can view a list of all the logs that are captured across all the devices at the site. You can also download logs for further verification.

Download (0 Bytes / 1 GB)

Search Device Logs

<input type="checkbox"/>	Name	Last Modified	Size
<input type="checkbox"/>	ps.1.log	February 25, 2020 10:12 AM	24.52 MB
<input type="checkbox"/>	init.log	February 25, 2020 10:12 AM	2.65 MB
<input type="checkbox"/>	SDWAN_filetransfer.log	February 25, 2020 10:12 AM	1.08 MB
<input type="checkbox"/>	SDWAN_ip_learned.log	February 25, 2020 10:12 AM	1.08 MB
<input type="checkbox"/>	SDWAN_snmp_poll.log	February 25, 2020 10:12 AM	1.07 MB
<input type="checkbox"/>	SDWAN_config_update.old.log	February 25, 2020 10:12 AM	1.91 MB
<input type="checkbox"/>	SDWAN_snmp_poll.old.log	February 25, 2020 10:12 AM	1.91 MB
<input type="checkbox"/>	SDWAN_dynamic_virtual_path.old.log	February 25, 2020 10:12 AM	7.63 MB
<input type="checkbox"/>	SDWAN_management.log	February 25, 2020 10:12 AM	32.42 KB
<input type="checkbox"/>	launch_proc.log	February 25, 2020 10:12 AM	38.02 KB
<input type="checkbox"/>	SDWAN_filetransfer.old.log	February 25, 2020 10:12 AM	1.91 MB
<input type="checkbox"/>	SDWAN_common.old.log	February 25, 2020 10:12 AM	3.81 MB
<input type="checkbox"/>	SDWAN_dynamic_virtual_path.log	February 25, 2020 10:12 AM	1.07 MB

Show Tech Support Bundle

The Show Tech Support (STS) Bundle contains important real-time system information such as access logs, diagnostics logs, firewall logs. The STS bundle is used to troubleshoot issues in the SD-WAN appliances. You can create, download the STS bundle, and share it with Citrix Support Representatives.

If a site is configured in HA deployment mode, you can select the **Active or Standby appliance** for which to create or download the STS bundle.





To create a new STS bundle for a site appliance, at the site level, navigate to **Troubleshooting > STS bundle** and click **Create New**.

Select Device

Active

Create New

Search

Name	Last Updated At	File Size	Status	Action
bangalore_mcn-8dc156e...	August 12, 2020 2:11 PM	16.04 MB	Available For Download	 
new_test-8dc156e9-af52...	August 11, 2020 10:36 AM	16.34 MB	Available For Download	 

* STS is Available for Only 5 Days

Provide a name for the STS bundle. The name must begin with a letter and can contain letters, numbers, dashes, and under-scores. The maximum length of the name is 32 characters. The user provided name is used as a prefix in the final name. The service generates a full name to ensure unique names (timestamp) and to help recognize the device from the STS package (serial number). If no name is provided a name is auto-generated while creating the bundle.

Create Diagnostic Information Dump

Create a diagnostic dump.

If the filename is left blank, one will be auto-generated.

Filename

sts-bundle-1

Cancel

Create

At any given time, the STS process is in one of the following states:

STS Status	Description
Requested	A new STS bundle is requested. This takes a few minutes. You can choose to cancel the STS creation process, if necessary.
Uploading	The created STS package is uploaded to the cloud service. The duration depends on the size of the package. The status is updated every 5 seconds. You cannot cancel the STS upload process.
Failure	The STS process has failed during creation or upload. You can delete the entries of failed STS operations.
Available for download	The STS creation and upload process are successful. You can now download or delete the STS packages.

The STS bundles and failure records are maintained for 7 days, post which it is auto-deleted.

April 22, 2021

Customer/Network reports

The **Customer Reports** provide visibility into network-wide alerts, usage trends, inventory, quality, diagnostics, and firewall status aggregated across all the sites in a customer network.

Alerts

The customer can review a detailed report of all the events and alerts generated across all the sites in this network.

It includes the severity, site at which the alert originated, alert message, time, and other details.

Network Reports : Alerts					
					Site Group: All
Delete Alerts					509 TOTAL 41 HIGH 67 MEDIUM 401 LOW
Search					
<input type="checkbox"/>	Severity	Site	Source	Message	Time
<input type="checkbox"/>	Low	San Francisco	APPLIANCE	The state of Virtual Path San_Francisco-Madrid has changed from BAD to GOOD	Jan 30th 2020, 12:35 am
<input type="checkbox"/>	Low	San Francisco	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-...	Jan 30th 2020, 12:35 am
<input type="checkbox"/>	Low	San Francisco	APPLIANCE	Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DS...	Jan 30th 2020, 12:35 am
<input type="checkbox"/>	Low	San Francisco	APPLIANCE	Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DS...	Jan 30th 2020, 12:35 am
<input type="checkbox"/>	Low	San Francisco	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-...	Jan 30th 2020, 12:35 am
<input type="checkbox"/>	High	San Francisco	APPLIANCE	The Virtual Path San_Francisco-Madrid is no longer DEAD	Jan 30th 2020, 12:35 am
<input type="checkbox"/>	Low	NewYork	APPLIANCE	WAN Link NewYork-Internet-AOL-1 is now up.	Jan 30th 2020, 12:16 am
<input type="checkbox"/>	Low	San Francisco	APPLIANCE	Ethernet link on device 4 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am

Suitable filtering options can be used as needed for example: Look for all the high severity alerts across all the sites, or all the alerts for a particular site and so on.

You can also select and clear alerts.

Usage

Customers can review usage trends such as **Top Applications**, **Top Application Categories**, **App Bandwidth**, and **Top Sites** across all the sites in their network.

Top application and application categories

The **Top Applications** and **Top Application Categories** chart shows the top applications and top application families that are widely used across all the sites. This allows you to analyze the data consumption pattern and reassign the bandwidth limit for each class of data within the network.

Network Reports : Usage

Relative Time

Interval: Last 1 Hour

Site Group: All

Application Usage Network Usage

Report Type

Apps

Top Apps

All

Top Applications

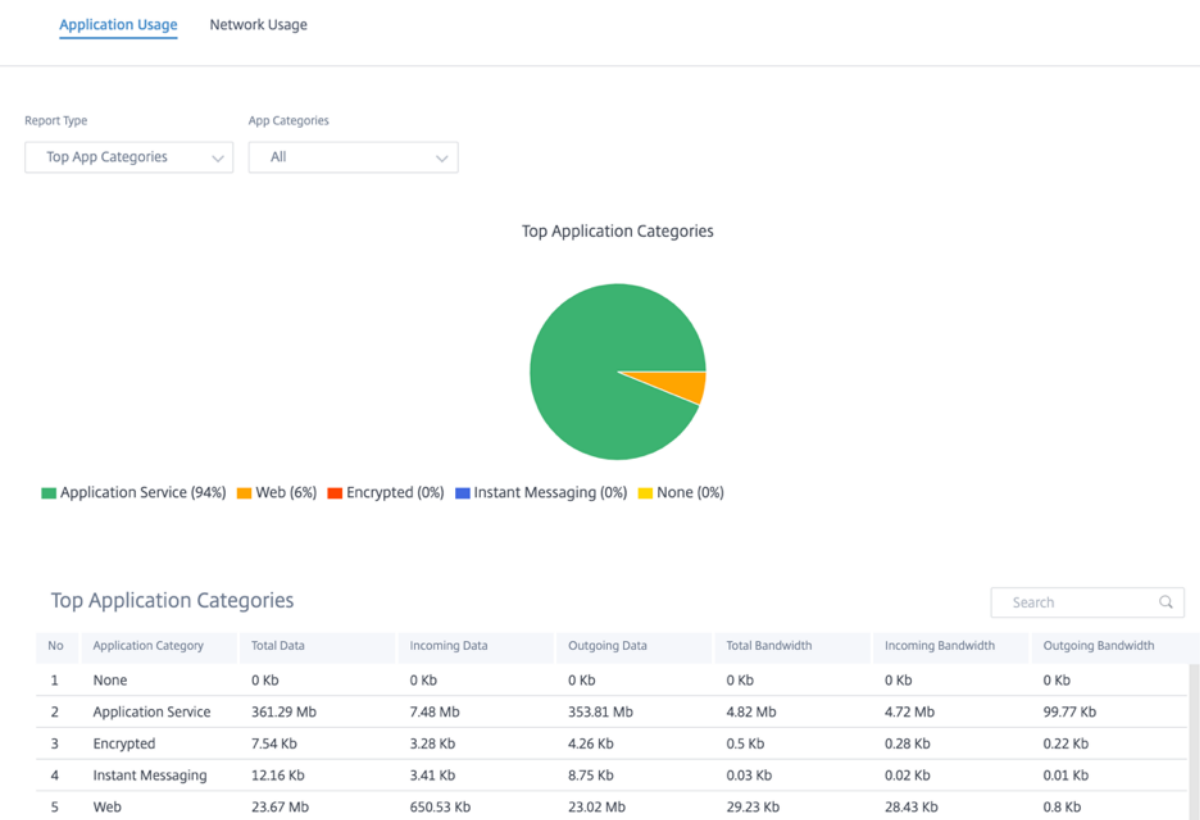


windows_marketplace (94%) windows_update (5%) microsoft (1%) lync_online (0%) cloudflare (0%) Others (0%)

Top Applications

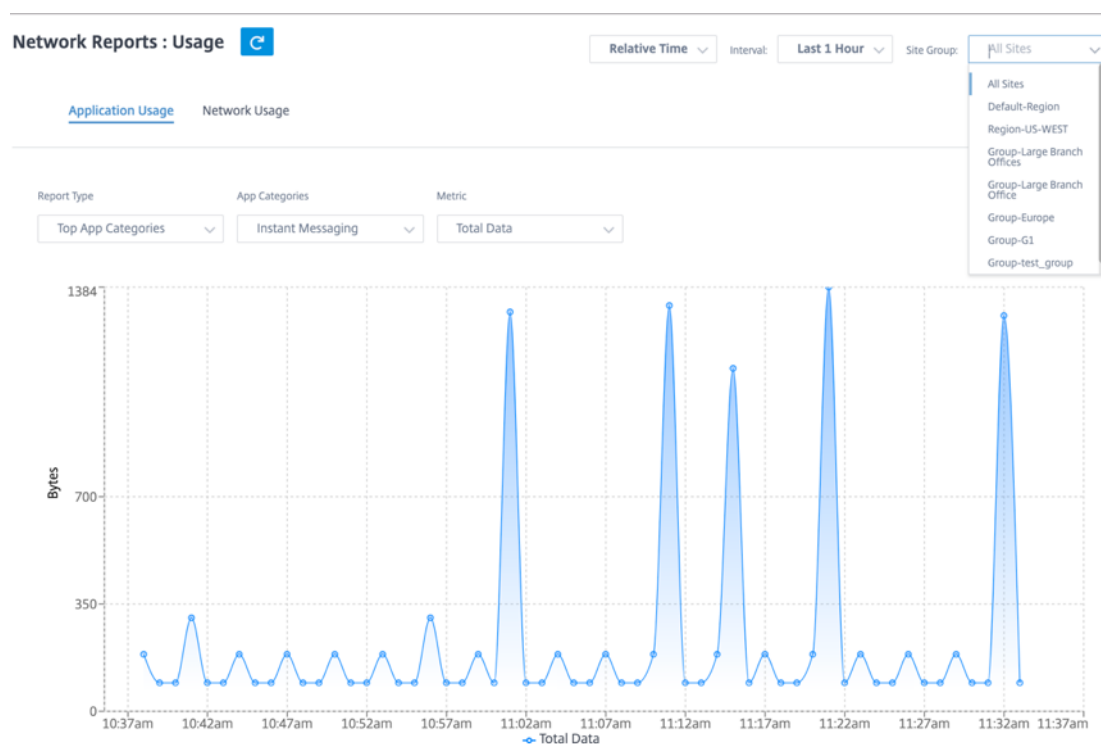
Search

No	Applications	Total Data	Incoming Data	Outgoing Data	Total Bandwidth	Incoming Bandwidth	Outgoing Bandwidth
1	Unknown	0 Kb	0 Kb	0 Kb	0 Kb	0 Kb	0 Kb
2	https	44.54 Kb	17.57 Kb	26.97 Kb	2.97 Kb	1.8 Kb	1.17 Kb
3	windowslive	19.77 Kb	6.53 Kb	13.23 Kb	1.32 Kb	0.88 Kb	0.44 Kb
4	ocsp	7.54 Kb	3.28 Kb	4.26 Kb	0.5 Kb	0.28 Kb	0.22 Kb
5	windows_update	18.65 Mb	381.6 Kb	18.27 Mb	226.08 Kb	221.45 Kb	4.63 Kb
6	google_gen	34.6 Kb	9.61 Kb	24.99 Kb	1.15 Kb	0.83 Kb	0.32 Kb
7	windows_marketpl...	361.29 Mb	7.48 Mb	353.81 Mb	4.82 Mb	4.72 Mb	99.77 Kb



Application bandwidth

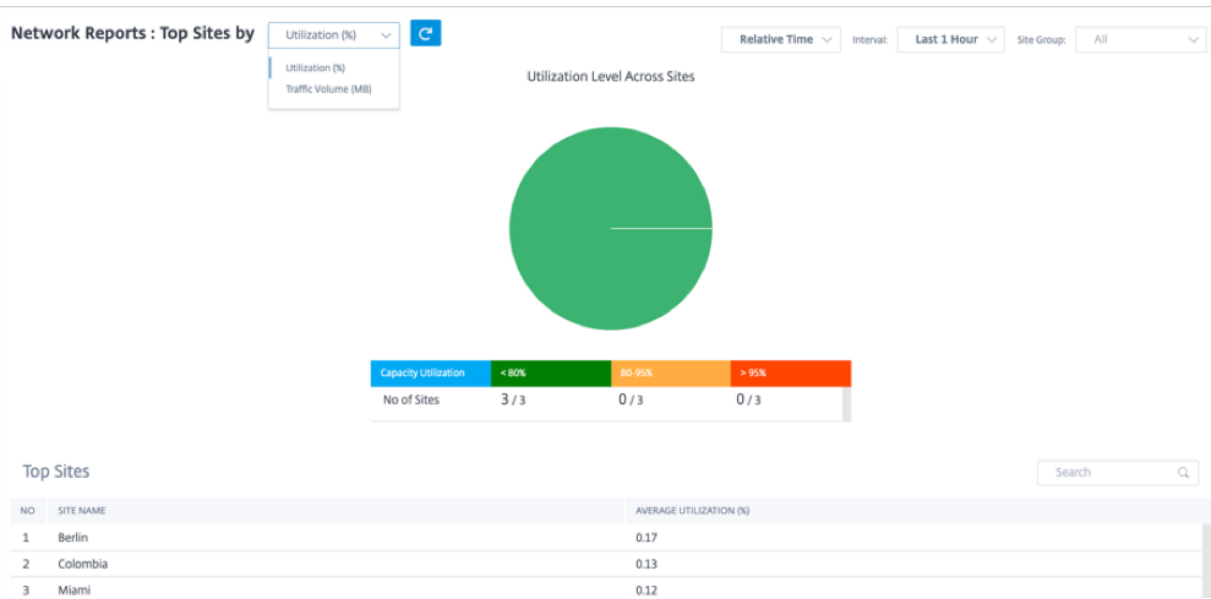
You can view the bandwidth usage statistics for the selected site group or for all sites. The bandwidth statistics are collected for the selected time interval. You can filter the statistics report based on the **Report Type, Apps or Apps Categories, and Metrics.**



- **Report Type:** Select **Top App or App Categories** from the list.
- **Apps/App Categories:** Select top application or categories (such as network service) from the list.
- **Metric:** Select the bandwidth metric (such as Total Data, Incoming Data, Total Bandwidth) from the list.

Network usage

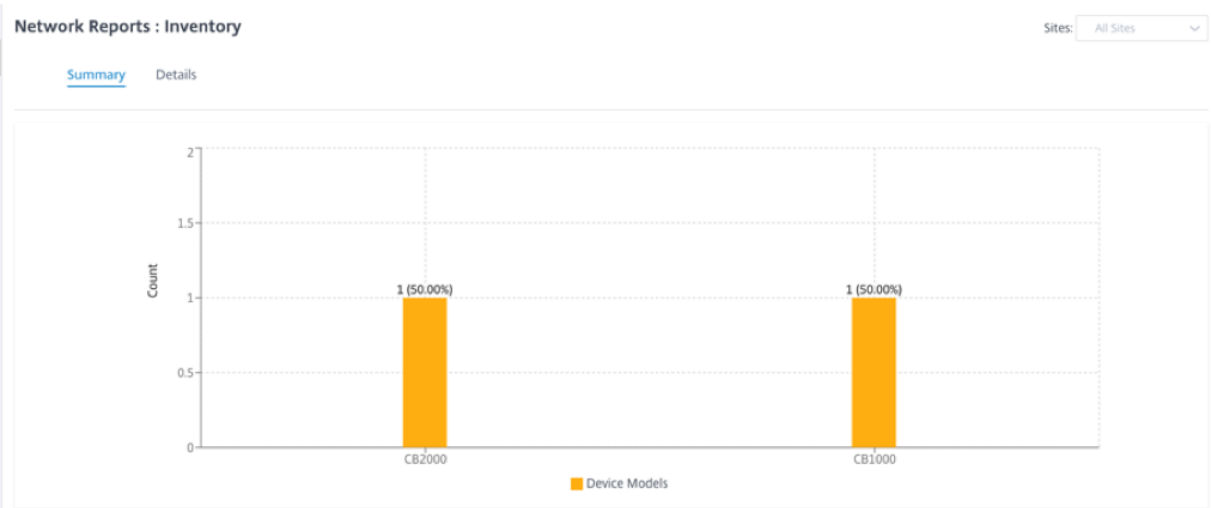
The **Top Sites** chart depicts the top sites in the customer network that have the highest bandwidth usage. You can view the Sites by Utilization (%) or Traffic Volume (MB).



Inventory

The customer can view the entire device inventory across all the sites in the network. You can choose to view an inventory summary or a detailed view.

The inventory summary view provides a chart of the inventory spread, depicting the various appliance models and the number of each type of appliances used across all sites in the customer network.



Suitable filtering options can be used as needed for example: Look for all appliances belonging to a specific site, or all appliances with a certain device model and so on

The inventory detailed view provides a list of all the appliances that are deployed and those appliances that are configured but not deployed yet. Along with the customer, site name, device role, device serial number, current software, and device management IP address.

Network Reports : Inventory

Sites: All Sites

SummaryDetails

Search

DEPLOYEDUNDEPLOYED

SITE NAME	DEVICE ROLE	DEVICE MODEL	SERIAL NUMBER	CURRENT SOFTWARE	MANAGEMENT IP
SFO	MCN	2000	7A9D12F8VZ	10.1.1.37.715522	10.200.33.72
Chennai	Branch	1000	JNHF2CKG1X	10.1.1.37.715522	10.200.32.42

Page Size: 25

Showing 1 - 2 of 2 items

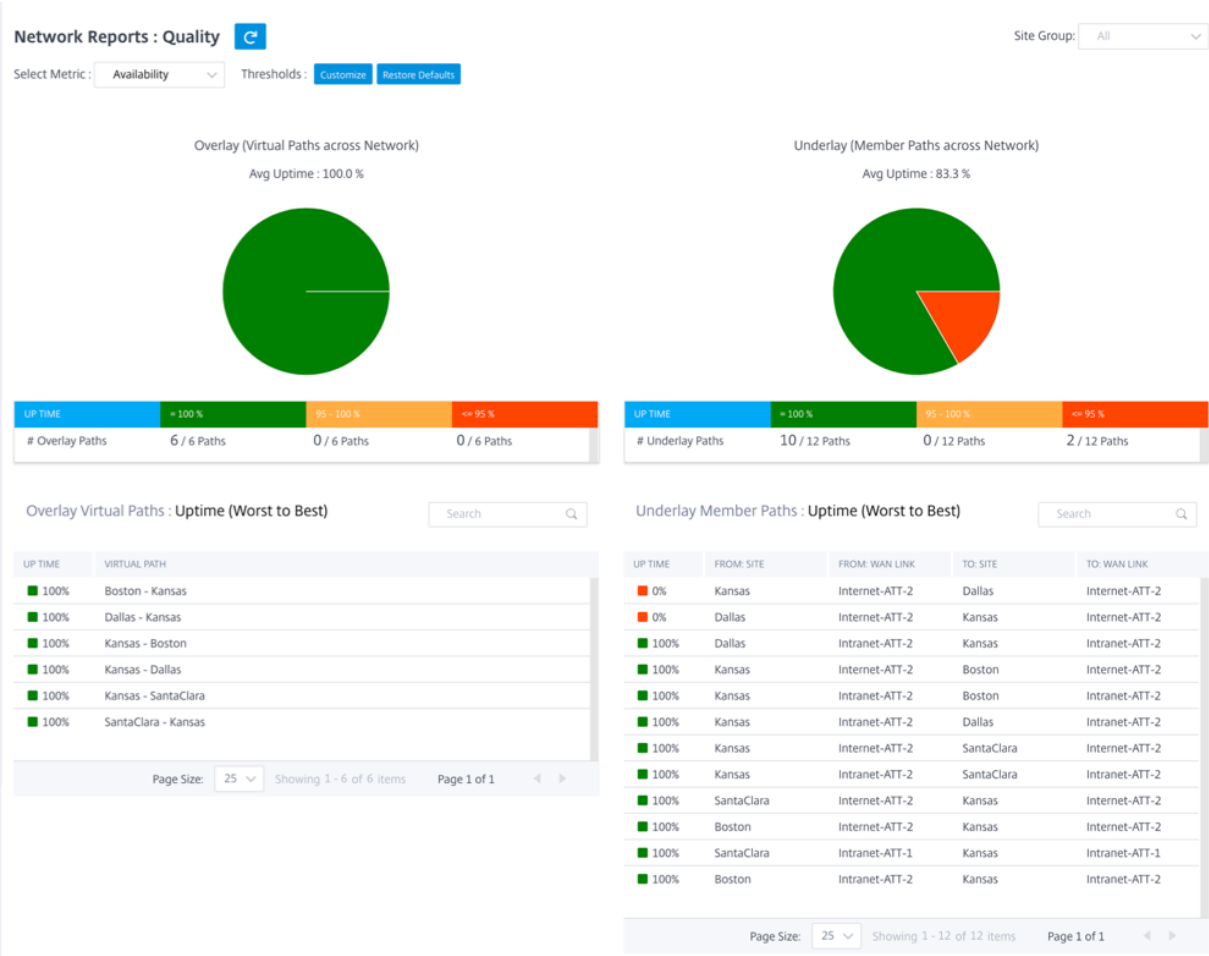
Page 1 of 1

HDX dashboard and reports

For details on HDX dashboard and reports, see [HDX dashboard and reports](#).

Quality

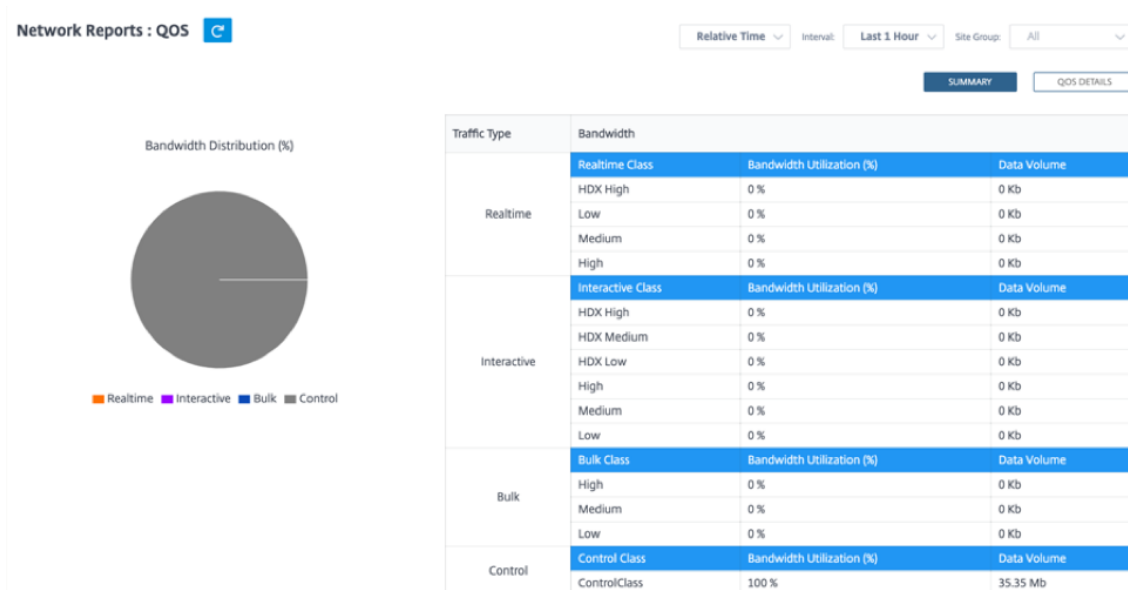
The **Network Quality Report** enables a network-level comparison between the virtual overlay and the physical underlay in terms of uptime, loss, latency, and jitter. This helps effectively monitor how the overlay is faring relative to the underlay network, and also aids troubleshooting.



Quality of Service

Quality of Service (QoS) manages data traffic to reduce packet loss, latency, and jitter on the network. For more information, see [Quality of Service](#). The following are two ways to view the Quality-of-Service (QoS) report:

- **Summary View:** Summary view provides an overview of bandwidth consumption across all types of traffic - real-time, interactive, bulk, and control across the network and per site.



- **Real-time:** Used for low latency, low bandwidth, time-sensitive traffic. Real-time applications are time sensitive but don't really need high bandwidth (for example voice over IP). Real-time applications are sensitive to latency and jitter, but can tolerate some loss.
- **Interactive:** Used for interactive traffic with low to medium latency requirements and low to medium bandwidth requirements. Interactive applications involve human input in the form of mouse clicks or cursor moves. The interaction is typically between a client and a server. The communication might not need high bandwidth but is sensitive to loss and latency. However, server to client does need high bandwidth to transfer graphical information, which might not be sensitive to loss.
- **Bulk:** Used for high bandwidth traffic that can tolerate high latency. Applications that handle file transfer and need high bandwidth are categorized as bulk class. These applications involve little human interference and are mostly handled by the systems themselves.
- **Control:** Used to transfer control packets that contain routing, scheduling, and link statistics information.
- **Detailed View:** The detailed view captures trends around bandwidth consumption, traffic volume, packets dropped and so on for each QoS class associated with an overlay virtual path.

Network Reports : QOS

Relative Time Interval: Last 1 Hour Site Group: All

SUMMARY QOS DETAILS

Site: All Traffic Type: All Select Priority: All

SITE	VIRTUAL PATH	TRAFFIC TYPE	PRIORITY	BANDWIDTH	DATA VOLUME	DROP (%)	DROP VOLUME
Berlin	Berlin-Miami	Control	ControlClass	13.44 Kbps	5.95 Mb	0 %	0 Kb
Berlin	Berlin-Colombia	Control	ControlClass	23.03 Kbps	10.19 Mb	0 %	0 Kb
Miami	Miami-Berlin	Control	ControlClass	17.35 Kbps	7.68 Mb	0 %	0 Kb
Colombia	Colombia-Berlin	Control	ControlClass	26.98 Kbps	11.94 Mb	0 %	0 Kb

Page Size: 25 Showing 1 - 4 of 4 items Page 1 of 1

This report is available at the site level where the user can view QoS statistics based on the virtual path between the two sites. For more information see [Site reports](#).

Historical statistics

For each site, you can view the statistics as graphs for the following network parameters:

- Sites
- Virtual Paths
- Paths
- WAN Links
- Interfaces
- Classes
- GRE Tunnels
- IPsec Tunnels

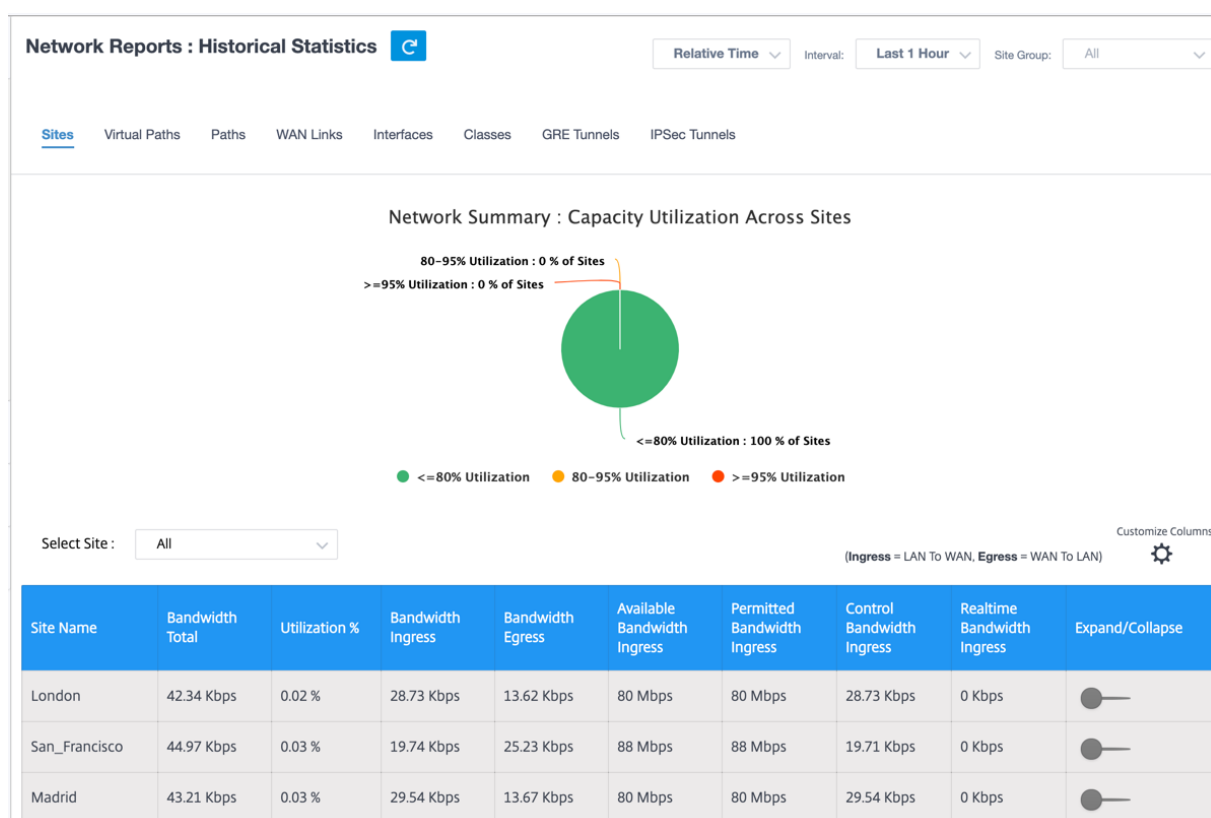
The statistics are collected as graphs. These graphs are plotted as timeline versus usage, allowing you to understand the usage trends of various network object properties. You can view graphs for network-wide application statistics.

You can view or hide the graphs and customize the columns as needed.

Sites

To view the Site statistics, navigate to **Reports > Historical Statistics > Sites** tab.

Select the site name from the list.

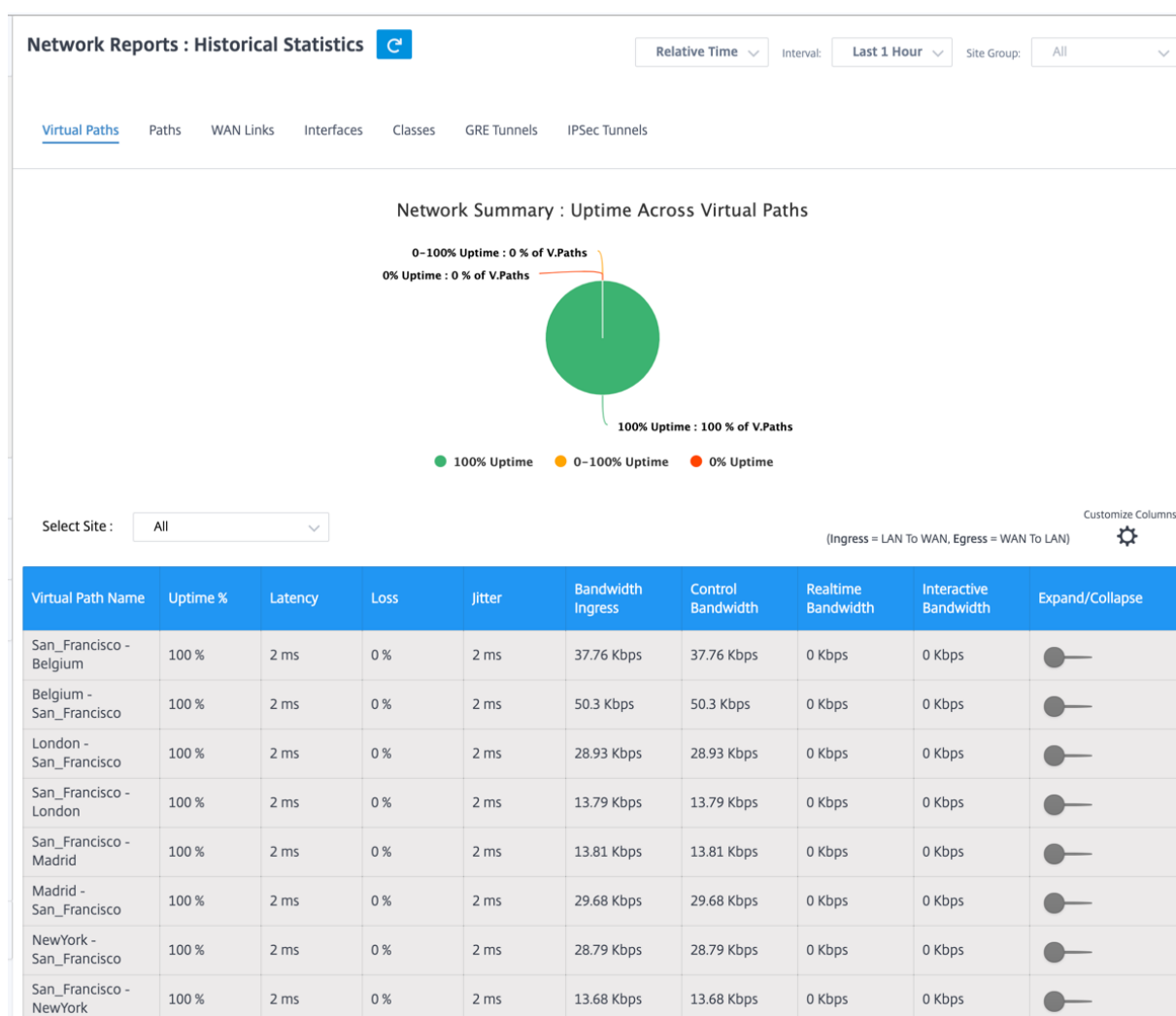


You can view the following metrics:

- **Site Name:** The site name.
- **Bandwidth Total:** Total bandwidth consumed by all packet types. Bandwidth = Control Bandwidth + Real-time Bandwidth + Interactive Bandwidth + Bulk Bandwidth.
- **Utilization:** You can view the site statistics by Utilization (%).
- **Bandwidth Ingress:** The max and the min download speed through the WAN port.
- **Bandwidth Egress:** The max and the min upload speed through the WAN port.
- **Available Bandwidth Ingress:** Total bandwidth allocated to all the WAN links of a site.
- **Permitted Bandwidth Ingress:** Bandwidth available for transmitting information.
- **Control Bandwidth Ingress:** Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.
- **Realtime Bandwidth Ingress:** Bandwidth consumed by applications that belong to the real-time class type in the NetScaler SD-WAN configuration. The performance of such applications depends on a great extent upon network latency. A delayed packet is worse than a lost packet (for example, VoIP, Skype for Business).
- **Expand/Collapse:** You can expand or collapse the data as needed.

Virtual paths

To view the **Virtual Paths** statistics, navigate to **Reports > Statistics > Virtual Paths** tab.



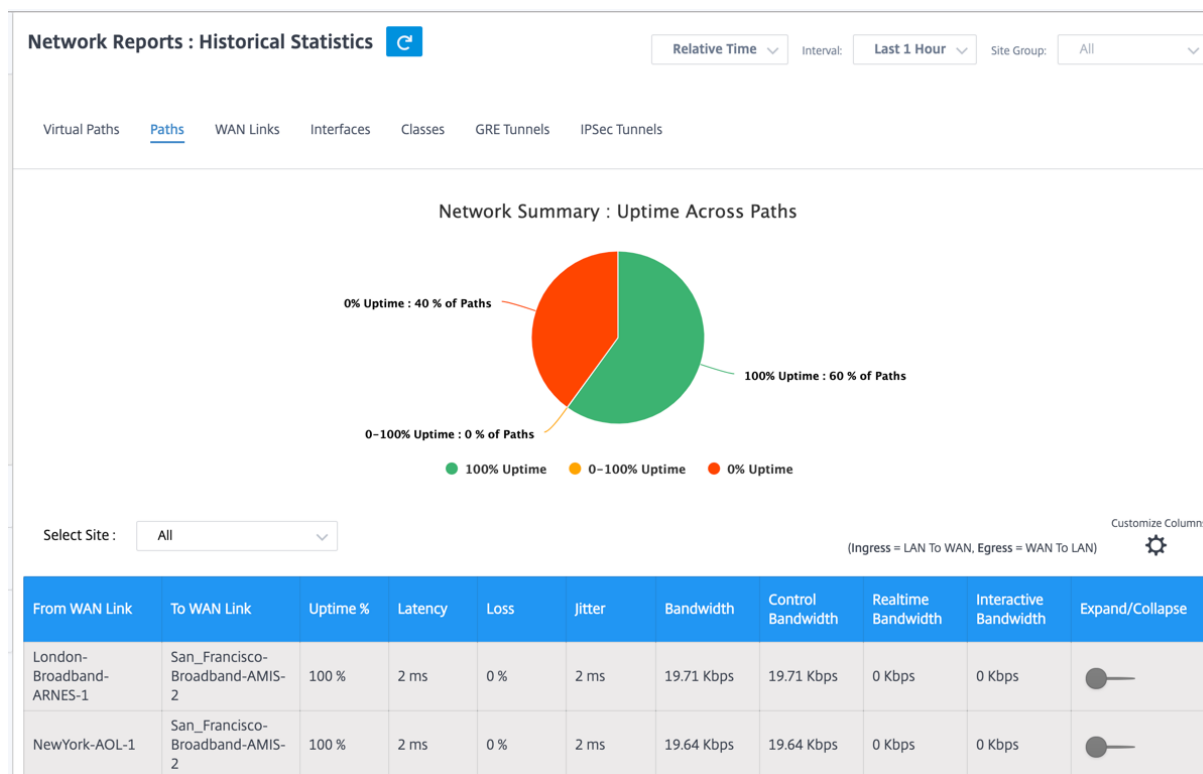
You can view the following metrics:

- **Virtual Path Name:** The virtual path name.
- **Latency:** The latency in milliseconds for real-time traffic.
- **Loss:** Percentage of packets lost.
- **Jitter:** Variation in the delay of received packets, in milliseconds.
- **Bandwidth Ingress:** Ingress (LAN to WAN) Bandwidth usage for the selected time period.
- **Control Bandwidth:** Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.
- **Real-time Bandwidth:** Bandwidth consumed by applications that belong to the real-time class type in the SD-WAN configuration. The performance of such applications depends on a great extent upon network latency. A delayed packet is worse than a lost packet (for example, VoIP, Skype for Business).
- **Interactive Bandwidth:** Bandwidth consumed by applications that belong to the interactive class type in the SD-WAN configuration. The performance of such applications depends on a great extent upon network latency, and packet loss (for example, XenDesktop, XenApp).

- **Bulk Bandwidth:** Bandwidth consumed by applications that belong to the bulk class type in the SD-WAN configuration. These applications involve little human intervention and are handled by the systems themselves (for example, FTP, backup operations).
- **Expand/Collapse:** You can expand or collapse the data as needed.

Paths

To view the **Paths** statistics, navigate to **Reports > Statistics > Paths** tab.



You can view the following metrics:

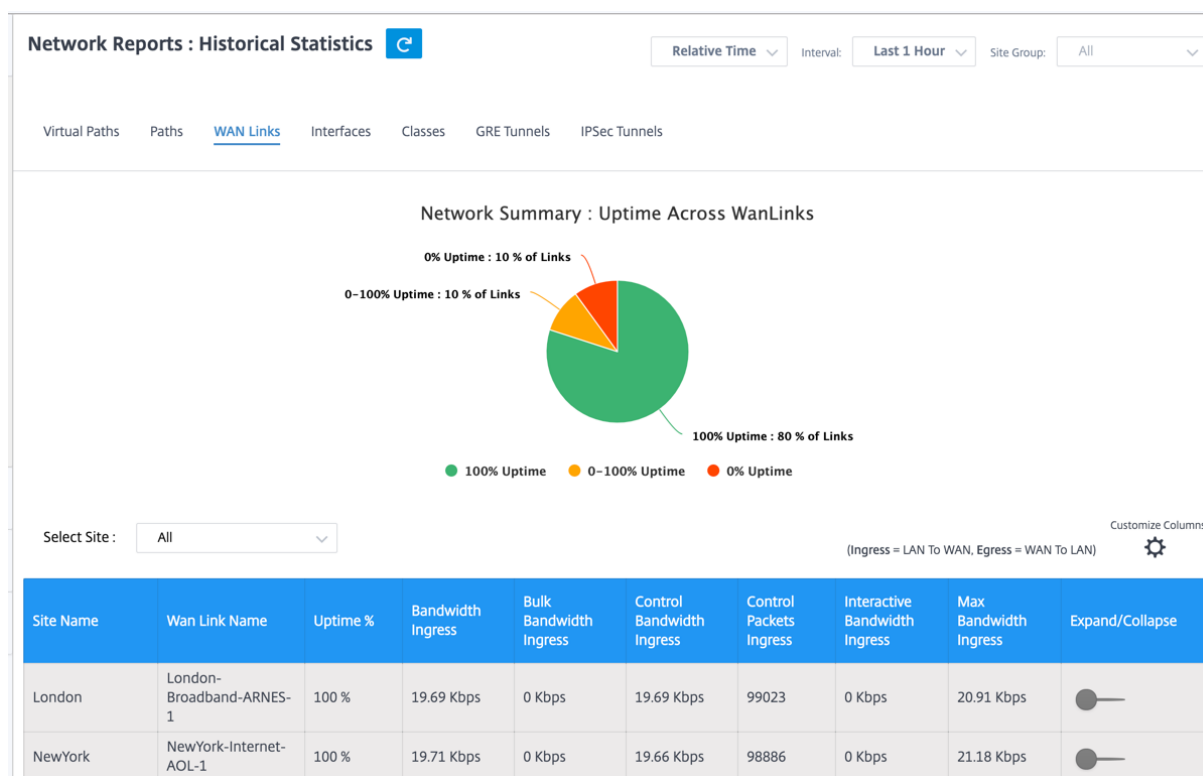
- **From WAN Link:** The source WAN link.
- **To WAN Link:** The destination WAN link.
- **Latency:** The latency in milliseconds for real time traffic.
- **Loss:** Percentage of packets lost.
- **Jitter:** Variation in the delay of received packets, in milliseconds.
- **Bandwidth:** Total bandwidth consumed by all packet types. Bandwidth= Control Bandwidth + Real-time Bandwidth + Interactive Bandwidth + Bulk Bandwidth.
- **Control Bandwidth:** Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.
- **Real-time Bandwidth:** Bandwidth consumed by applications that belong to the real-time class type in the SD-WAN configuration. The performance of such applications depends on a great

extent upon network latency. A delayed packet is worse than a lost packet (for example, VoIP, Skype for Business).

- **Interactive Bandwidth:** Bandwidth consumed by applications that belong to the interactive class type in the SD-WAN configuration. The performance of such applications depends on a great extent upon network latency, and packet loss (for example, XenDesktop, XenApp).
- **Bulk Bandwidth:** Bandwidth consumed by applications that belong to the bulk class type in the SD-WAN configuration. These applications involve little human intervention and are handled by the systems themselves (for example, FTP, backup operations).
- **Expand/Collapse:** You can expand or collapse the data as needed.

WAN links

To view the statistics at **WAN Link** level, navigate to **Reports > Statistics > WAN Links** tab.



You can view the following metrics:

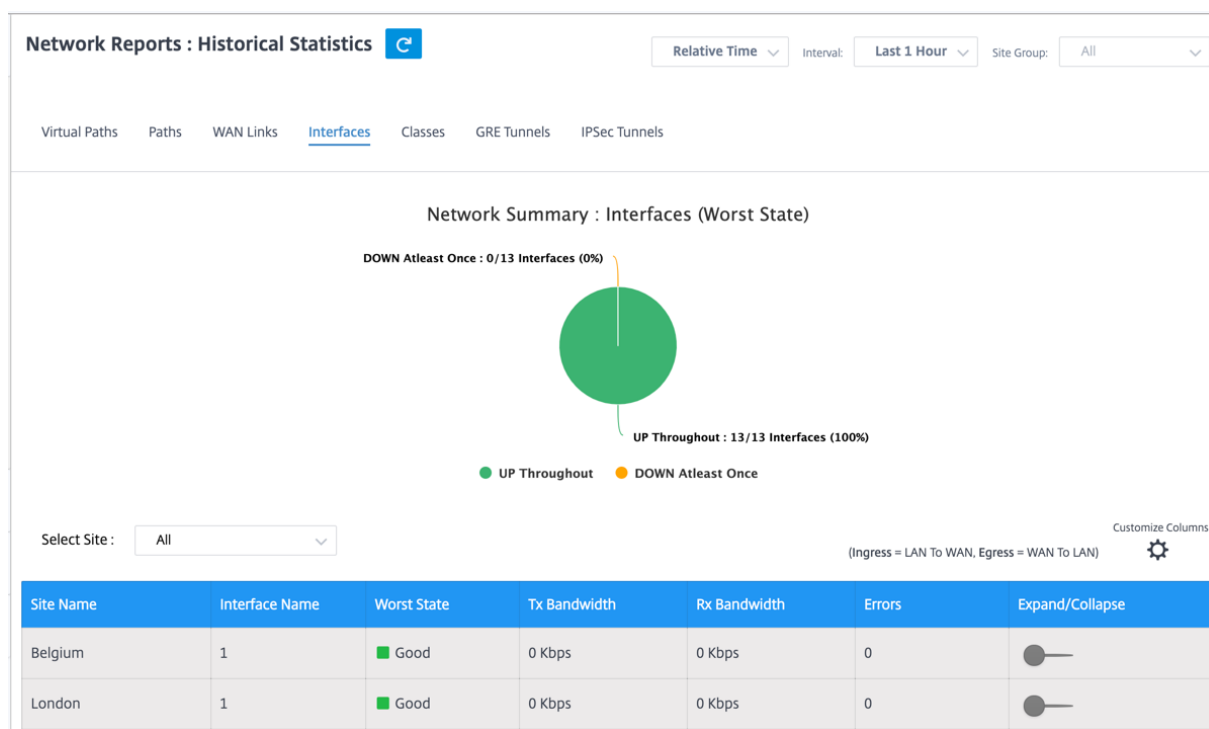
- **WAN Link Name:** The path name.
- **Bandwidth Ingress:** Ingress (LAN to WAN) Bandwidth usage for the selected time period.
- **Bulk Bandwidth Ingress:** Ingress (LAN to WAN) Virtual Path Bandwidth used by Bulk traffic for the selected time period.
- **Control Bandwidth Ingress:** Ingress (LAN to WAN) Virtual Path Bandwidth used by Control traffic for the selected time period.

- **Control Packet Ingress:** Ingress (LAN to WAN) Virtual Path Control packets for the selected time period.
- **Interactive Bandwidth Ingress:** Ingress (LAN to WAN) Virtual Path Bandwidth used by Interactive traffic for the selected time period.
- **Max Bandwidth Ingress:** Max Ingress (LAN to WAN) Bandwidth used in a minute for the selected time period.
- **Min Bandwidth Ingress:** Min Ingress (LAN to WAN) Bandwidth used in a minute for the selected time period.
- **Expand/Collapse:** You can expand or collapse the data as needed.

Interfaces

The Interfaces statistic report 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.

To view **Interface** statistics, navigate to **Reports > Statistics > Interfaces** tab.



You can view the following metrics:

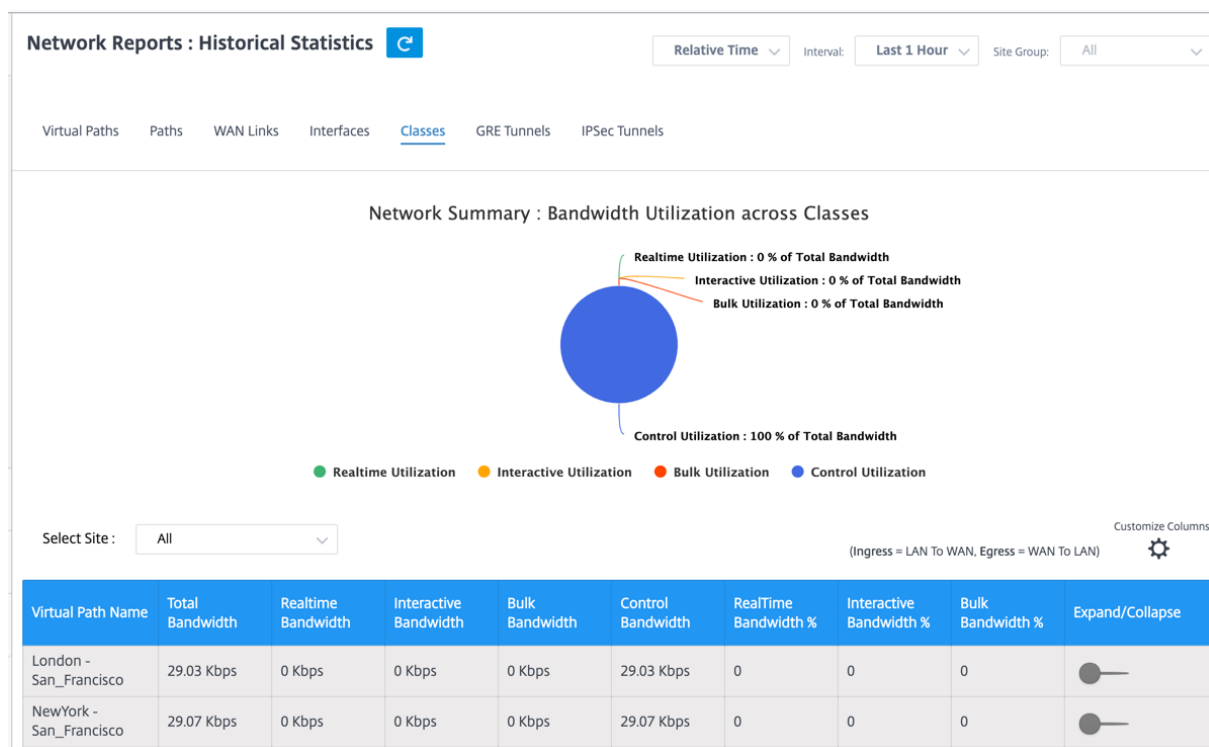
- **Interface Name:** The name of the Ethernet interface.
- **Tx Bandwidth:** Bandwidth transmitted.
- **Rx Bandwidth:** Bandwidth received.
- **Errors:** Number of errors observed during the selected time period.

- **Expand/Collapse:** You can expand or collapse the data as needed.

Classes

The virtual services can be assigned to particular QoS classes, and different bandwidth restraints can be applied to different classes.

To view **Class** statistics, navigate to **Reports > Statistics > Classes** tab.



You can view the following metrics:

- **QoS Class:** The class name.
- **Bandwidth:** Transmitted bandwidth.
- **Data Volume:** Data sent, in Kbps.
- **Drop Volume:** Percentage of data dropped.
- **Drop Percent:** Percentage of data dropped.
- **Expand/Collapse:** You can expand or collapse the data as needed.

GRE tunnels

You can use a tunneling mechanism to transport packets of one protocol within another protocol. The protocol that carries the other protocol is called the transport protocol, and the carried protocol is called the passenger protocol. Generic Routing Encapsulation (GRE) is a tunneling mechanism that uses IP as the transport protocol and can carry many different passenger protocols.

The tunnel source address and destination address are used to identify the two endpoints of the virtual point-to-point links in the tunnel. For more information about configuring GRE tunnels on Citrix SD-WAN appliances, see [GRE Tunnel](#).

To view **GRE Tunnel** statistics, navigate to **Reports > Statistics > GRE Tunnels** tab.

You can view the following metrics:

- **Site Name:** The site name.
- **Tx Bandwidth:** Bandwidth transmitted.
- **Rx Bandwidth:** Bandwidth received.
- **Packet 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.
- **Expand/Collapse:** You can expand or collapse the data as needed.

IPsec tunnels

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 Citrix SD-WAN appliances, see [IPsec Tunnel Termination](#).

To view **IPsec Tunnel** statistics, navigate to **Reporting > statistics > IPsec Tunnels** tab.


You can view the following metrics:


- **Tunnel Name:** The tunnel name.
- **Tunnel State:** IPsec tunnel state.
- **MTU:** Maximum transmission unit—size of the largest IP datagram that can be transferred through a specific link.
- **Packet Received:** Number of packets received.
- **Packets Sent:** Number of packets Sent.
- **Packet Dropped:** Number of packets dropped, because of network congestion.
- **Bytes Dropped:** Number of bytes dropped.
- **Expand/Collapse:** You can expand or collapse the data as needed.


Real time statistics



You can also get the following real time statistics information under **Troubleshooting > Statistics**:

- ARP
- Routes
- Ethernet
- Observed Protocols
- Application
- Rules

Network Reports : Real Time Statistics 

Site Group: All 

[ARP](#) [Routes](#) [Virtual Path Services](#) [Classes](#) [Ethernet](#) [Observed Protocols](#) [Wan Path](#) [Application QOS](#) [Other Stats](#) 


Belgium  Retrieve latest data Search 


Gateway ARP Timer: 1000
End User ARP Timer: 1000



Num	Interface	Routing Domain	VLAN	IP Address	MAC Address	State	Type
1	2		0	172.10.30.1	26:63:82:97:57:37	READY_ACTIVE	PERSISTENT
0	3		0	172.10.40.1	06:12:90:dd:91:5f	READY_ACTIVE	PERSISTENT


Flows

At the network level, select the site from the drop-down list before you can fetch the statistics. The **Flows** feature provides unidirectional flow information related to a particular session going through the appliance. This provides information on the destination service type the flow is falling into and also the information related to the rule and class type and also the transmission mode.

Network Reports : Real Time Flows 

Site Group: All 

San Francisco  Retrieve latest data Search 

☒ Upload ☒ Download  Customize Columns

Info	No	Application	Source IP Addr	Dest IP Addr	Source Port	Dest Port	Proto IP	Packets	PPS	Class	Service Name	Age (ms)	Bytes
①	1	N/A	172.10.10.6	192.229.232.240	49976	80	TCP (6)	3	0.004	N/A	-	792120	156
①	2	N/A	172.10.10.6	192.229.232.240	49837	80	TCP (6)	3	0.001	N/A	-	4114023	156
①	3	N/A	172.10.10.6	192.229.232.240	49835	80	TCP (6)	3	0.001	N/A	-	4140148	156
①	4	N/A	172.10.10.6	192.229.232.240	49833	80	TCP (6)	3	0.001	N/A	-	4179835	156
①	5	N/A	172.10.10.6	192.229.232.240	49970	80	TCP (6)	3	0.002	N/A	-	1745589	156
①	6	N/A	172.10.10.6	192.229.232.240	49831	80	TCP (6)	3	0.001	N/A	-	4220070	156
①	7	N/A	172.10.10.6	192.229.232.240	49825	80	TCP (6)	3	0.001	N/A	-	4258507	156
①	8	Google Talk (incl. Hangouts and Allo and Duo)(gtalk)	172.10.10.6	74.125.130.188	49743	443	TCP (6)	134	0.025	N/A	-	1609	6436

Firewall connections

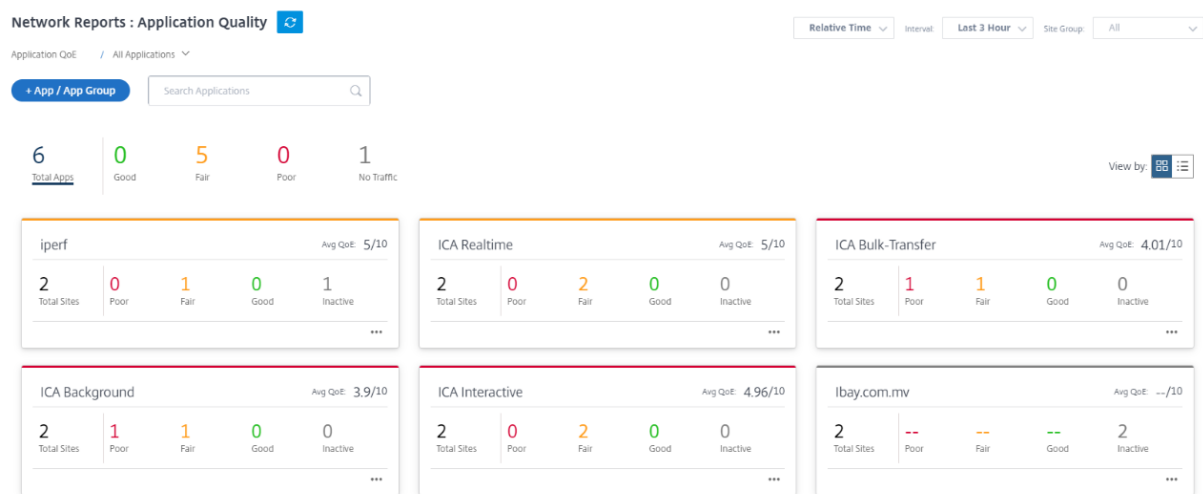
At the network level, select the site from the drop-down list before you can fetch the statistics. The **Firewall connections** provide the state of the connection related to a particular session based on the firewall action configured. Firewall connections also provide complete details about the source and destination of the connection.

Application	Family	Routing Domain	IP Protocol	IP Addr	Port	Service Type	Service Name	Zone	IP #
Domain Name Se...	Network Service	Default_Routing...	UDP	172.10.10.6	49794	Local	VIF-Bridge-1-VL...	Default_LAN_Zone	10.1
Domain Name Se...	Network Service	Default_Routing...	UDP	172.10.10.6	56626	Local	VIF-Bridge-1-VL...	Default_LAN_Zone	10.1
Microsoft(micros...	Web	Default_Routing...	TCP	172.10.10.6	49775	Local	VIF-Bridge-1-VL...	Default_LAN_Zone	52.1
Domain Name Se...	Network Service	Default_Routing...	UDP	172.10.10.6	61426	Local	VIF-Bridge-1-VL...	Default_LAN_Zone	10.1
Google Talk (incl...	Instant Messaging	Default_Routing...	TCP	172.10.10.6	49743	Local	VIF-Bridge-1-VL...	Default_LAN_Zone	74.1

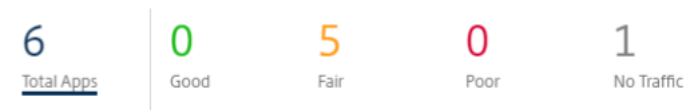
Application Quality

Application QoE is a measure of Quality of Experience of applications in the SD-WAN network. It measures the quality of applications that flow through the virtual paths between two SD-WAN appliances. The Application QoE score is a value between 0 and 10. The score range that it falls in determines the quality of an application. Application QoE enables network administrators to review the quality of experience of applications and take proactive measures when the quality goes below the acceptable threshold.

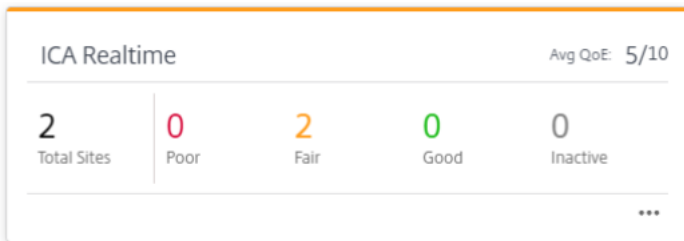
Quality	Range	Color Coding
Good	8–10	Green
Fair	4–8	Orange
Poor	0–4	Red



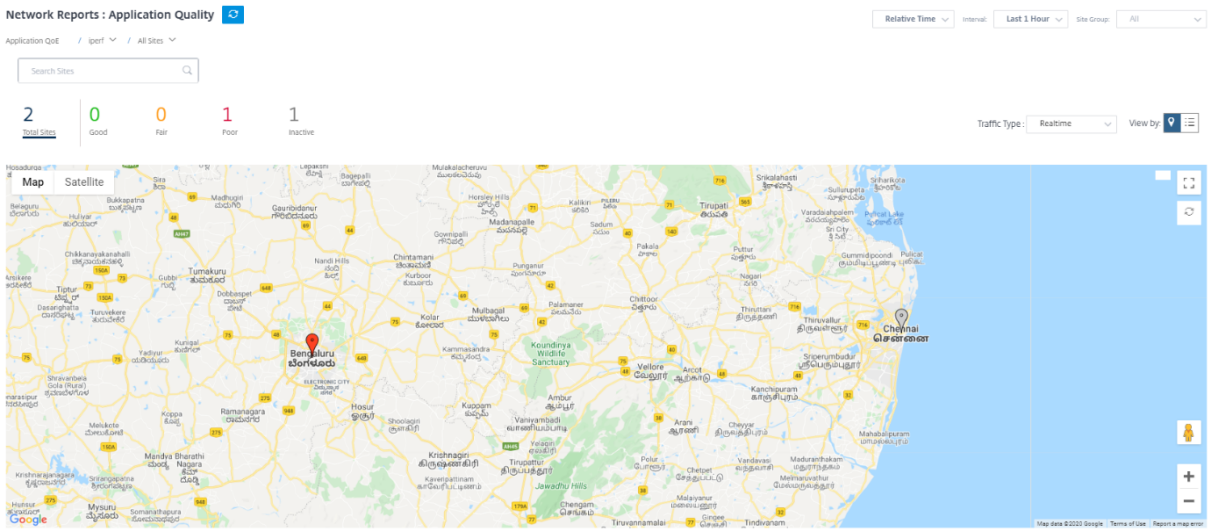
The top of the dashboard displays the overall number of applications and the number of applications that have good, fair, or poor Application QoE in the network. It also displays the number of applications that do not have any traffic.



The individual application card displays the number of sites that have poor, fair, or good Application QoE for the specific application. It also displays the number of sites that are not actively using the application. The Avg QoE is the average QoE score of the application across all the sites in the network.

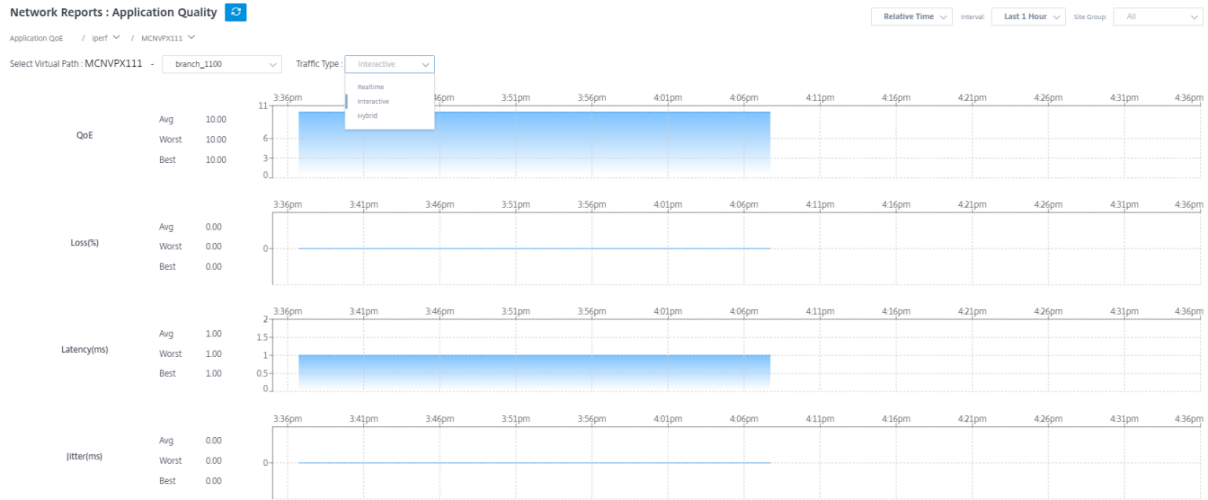


Click an individual application card to view the details on the number of sites that have good, fair, or poor application QoE for the selected application. A map view of all the sites that is running the selected application is displayed. Click a site in the map to further drill down and view the Application QoE statistics of the various virtual paths at the site.



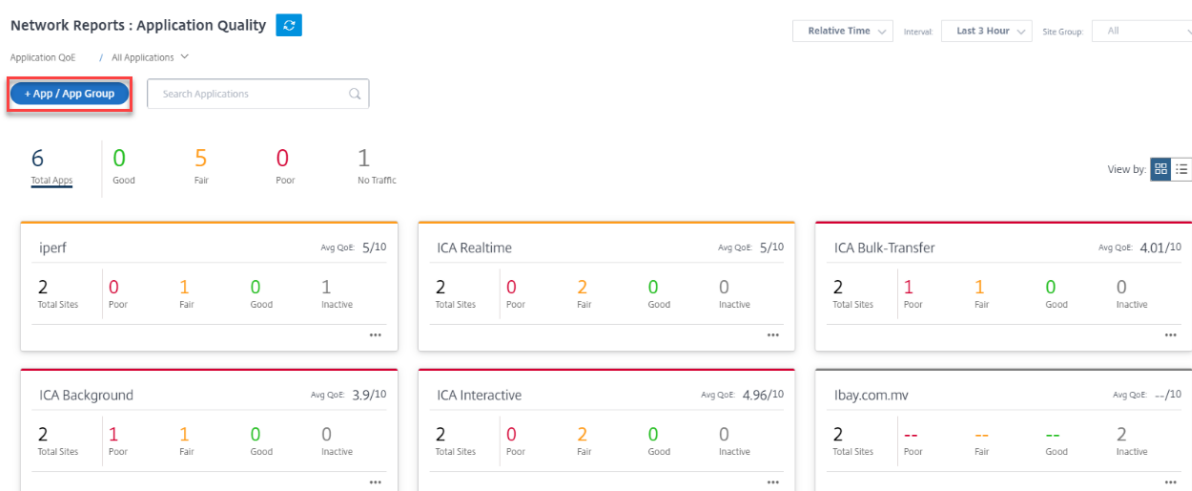
You can view the following metrics for Real-time, Interactive, and Hybrid traffic for the selected time-frame:

- **QoE:** The QoE score for the traffic.
- **Loss:** The loss percentage for the traffic.
- **Latency:** The latency in milliseconds for the traffic.
- **Jitter:** The jitter observed in milliseconds for the traffic.



Application QoE profiles

Click **+ App / App Group** to map applications, custom applications, or application groups to the default or custom QoE profiles.



The QoE profiles define the threshold for real-time, interactive, and hybrid traffic. The QoE thresholds as per the QoE profiles are applied to the selected application or application group.

Add App/App Group

Type * Application Application * Ibay.com.mv(ibay) QoE Profile * new_qoe_profile + New QoE Profile

Cancel Ok

Click **+ New QoE Profile** to create a new application QoE profile and enter the value for the following parameters:

- **Profile Name:** A name to identify the profile that sets thresholds for real-time and interactive traffic.
- **Traffic Type:** Choose the type of traffic – Real-time, Interactive, or Hybrid. If the traffic type is Hybrid, you can configure both Real-time and Interactive QoE profile thresholds.
- **Realtime Configuration:** Configure thresholds for traffic flows that select the real-time QoS policy. A flow of a real-time application that meets the following thresholds for latency, loss, and jitter is considered to be of good quality.
 - **One Way latency:** The latency threshold in milliseconds. The default QoE profile value is 160 ms.
 - **Jitter:** The jitter threshold in milliseconds. The default QoE profile value is 30 ms.
 - **Packet Loss:** The percentage of packet loss. The default QoE profile value is 2%.
- **Interactive Configuration:** Configure thresholds for traffic flows that select the interactive QoS policy. A flow of an interactive application that meets the following threshold for burst ratio and

packet loss is considered to be of good quality.

- **Expected Burst Rate:** The percentage of expected burst rate. The egress burst rate must be at least the configured percentage of ingress burst rate. The default QoE profile value is 60%.
- **Packet loss per flow:** The percentage of packet loss. The default QoE profile value is 1%.

The newly added application is displayed in the Application Quality dashboard.

You can also define and configure application QoE from App & DNS Settings for more information see, [Application quality profiles](#) and [Application quality configuration](#).

March 8, 2021

Site reports

The **Site Reports** provide visibility into site-level alerts, usage trends, quality, device information, and firewall statistics.

Alerts

The site administrator can review a detailed report of all the events and alerts generated at a site. It includes the severity, site at which the alert originated, alert message, time, and other details.

Site Report : Alerts				
Delete Alerts		Search <input type="text"/>		<div>216 TOTAL</div> <div>10 HIGH</div> <div>17 MEDIUM</div> <div>189 LOW</div>
<input type="checkbox"/>	Severity	Source	Message	Time
<input type="checkbox"/>	Low	APPLIANCE	The state of Virtual Path San_Francisco-Madrid has changed from BAD to GOOD	Jan 30th 2020, 12:35 am
<input type="checkbox"/>	Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang...	Jan 30th 2020, 12:35 am
<input type="checkbox"/>	Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang...	Jan 30th 2020, 12:35 am
<input type="checkbox"/>	Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang...	Jan 30th 2020, 12:35 am
<input type="checkbox"/>	Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang...	Jan 30th 2020, 12:35 am
<input type="checkbox"/>	High	APPLIANCE	The Virtual Path San_Francisco-Madrid is no longer DEAD	Jan 30th 2020, 12:35 am
<input type="checkbox"/>	Low	APPLIANCE	Ethernet link on device 4 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
<input type="checkbox"/>	Low	APPLIANCE	Ethernet link on device 3 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
<input type="checkbox"/>	Low	APPLIANCE	Ethernet link on device 2 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
<input type="checkbox"/>	Low	APPLIANCE	Ethernet link on device 1 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
<input type="checkbox"/>	Low	APPLIANCE	The state of Virtual Path San_Francisco-Madrid has changed from BAD to GOOD	Jan 24th 2020, 12:05 pm
<input type="checkbox"/>	Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang...	Jan 24th 2020, 12:05 pm
<input type="checkbox"/>	Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang...	Jan 24th 2020, 12:05 pm
<input type="checkbox"/>	Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path San_Francisco-Broadband-AMIS-2->Madrid-DSL-ono-1 state has chang...	Jan 24th 2020, 12:05 pm
<input type="checkbox"/>	Low	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang...	Jan 24th 2020, 12:05 pm
<input type="checkbox"/>	High	APPLIANCE	The Virtual Path San_Francisco-Madrid is no longer DEAD	Jan 24th 2020, 12:05 pm
<input type="checkbox"/>	Medium	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1->San_Francisco-Broadband-AMIS-2 state has chang...	Jan 24th 2020, 12:05 pm

Suitable filtering options can be used as needed for example: Look for all the high severity alerts at the site or the alerts that occurred during a particular period.

You can also select and clear alerts.

Usage

Site administrators can review usage trends such as **Top Applications**, **Top Application Categories**, and **App Bandwidth** in a particular site.

Top applications and application categories

The **Top Applications** and **Top Application Categories** chart shows the top applications and top application families that are widely used in the site. This allows you to analyze the data consumption pattern and reassign the bandwidth limit for each class of data within the site.

You can also view the bandwidth usage statistics. The bandwidth statistics are collected for the selected time interval. You can filter the statistics report based on the **Report Type**, **Apps or Apps Categories**, and **Metrics**.

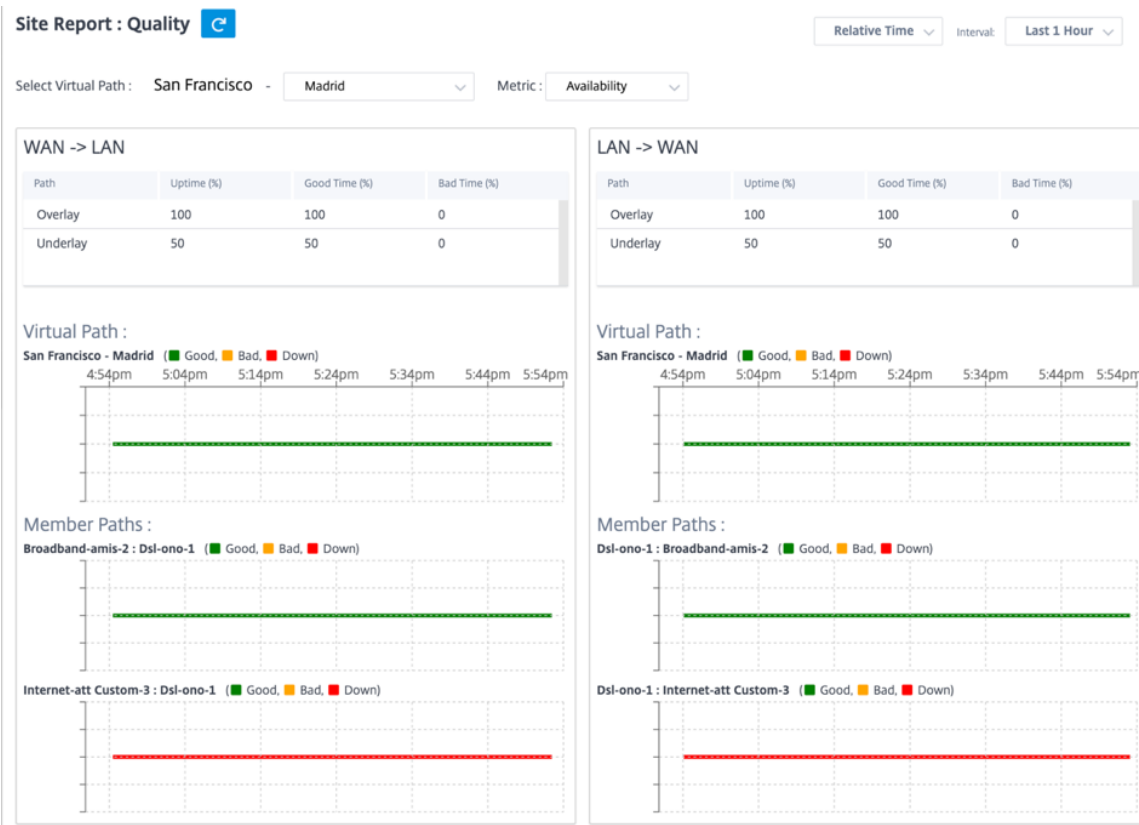


- **Report Type:** Select **Top App or App Categories** from the list.
- **Apps/App Categories:** Select top application or categories (such as network service) from the list.
- **Metric:** Select the bandwidth metric (such as Total Data, Incoming Data, Total Bandwidth) from the list.

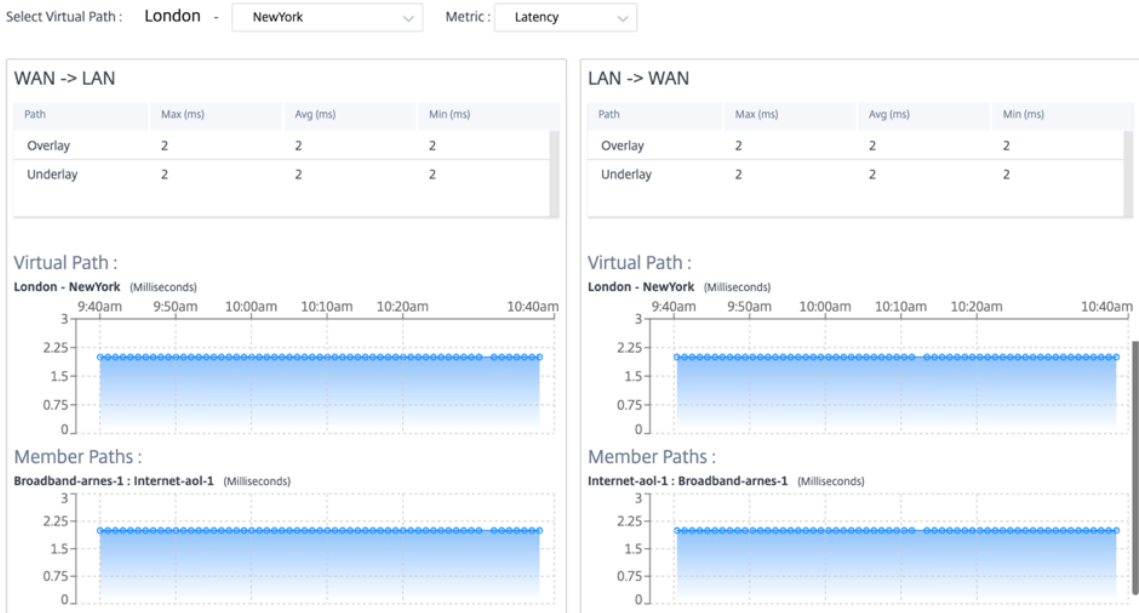
Quality

Site administrators can use the Quality reports to analyze the Quality of Experience (QoE) at the site for each QoS metric such as availability, loss, latency, and jitter. The quality metric is displayed for both the overlay virtual paths and its underlying member paths.

- **Availability**

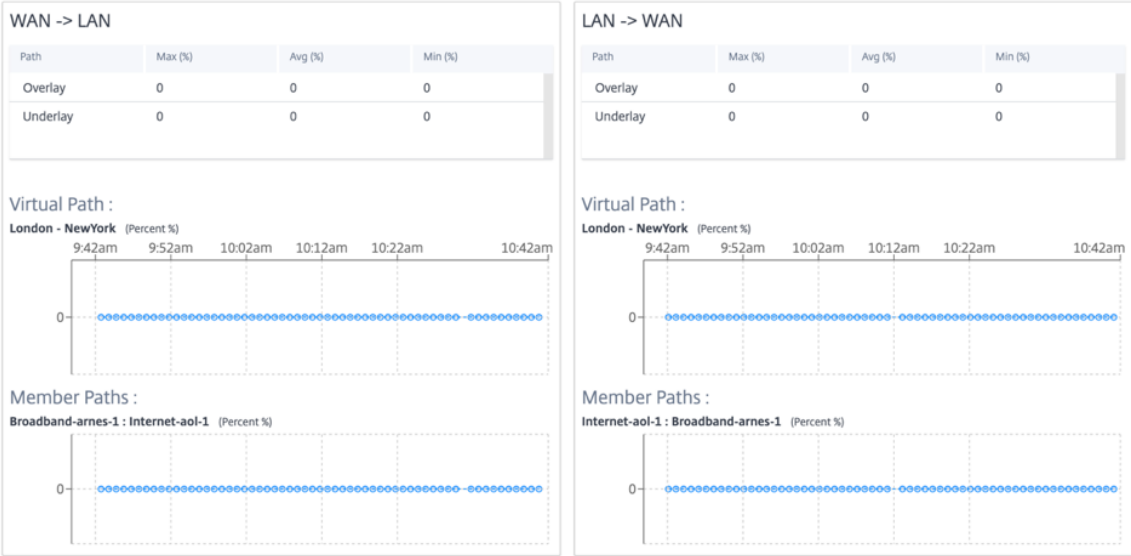


• Latency



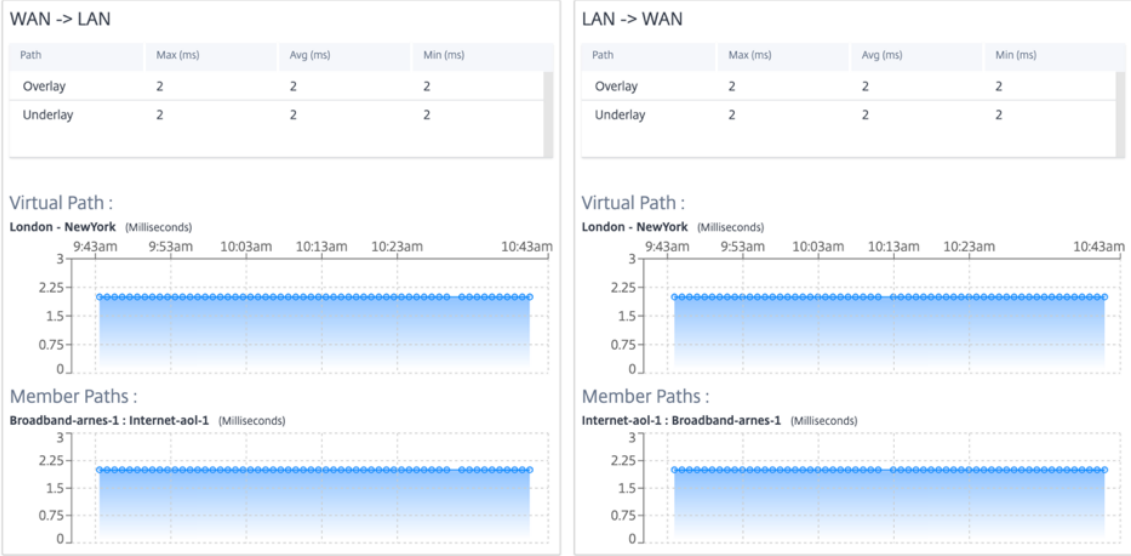
• Loss

Select Virtual Path : London - NewYork Metric : Loss

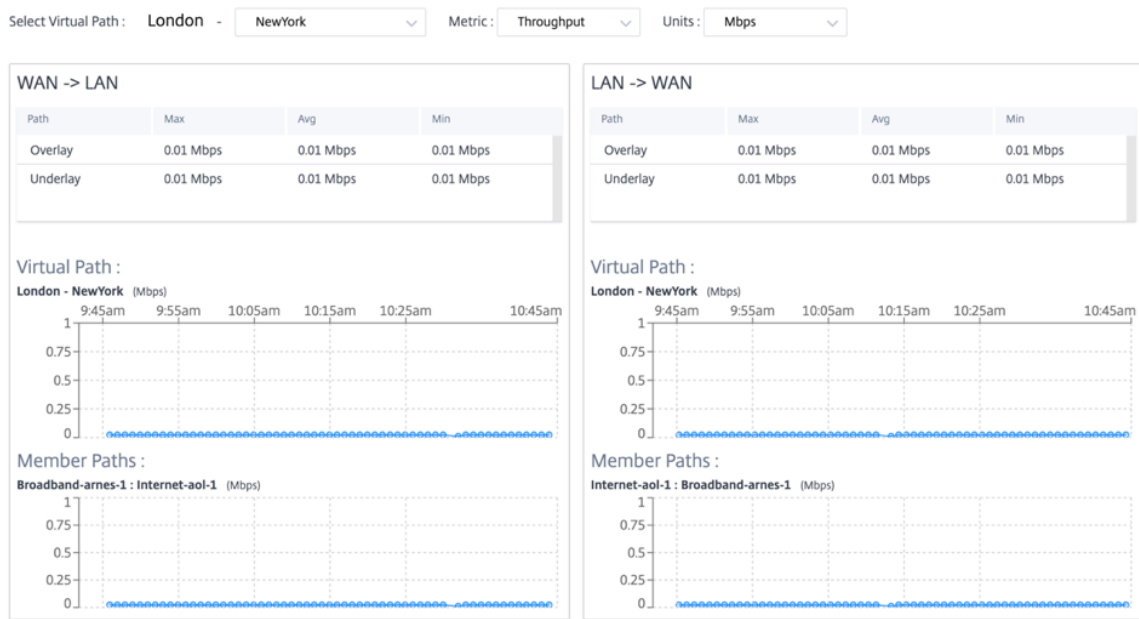


• Jitter

Select Virtual Path : London - NewYork Metric : Jitter



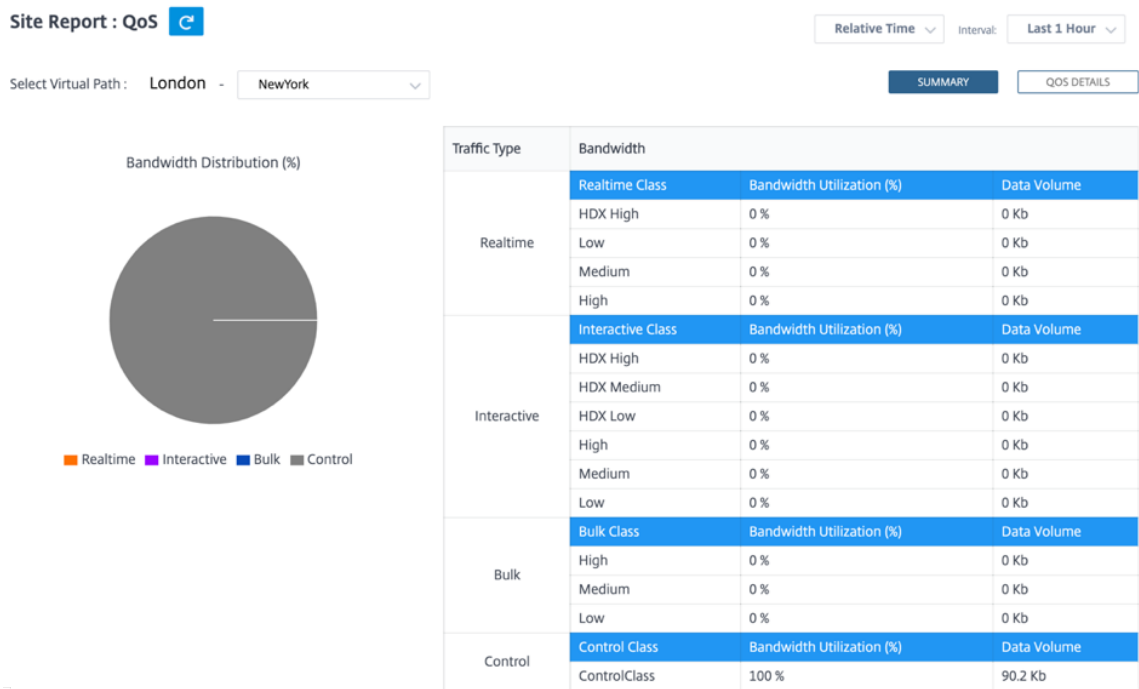
• Throughput



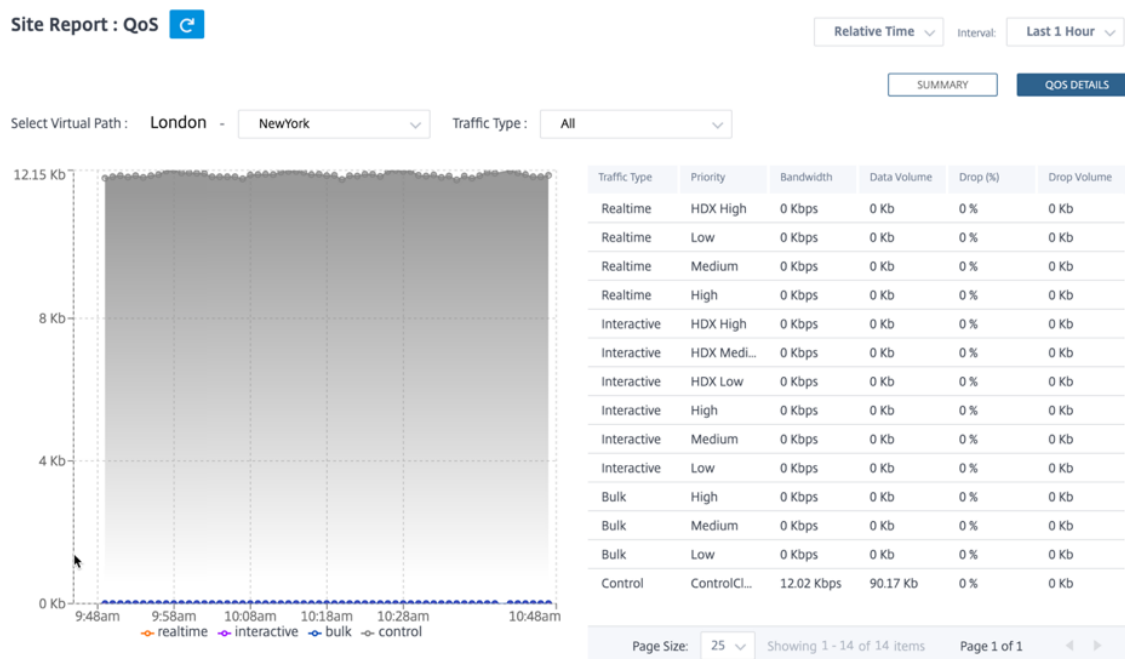
Quality of Service

Quality of Service (QoS) manages data traffic to reduce packet loss, latency, and jitter on the network. For more information, see [Quality of Service](#). The following are two ways to view the Quality-of-Service (QoS) report:

- **Summary View:** Summary view provides an overview of bandwidth consumption across all types of traffic - real-time, interactive, bulk, and control across the network and per site.



- **Real-time:** Used for low latency, low bandwidth, time-sensitive traffic. Real-time applications are time sensitive but don't really need high bandwidth (for example voice over IP). Real-time applications are sensitive to latency and jitter, but can tolerate some loss.
- **Interactive:** Used for interactive traffic with low to medium latency requirements and low to medium bandwidth requirements. Interactive applications involve human input in the form of mouse clicks or cursor moves. The interaction is typically between a client and a server. The communication might not need high bandwidth but is sensitive to loss and latency. However, server to client does need high bandwidth to transfer graphical information, which might not be sensitive to loss.
- **Bulk:** Used for high bandwidth traffic that can tolerate high latency. Applications that handle file transfer and need high bandwidth are categorized as bulk class. These applications involve little human interference and are mostly handled by the systems themselves.
- **Control:** Used to transfer control packets that contain routing, scheduling, and link statistics information.
- **Detailed View:** The detailed view captures trends around bandwidth consumption, traffic volume, packets dropped and so on For each QoS class associated with an overlay virtual path. You can view QoS statistics based on the virtual path between two sites.



Historical statistics

For each site, you can view the statistics as graphs for the following network parameters:

- Virtual Paths

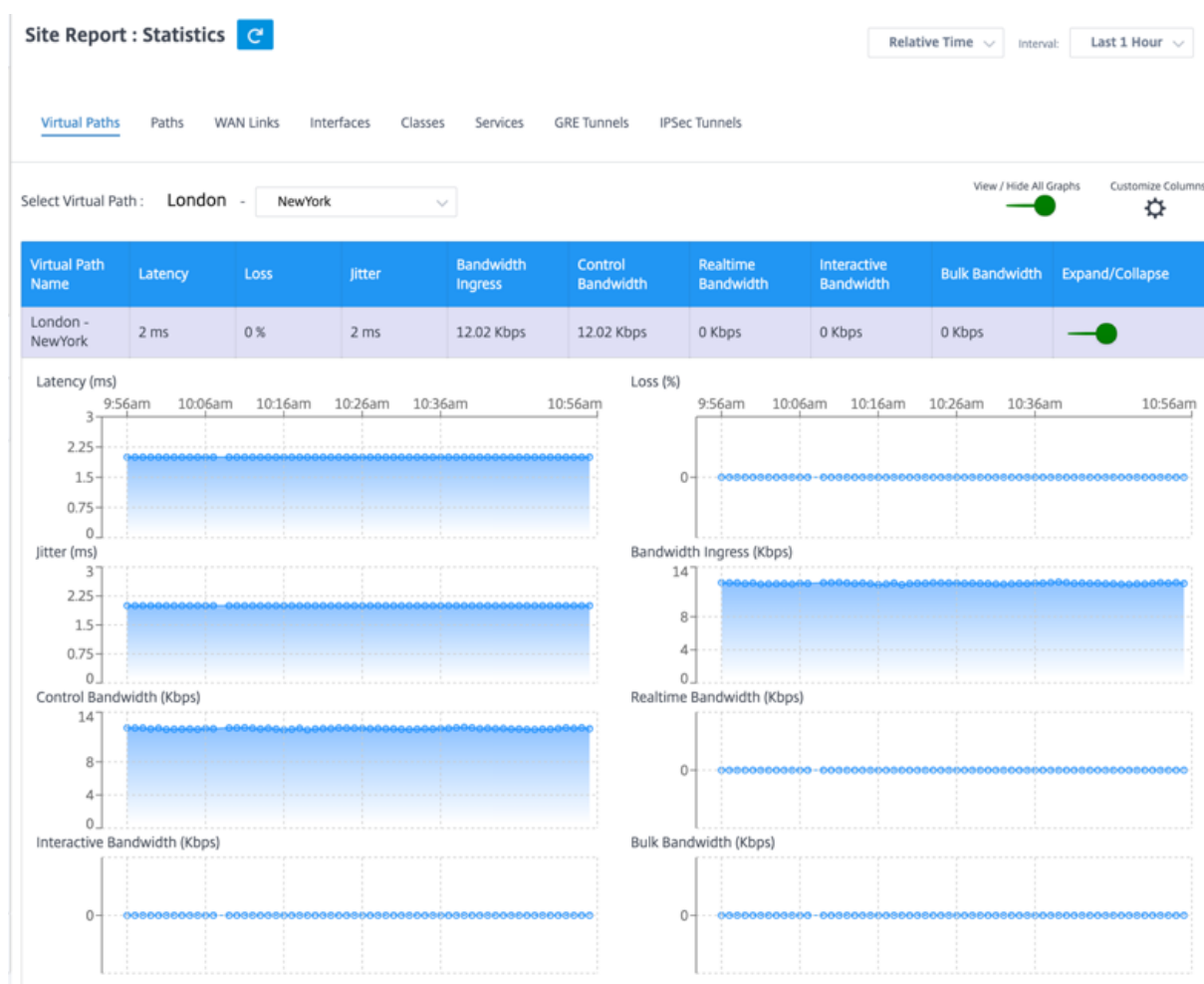
- Paths
- WAN Links
- Interfaces
- Classes
- Services
- GRE Tunnels
- IPsec Tunnels

The statistics are collected 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.

You can view or hide the graphs and customize the columns as needed.

Virtual paths

To view the **Virtual Paths** statistics, navigate to **Reports > Statistics > Virtual Paths** tab.



You can view the following metrics:

- **Virtual Path Name:** The virtual path name.
- **Latency:** The latency in milliseconds for real time traffic.
- **Loss:** Percentage of packets lost.
- **Jitter:** Variation in the delay of received packets, in milliseconds.
- **Bandwidth Ingress: Ingress (LAN > WAN) Bandwidth** usage for the selected time period.
- **Control Bandwidth:** Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.
- **Real-time Bandwidth:** Bandwidth consumed by applications that belong to the real-time class type in the SD-WAN configuration. The performance of such applications depends on a great extent upon network latency. A delayed packet is worse than a lost packet (for example, VoIP, Skype for Business).
- **Interactive Bandwidth:** Bandwidth consumed by applications that belong to the interactive class type in the SD-WAN configuration. The performance of such applications depends on a great extent upon network latency, and packet loss (for example, XenDesktop, XenApp).
- **Bulk Bandwidth:** Bandwidth consumed by applications that belong to the bulk class type in the SD-WAN configuration. These applications involve little human intervention and are mostly handled by the systems themselves (for example, FTP, backup operations).
- **Expand/Collapse:** You can expand or collapse the data as needed.

Paths

To view the **Paths** statistics, navigate to **Reports > Statistics > Paths** tab.

Site Report : Statistics

Relative Time

Interval:

Last 1 Hour

Virtual Paths

Paths

WAN Links

Interfaces

Classes

Services

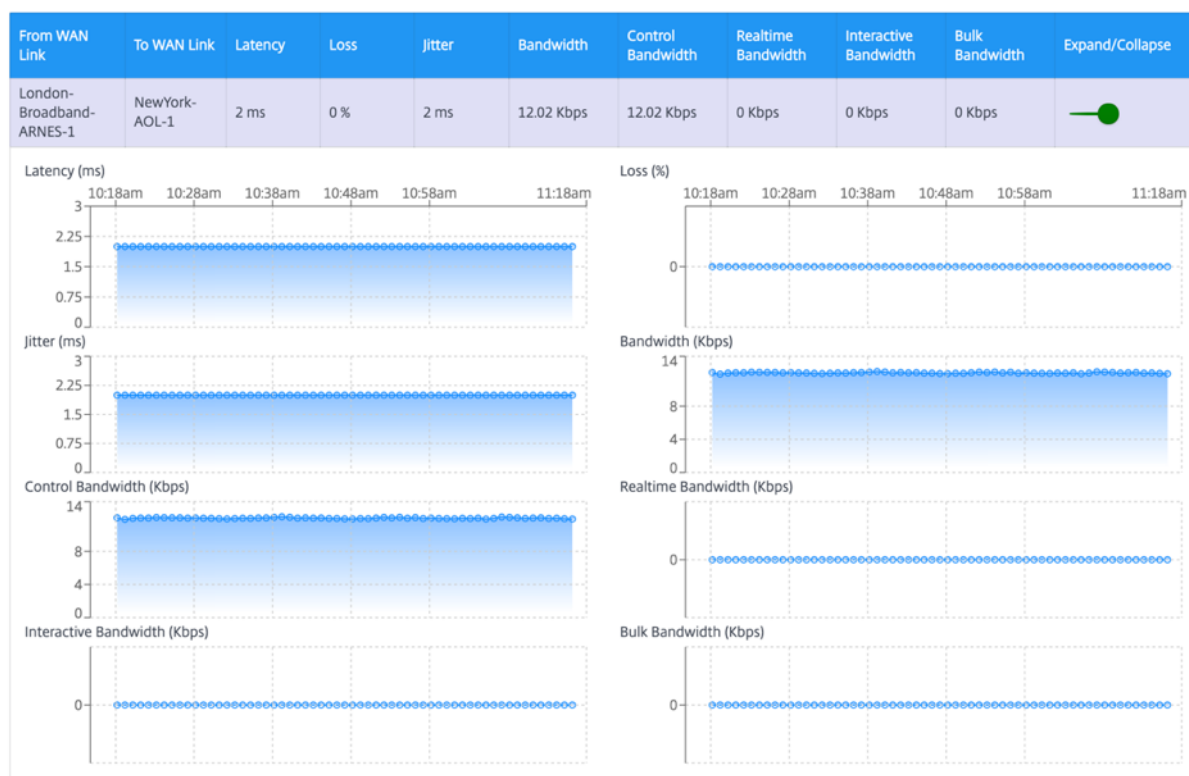
GRE Tunnels

IPSec Tunnels

Select Virtual Path : London - NewYork

View / Hide All Graphs

Customize Columns



You can view the following metrics:

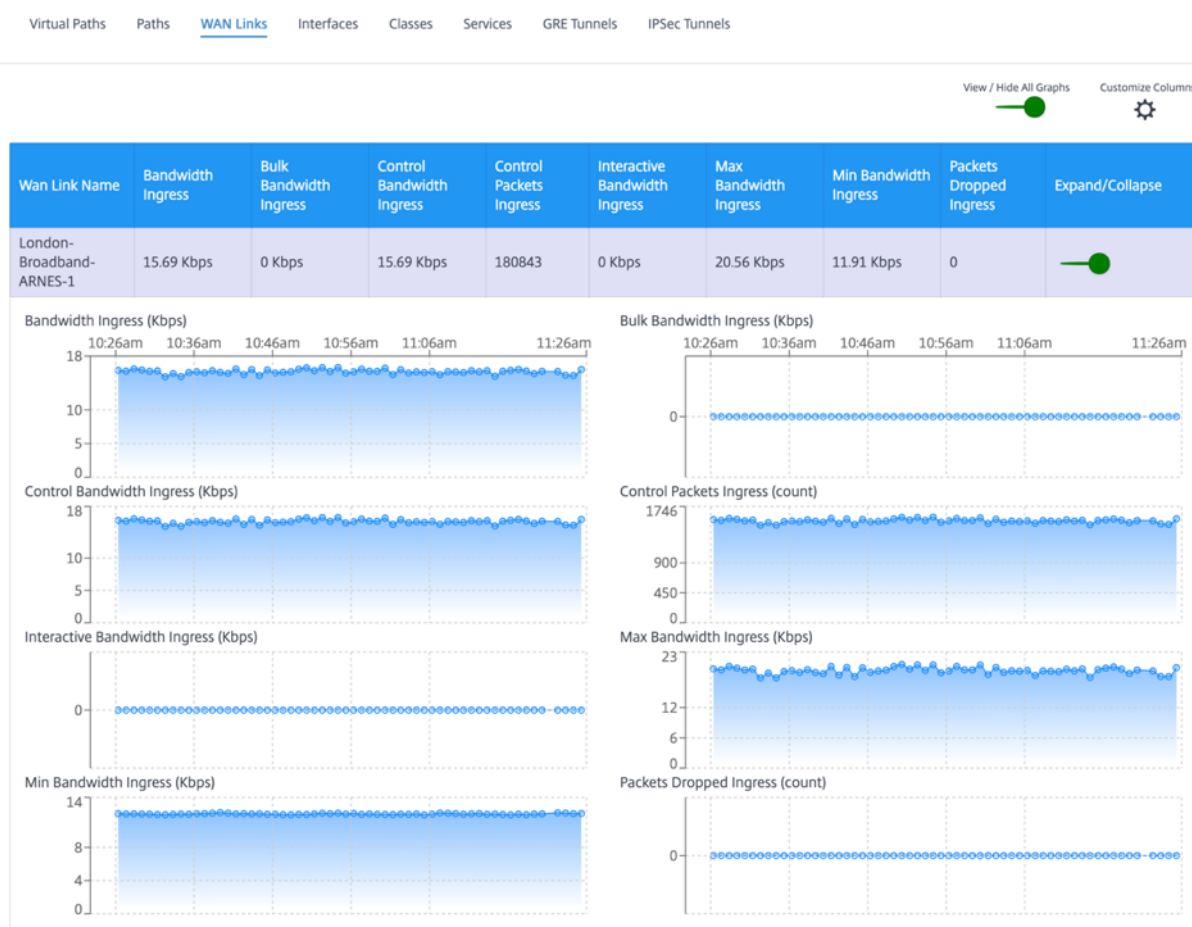
- **From WAN Link:** The source WAN link.
- **To WAN Link:** The destination WAN link.
- **Latency:** The latency in milliseconds for real time traffic.
- **Loss:** Percentage of packets lost.
- **Jitter:** Variation in the delay of received packets, in milliseconds.
- **Bandwidth:** Total bandwidth consumed by all packet types. Bandwidth= Control Bandwidth + Real-time Bandwidth + Interactive Bandwidth + Bulk Bandwidth.
- **Control Bandwidth:** Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.
- **Real-time Bandwidth:** Bandwidth consumed by applications that belong to the real-time class type in the SD-WAN configuration. The performance of such applications depends on a great extent upon network latency. A delayed packet is worse than a lost packet (for example, VoIP, Skype for Business).
- **Interactive Bandwidth:** Bandwidth consumed by applications that belong to the interactive

class type in the SD-WAN configuration. The performance of such applications depends on a great extent upon network latency, and packet loss (for example, XenDesktop, XenApp).

- **Bulk Bandwidth:** Bandwidth consumed by applications that belong to the bulk class type in the SD-WAN configuration. These applications involve little human intervention and are mostly handled by the systems themselves (for example, FTP, backup operations).
- **Expand/Collapse:** You can expand or collapse the data as needed.

WAN links

To view the statistics at **WAN Link** level, navigate to **Reports > Statistics > WAN Links** tab.



You can view the following metrics:

- **WAN Link Name:** The path name.
- **Bandwidth Ingress: Ingress (LAN > WAN) Bandwidth** usage for the selected time period.
- **Bulk Bandwidth Ingress: Ingress (LAN > WAN) virtual path bandwidth** used by Bulk traffic for the selected time period.
- **Control Bandwidth Ingress: Ingress (LAN > WAN) virtual path bandwidth** used by Control traffic for the selected time period.

- **Control Packet Ingress: Ingress (LAN > WAN) Virtual Path Control packets** for the selected time period.
- **Interactive Bandwidth Ingress: Ingress (LAN > WAN) virtual path bandwidth** used by Interactive traffic for the selected time period.
- **Max Bandwidth Ingress: Maximum ingress (LAN > WAN) bandwidth** used in a minute for the selected time period.
- **Min Bandwidth Ingress: Minimum ingress (LAN > WAN) bandwidth** used in a minute for the selected time period.
- **Expand/Collapse:** You can expand or collapse the data as needed.

Interfaces

The Interfaces statistic report 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.

To view **Interface** statistics, navigate to **Reports > Statistics > Interfaces** tab.

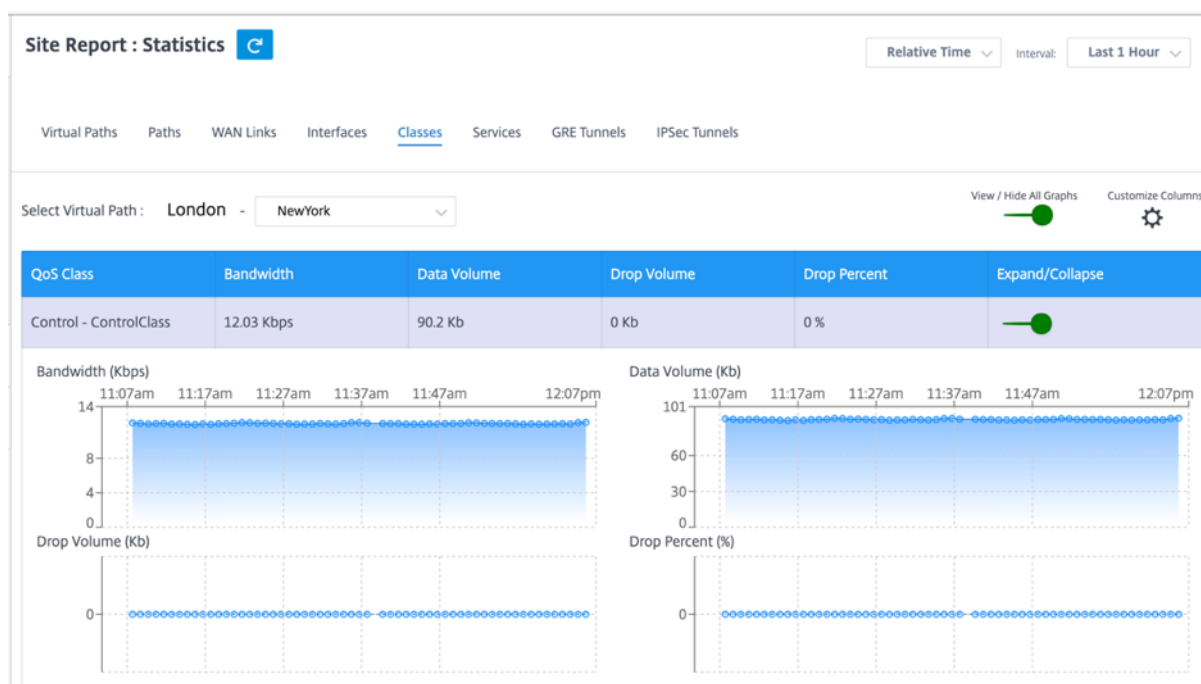
You can view the following metrics:

- **Interface Name:** The name of the Ethernet interface.
- **Tx Bandwidth:** Bandwidth transmitted.
- **Rx Bandwidth:** Bandwidth received.
- **Errors:** Number of errors observed during the selected time period.
- **Expand/Collapse:** You can expand or collapse the data as needed.

Classes

The virtual services can be assigned to particular QoS classes, and different bandwidth restraints can be applied to different classes.

To view **Class** statistics, navigate to **Reports > Statistics > Classes** tab.



You can view the following metrics:

- **QoS Class:** The class name.
- **Bandwidth:** Transmitted bandwidth.
- **Data Volume:** Data sent, in Kbps.
- **Drop Volume:** Percentage of data dropped.
- **Drop Percent:** Percentage of data dropped.
- **Expand/Collapse:** You can expand or collapse the data as needed.

Services

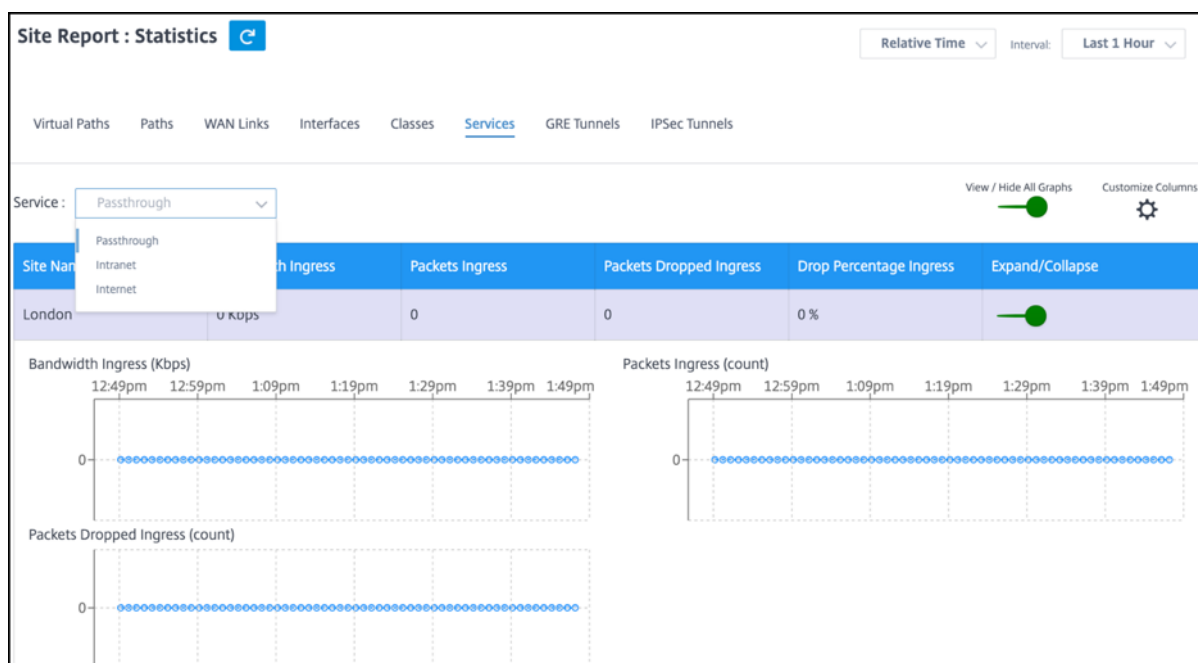
To view the **Services** statistics, navigate to **Reports > Statistics > Services** tab.

Select the service type from the list. The options are as follows:

- **Passthrough** – This service manages traffic that is to be passed through the Virtual WAN. Traffic directed to the Passthrough Service includes broadcasts, ARPs, and other non-IPv4 traffic, and traffic on the Virtual WAN Appliance local subnet, configured subnets, or Rules applied by the Network Administrator. This traffic is not delayed, shaped, or changed by the SD-WAN. Therefore, you must ensure that Passthrough traffic does not consume substantial resources on the WAN links that the SD-WAN Appliance is configured to use for other services.
- **Intranet** – This service manages Enterprise Intranet traffic that has not been defined for transmission across a Virtual Path. As with Internet traffic, it remains unencapsulated, and the SD-WAN manages bandwidth by rate-limiting this traffic relative to other service types during times of congestion. Under certain conditions, and if configured for Intranet Fallback on the Virtual

Path, traffic that ordinarily travels with a Virtual Path can instead be treated as Intranet traffic, to maintain network reliability.

- **Internet** – This service manages traffic between an Enterprise site and sites on the public Internet. Traffic of this type is not encapsulated. During times of congestion, the SD-WAN actively manages bandwidth by rate-limiting Internet traffic relative to the Virtual Path, and Intranet traffic according to the SD-WAN configuration established by the Administrator.



You can view the following metrics:

- **Site Name:** The site name.
- **Bandwidth Ingress: Ingress (LAN > WAN) Bandwidth** usage for the selected time period.
- **Packet Ingress: (LAN > WAN) Packets** sent for the selected time interval.
- **Expand/Collapse:** You can expand or collapse the data as needed.

GRE tunnels

You can use a tunneling mechanism to transport packets of one protocol within another protocol. The protocol that carries the other protocol is called the transport protocol, and the carried protocol is called the passenger protocol. Generic Routing Encapsulation (GRE) is a tunneling mechanism that uses IP as the transport protocol and can carry many different passenger protocols.

The tunnel source address and destination address are used to identify the two endpoints of the virtual point-to-point links in the tunnel. For more information about configuring GRE tunnels on Citrix SD-WAN appliances, see [GRE Tunnel](#).

To view **GRE Tunnel** statistics, navigate to **Reports > Statistics > GRE Tunnels** tab.

You can view the following metrics:

- **Site Name:** The site name.
- **Tx Bandwidth:** Bandwidth transmitted.
- **Rx Bandwidth:** Bandwidth received.
- **Packet 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.
- **Expand/Collapse:** You can expand or collapse the data as needed.

IPsec tunnels

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 Citrix SD-WAN appliances, see [IPsec Tunnel Termination](#).

To view **IPsec Tunnel** statistics, navigate to **Reporting > statistics > IPsec Tunnels** tab.

You can view the following metrics:

- **Tunnel Name:** The tunnel name.
- **Tunnel State:** IPsec tunnel state.
- **MTU:** Maximum transmission unit—size of the largest IP datagram that can be transferred through a specific link.
- **Packet Received:** Number of packets received.
- **Packets Sent:** Number of packets Sent.
- **Packet Dropped:** Number of packets dropped, because of network congestion.
- **Bytes Dropped:** Number of bytes dropped.
- **Expand/Collapse:** You can expand or collapse the data as needed.

Real time statistics

You can also get the following real time statistics information under **Troubleshooting > Statistics**:

- Address Resolution Protocol (ARP)
- Routes

- Virtual Path Services
- Classes
- Ethernet
- Observed Protocols
- WAN Path
- Application QoS
- Other Statistics (Rules, Rule Applications, Applications, Site, Multicast Group, IPsec Tunnel, GRE Tunnel, WAN Link Usage, Intranet, Access Interfaces, WAN Links, and MPLS Queues)

Site Report : Real Time Statistics

ARP Routes Virtual Path Services Classes Ethernet Observed Protocols Wan Path Application QoS Rules ▾

Retrieve latest data

No Rows To Show

Rules
Rule Applications
Applications
Site
Multicast Group
IPsec Tunnel

Search

Page 0 of 0

Address Resolution Protocol

To view ARP statistics, navigate to **Reports > Real Time > ARP** tab.

Click **Retrieve latest data** to get the current data.

Site Report : Real Time Statistics

ARP Routes Virtual Path Services Classes Ethernet Observed Protocols Wan Path Application QoS Other Stats ▾

Retrieve latest data

Gateway ARP Timer: 1000
End User ARP Timer: 1000

Num	Interface	Routing Domain	VLAN	IP Address	MAC Address	State	Type
3	3		0	172.10.20.1	86:db:1f:df:62:63	READY_ACTIVE	PERSISTENT
2	2		0	172.10.10.1	c6:23:ae:26:33:56	READY_ACTIVE	PERSISTENT
1	1		0	172.10.10.6	f6:9d:fc:db:18:76	READY_ACTIVE	END_USER
0	0		0	176.10.10.1	00:00:00:00:00:00	REPLY_PENDING	PERSISTENT

1 to 4 of 4 Page 1 of 1

Routes

To view Route statistics, navigate to **Reports > Real Time > Routes** tab.

Site Report : Real Time Statistics

ARP Routes Virtual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats ▾

Retrieve latest data

Search 🔍

routes_Default_RoutingDomain

Num	Network Address	Gateway IP Address	Service	Firewall Zone	Reachable	Site IP Address	Site	Type
0	172.10.10.0/24	*	Local	Default_LAN_Zone	YES	*	San_Francisco	Static
1	172.10.20.0/24	*	Local	Default_LAN_Zone	YES	*	San_Francisco	Static
2	176.10.10.0/24	*	Local	Default_LAN_Zone	YES	*	San_Francisco	Static
3	172.10.30.0/24	*	San_Francisco-Belgi...	Default_LAN_Zone	YES	*	Belgium	Dynamic
4	172.10.40.0/24	*	San_Francisco-Belgi...	Default_LAN_Zone	YES	*	Belgium	Dynamic
5	192.168.40.0/24	*	San_Francisco-New...	Default_LAN_Zone	YES	*	NewYork	Dynamic
6	192.168.80.0/24	*	San_Francisco-Lond...	Default_LAN_Zone	YES	*	London	Dynamic
7	192.168.90.0/24	*	San_Francisco-Madrid	Default_LAN_Zone	YES	*	Madrid	Dynamic
8	0.0.0.0/0	*	Internet	Internet_Zone	YES	*	San_Francisco	Static
9	0.0.0.0/0	*	San_Francisco-Belgi...	Internet_Zone	YES	*	Belgium	Dynamic
10	0.0.0.0/0	*	San_Francisco-Lond...	Internet_Zone	YES	*	London	Dynamic
11	0.0.0.0/0	*	Passthrough	Any	YES	*	*	Static
12	0.0.0.0/0	*	Discard	Any	YES	*	*	Static

Virtual Path Services

To view virtual path service statistics, navigate to **Reports > Real Time > Virtual Path Services** tab.

Site Report : Real Time Statistics

ARP Routes Virtual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats ▾

Retrieve latest data

Search 🔍

From Site	To Site	State	MTU	Latency BOWT (mS)	Worst Jitter (mS)	Best Jitter (mS)	Receive Rate (Mbps)
San_Francisco	Belgium	GOOD	1492	2	2	2	26.70
Belgium	San_Francisco	GOOD	N/A	2	2	2	29.02
San_Francisco	London	GOOD	1492	2	2	2	8.73
London	San_Francisco	GOOD	N/A	2	2	2	12.76
San_Francisco	Madrid	GOOD	1492	2	2	2	8.72
Madrid	San_Francisco	GOOD	N/A	2	2	2	13.29
San_Francisco	NewYork	GOOD	1492	2	2	2	8.74
NewYork	San_Francisco	GOOD	N/A	2	2	2	12.75

Classes

To view Class statistics, navigate to **Reports > Real Time > Classes** tab.

Site Report : Real Time Statistics

ARPRoutesVirtual Path ServicesClassesEthernetObserved ProtocolsWan PathApplication QOSOther Stats

Retrieve latest data

Search

Virtual Path Service : San_Francisco-Madrid

Class	Name	Type	Wait (mS)	Pending kB	Pending Pkts	Sent kB	Sent Pkts	Dropped kB	Dropped Pkt
0	HDX_priority_tag_0	realtime	0	0	0	0	0	0	0
1	HDX_priority_tag_1	interact	0	0	0	0	0	0	0
2	HDX_priority_tag_2	interact	0	0	0	0	0	0	0
3	HDX_priority_tag_3	interact	0	0	0	0	0	0	0
4	class_4	bulk	0	0	0	0	0	0	0
5	class_5	bulk	0	0	0	0	0	0	0
6	class_6	bulk	0	0	0	0	0	0	0
7	class_7	bulk	0	0	0	0	0	0	0
8	RealTime_Low	realtime	0	0	0	0	0	0	0

Ethernet

To view Ethernet statistics, navigate to **Reports > Real Time > Ethernet** tab.

Site Report : Real Time Statistics

ARPRoutesVirtual Path ServicesClassesEthernetObserved ProtocolsWan PathApplication QOSOther Stats

Retrieve latest data

Search

Port	Link State	Frames Sent	Bytes Sent	Frames Received	Bytes Received	Errors
1	UP	257217	369288045	146919	10111132	0
2	UP	903360	75647738	1110000	457690503	0
3	UP	811072	71615021	821492	73408789	0
4	UP	5712	365568	48	3688	0

Observed Protocols

To view observed protocol statistics, navigate to **Reports > Real Time > Observed Protocols** tab.

Site Report : Real Time Statistics

ARP Routes Virtual Path Services Classes Ethernet **Observed Protocols** Wan Path Application QoS Other Stats ▾

Retrieve latest data

Search 🔍

						LAN to WAN		
Rule Group	Rule	Protocol	Port	Service Type	Service Instance	Packets	Bytes	Kb/s
http/www/www-http	585	TCP	80	INTERNET	-	119265	5346866	5.6
https	585	TCP	443	INTERNET	-	17761	1396640	1.4
UNCOMMON	585	TCP	-	INTERNET	-	3	156	0.0
domain	585	UDP	53	INTERNET	-	263	19173	0.0
ntp	585	UDP	123	INTERNET	-	1	76	0.0
https	585	UDP	443	INTERNET	-	48	55856	0.0

WAN Path

To view WAN path statistics, navigate to **Reports > Real Time > WAN Path** tab.

Site Report : Real Time Statistics

ARP Routes Virtual Path Services Classes Ethernet Observed Protocols **Wan Path** Application QoS Other Stats ▾

Retrieve latest data

Search 🔍

Num	From Link	To Link	Congestion	Path State	Reason	Duration (S)	Virtual Path Service State	Source
1	San_Francisco-Broa...	Belgium-Internet-Ve...	NO	GOOD	N/A	8494	GOOD	4980
2	San_Francisco-Inter...	Belgium-Internet-Ve...	UNKNOWN	DEAD	GATEWAY	11724	GOOD	4980
3	San_Francisco-MPL...	Belgium-MPLS-ATT-...	NO	GOOD	N/A	8494	GOOD	4980
4	San_Francisco-MPL...	Belgium-MPLS-ATT-...	NO	GOOD	N/A	8494	GOOD	4980
5	Belgium-Internet-Ve...	San_Francisco-Broa...	NO	GOOD	N/A	8494	GOOD	4980
6	Belgium-Internet-Ve...	San_Francisco-Inter...	UNKNOWN	DEAD	SILENCE	11724	GOOD	4980
7	Belgium-MPLS-ATT-...	San_Francisco-MPL...	NO	GOOD	N/A	8494	GOOD	4980
8	Belgium-MPLS-ATT-...	San_Francisco-MPL...	NO	GOOD	N/A	8494	GOOD	4980
9	San_Francisco-Broa...	London-Broadband-...	NO	GOOD	N/A	7702	GOOD	4980
10	San_Francisco-Inter...	London-Broadband-...	UNKNOWN	DEAD	GATEWAY	11724	GOOD	4980
11	London-Broadband-...	San_Francisco-Broa...	NO	GOOD	N/A	7703	GOOD	4980
12	London-Broadband-...	San_Francisco-Inter...	UNKNOWN	DEAD	SILENCE	11724	GOOD	4980

Application QoS

To view application QoS statistics, navigate to **Reports > Real Time > Application QoS** tab.

Site Report : Real Time Statistics

ARP Routes Virtual Path Services Classes Ethernet Observed Protocols Wan Path **Application QOS** Other Stats ▾

Retrieve latest data

Search 

Num	Site	Service	Routing Domain	IP Address		Port		Application Object	Application	Ap
				Src	Dst	Src	Dst			
0	San_Francisco	San_Francisco-Belgi...	*	*	*	*	*	ica_priority_0	*	0
1	San_Francisco	San_Francisco-Belgi...	*	*	*	*	*	ica_priority_1	*	0
2	San_Francisco	San_Francisco-Belgi...	*	*	*	*	*	ica_priority_2	*	0
3	San_Francisco	San_Francisco-Belgi...	*	*	*	*	*	ica_priority_3	*	0
4	San_Francisco	San_Francisco-Belgi...	*	*	*	*	*	ica	*	0

You can select other statistics as needed from the drop-down list and view the statistics.

MPLS Queues

MPLS queues allow you to define the queues corresponding to the Service Provider MPLS queues, on the MPLS WAN Links. For information on configuring MPLS queues, see [MPLS Queues](#).

To view MPLS Queue statistics, at the site level, navigate to **Reports > Real Time > Statistics**. Click **Other Stats**, select **MPLS Queues**, and click **Retrieve latest data**. The latest MPLS queues data is retrieved from the appliance and is displayed in the SD-WAN Orchestrator.

You can view the direction, no of packets, delta packets, and mismatched DSCP packets for Intranet and Virtual path services.

Site Reports:Real Time Statistics

ARP Routes Virtual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS **MPLS Queues** ▾

Retrieve latest data

Search 

Intranet Data Rates

Name	Direction	Intranet Packets	Intranet Kbps	Delta Intranet Packets	Delta Intranet kB	Mismatched DSCP Packets	Mismatched DSCP kB
branchv6queue	Recv	0	0.00	0	0.00	0	0.00
branchv6queue	Send	0	0.00	0	0.00	0	0.00

1 to 2 of 2 < < Page 1 of 1 > >

Virtual Path Service Data Rates

Name	Direction	Virtual Path Service Packets	Virtual Path Service Kbps	Delta Virtual Path Service Packets	Delta Virtual Path Service kB	Mismatched DSCP Packets	Mismatched DSCP kB	IP, TCP, UI Compress
branchv6queue	Recv	8670933	14.44	8670933	742073.60	0	0.00	0
branchv6queue	Send	8671465	14.39	8671465	739441.35	N/A	N/A	0

1 to 2 of 2 < < Page 1 of 1 > >

Private MPLS Queues

Private MPLS	MPLS Queue	Access Interface	IP Address	Proxy Address	Proxy ARP State	MAC	Last ARP Reply Age(ms)
BRANCH_1-WL-2	branchv6queue	BRANCH_1-WL-2-AI-1	b:3	N/A	N/A	N/A	
MCN_DC-WL-2	ipv6queue	N/A	0.0.0.0	N/A	N/A	N/A	

For private MPLS Queues, you can view the following details:

- **Private MPLS:** The private MPLS WAN link.
- **MPLS Queue:** The MPLS queue associated with the MPLS WAN link.
- **Access Interface:** The access interface associated with the MPLS queue.
- **IP Address:** The IP address associated with the MPLS queue.

- **Proxy Address:** The proxy IP address associated with the MPLS queue.
- **Proxy ARP State:** The state of proxy address resolution protocol. Enabled, disabled, or N/A
- **MAC:** The MAC address of the interface associated with the MPLS queue.
- **Last ARP Reply age:** Time in milliseconds when the last ARP reply was received.

For more details on troubleshooting, see [Troubleshooting MPLS queues](#).

Flows


The **Flows** feature provides unidirectional flow information related to a particular session going through the appliance. This provides information on the destination service type the flow is falling into and also the information related to the rule and class type and also the transmission mode.

Site Report : Real Time Flows

Retrieve latest data

Search

☒ Upload ☒ Download

Customize Columns

Info	No	Application	Source IP Addr	Dest IP Addr	Source Port	Dest Port	Proto IP	Packets	PPS	Class	Service Name	Age (mS)	Bytes
①	1	N/A	172.10.10.6	192.229.232.240	49976	80	TCP (6)	3	0.000	N/A	-	3702175	156
①	2	N/A	172.10.10.6	192.229.232.240	49837	80	TCP (6)	3	0.000	N/A	-	7024077	156
①	3	N/A	172.10.10.6	192.229.232.240	49835	80	TCP (6)	3	0.000	N/A	-	7050202	156
①	4	N/A	172.10.10.6	192.229.232.240	49833	80	TCP (6)	3	0.000	N/A	-	7089890	156
①	5	N/A	172.10.10.6	192.229.232.240	49970	80	TCP (6)	3	0.000	N/A	-	4655644	156
①	6	N/A	172.10.10.6	192.229.232.240	49831	80	TCP (6)	3	0.000	N/A	-	7130125	156
①	7	N/A	172.10.10.6	192.229.232.240	49825	80	TCP (6)	3	0.000	N/A	-	7168561	156
①	8	Google Talk (incl. Hangouts and Allo and Duo)(gtalk)	172.10.10.6	74.125.130.188	49743	443	TCP (6)	201	0.023	N/A	-	31279	9255

Firewall connections

The **Firewall connections** provide the state of the connection related to a particular session based on the firewall action configured. Firewall connections also provide complete details about the source and destination of the connection.

Site Report : Real Time Firewall Connections

Retrieve latest data

Search

Connections Displayed: 2

Connections In Use: 2/128000

Source									
Application	Family	Routing Domain	IP Protocol	IP Addr	Port	Service Type	Service Name	Zone	IP A
Microsoft(micros...	Web	Default_Routing...	TCP	172.10.10.6	49775	Local	VIF-Bridge-1-VL...	Default_LAN_Zone	52.
Google Talk (incl...	Instant Messaging	Default_Routing...	TCP	172.10.10.6	49743	Local	VIF-Bridge-1-VL...	Default_LAN_Zone	74.

Appliance reports (Preview)

Appliance reports deliver the network traffic and system usage reports. Using this data you can troubleshoot network issues or analyze the behavior of your Citrix SD-WAN devices. You can see the following tabs under Appliance Reports page:

- Interface
- Network
- CPU Usage
- Disk Usage
- Memory Usage

Click each tab to view or monitor the appliance graph by hour, day, weekly, and monthly. You can toggle between Absolute and Relative time as required. The table columns are customizable. Click **Customize** column right top corner of the table and select/deselect the options that you want to display or hide in the table.

Customize Columns to be Displayed

☒ Select All
 ☒ Bytes Received
 ☒ Packets Received
 ☒ Error Count Received

☒ Bytes Sent
 ☒ Packets Sent
 ☒ Error Count Sent

Cancel

Done

Interface

The **Interface** page shows the management interface errors/traffic. All the network is divided into different interface, such as Management Interface, Interface 1/2/3.

<div>Dashboard</div> <div>Reports</div> <div>Alerts</div> <div>Usage</div> <div>Quality</div> <div>QoS</div> <div>Historical Statistics</div> <div>Real Time</div> <div>Cloud Direct (preview)</div> <div>OS6 Metrics</div> <div>Appliance Reports</div> <div>Configuration</div>	Site Report : Appliance Reports							Relative Time	Interval: Last 1 Hour
	Interfaces							Customize Columns	
	Interface Name	Bytes Sent	Bytes Received	Packets Sent	Packets Received	Error Count Sent	Error Count Received	Actions	
	Interface 1	37 Kbps	41 Kbps	3193	3427	0	0		
	Interface 3	0 Kbps	0 Kbps	0	0	0	0		
	Management interface	8 Kbps	10 Kbps	273	321	0	0		
	Interface 2	1 Kbps	1 Kbps	79	79	0	0		

- **Interface Name** – Displays the interface name.
- **Bytes Sent** – Average number of bytes sent for the selected duration in Kbps.
- **Bytes Received** – Average number of bytes received for the selected duration in Kbps.
- **Packets Sent** – Average number of packets sent for the selected duration.

- **Packets Received** – Average number of packets received for the selected duration.
- **Error Count Sent** – Number of errors count sent for the selected duration.
- **Error Count Received** – Number of errors count received for the selected duration.
- **Actions** – You can switch on the action button to view the network graph.

Network

The **Network** page shows the number of TCP connections for each configured site.

Site Name	Active	Passive	Failed	Resets	Established	Actions
DC_MCN	1331309	535959	8968	67806	18	

- **Site Name** – Displays the site name.
- **Active** – Average number of active TCP connection counts for the selected duration.
- **Passive** – Average number of passive TCP connection counts for the selected duration.
- **Failed** – Average number of failed TCP connection counts for the selected duration.
- **Resets** – Average number of reset TCP connection counts for the selected duration.
- **Established** – Average number of established TCP connection counts for the selected duration.
- **Actions** – You can switch on the action button to view the network graph.

CPU usage

The **CPU Usage** page shows the CPU utilization of the SD-WAN device as a percentage. The CPU graph shows the average CPU consumption for the regular intervals over the selected time.

Site Name	System	Users	Nice	Idle	Io Wait	Irq	Sof Irq	Steal	Actions
DC_MCN	9.34 %	21.47 %	21.47 %	52.5 %	2.11 %	0 %	0.05 %	1.86 %	

- **Site Name** – Displays the site name.
- **System** – Percentage of total time the CPU spent processing system-space programs.
- **Users** – Percentage of total time the CPU spent processing user-space programs.
- **Nice** – Nice is when the CPU is running a user task having below-normal priority.
- **Idle** – Percentage of total time the CPU was in Idle mode.

- **Io Wait** – Percentage of total time the CPU spent waiting for I/O operations.
- **Irq** – The interrupt requests (IRQs) value that the kernel serves.
- **Steal** – When running in a virtualized environment, the hypervisor might steal cycles that are meant for your CPUs and give them to another, for various reasons. This time is known as steal.
- **Actions** – You can switch on the action button to view the network graph.

Disk usage


The **Disk Usage** page shows the amount of hard disk space used by the operating system and data partition in an I/O per second (IOPS) value.

Site Name	Disk Name	Read IOPS	Write IOPS	Latency	Read Throughput	Write Throughput	Disk Utilization	Actions
DC_MCN	loop0	0 IOPS/sec	0 IOPS/sec	0 ms	0 Kbps	0 Kbps	0 %	
DC_MCN	xvda	0 IOPS/sec	15 IOPS/sec	0 ms	0 Kbps	0 Kbps	21 %	

- **Site Name** – Displays the site name.
- **Disk Name** – Displays the hard disk name.
- **Read IOPS** – Displays the average number of read IOPS per second over the selected time frame.
- **Write IOPS** – Displays the average number of write IOPS per second over the selected time frame.
- **Latency** – Displays the latency value of the successful read and write requests from the selected volume workload over the selected time frame. It is recommended that below 10 ms latency value is best for I/O performance.
- **Read Throughput** – Displays the average disk throughput value of the disk read operation over the selected time in Kbps.
- **Write Throughput** – Displays the average disk throughput value of the disk write operation over the selected time in Kbps.
- **Disk Utilization** – Displays the average disk utilization value in percentage over the selected time frame.
- **Actions** – You can switch on the action button to view the network graph.


Memory usage


The **Memory Usage** page shows the report of the amount of memory used.

Site Report : Appliance Reports 

Relative Time Interval Last 1 Day

Interfaces Network CPU Usage Disk Usage Memory Usage

 Customize Columns

Site Name	Apps	Swap Cache	Slab Cache	Shmem	Cache	Buffers	Unused	Swap	Actions
DC_MCN	3.11 Gb	0 Kb	306.7 Mb	1.63 Mb	6.91 Gb	297 Mb	1.39 Gb	0 Kb	

- **Site Name** – Displays the site name.
- **Apps** – Displays the used application value in Gb.
- **Swap Cache** – Displays the swap cache number in Mb. Swap cache is a list of page table entries with one entry per physical page.
- **Slab Cache** – Displays the number of pre-allocated slabs of memory. In Mb
- **Shmem** – Displays the total used shared memory value in Mb.
- **Cache** – Displays the number of cache memories used in Gb.
- **Buffers** – Displays the number of the physical memory that is used by the buffer cache.
- **Unused** – Displays the number of unused memories for cache.
- **Swap** – Displays the number of swap spaces. The swap space is used if you need some space extension for your physical memory.
- **Actions** – You can switch on the action button to view the network graph.

Diagnostics

January 11, 2021

You can use Ping, Traceroute, Packet Capture, and Bandwidth test diagnostic utilities to test and investigate network connectivity issues on your SD-WAN network.

You can **Download**, **Copy**, and **Clear** the report results as needed.

☐ Ping
 ☐ Traceroute
 ☐ Packet Capture
 ☐ Bandwidth Test

- **Ping** – You can check network connectivity by pinging a remote host or a site. Enter the destination details, specify the number of times to send the ping request and the number of data bytes. Provide the destination **IP Address** and click **Run**.

☒ Ping
 ☐ Traceroute
 ☐ Packet Capture
 ☐ Bandwidth Test

Source Site

Source Site
Belgium

PING

IP Address: Interface: Default Gateway IP (Optional): Default

Routing Domain: Default_RoutingDomain Ping Count: 5 Packet Size (KB): 70

Cancel Run

Results

Download Copy Clear

```

*****Result of ping*****
PING 80.80.80.80 with 70 bytes of data (5 attempts)
 70 bytes from 80.80.80.80: icmp_seq=1 ttl=54 time=40.070 ms icmp_code=0
 70 bytes from 80.80.80.80: icmp_seq=2 ttl=54 time=39.714 ms icmp_code=0
 70 bytes from 80.80.80.80: icmp_seq=3 ttl=54 time=39.959 ms icmp_code=0
 70 bytes from 80.80.80.80: icmp_seq=4 ttl=54 time=39.990 ms icmp_code=0
 70 bytes from 80.80.80.80: icmp_seq=5 ttl=54 time=39.569 ms icmp_code=0
  
```

- **Traceroute** - You can trace the route and the number of hops between sites. Select the source and destination site along with the path to trace and click **Run**.

☐ Ping
 ☒ Traceroute
 ☐ Packet Capture
 ☐ Bandwidth Test

Source Site

Source Site
Belgium

Traceroute

Destination Site: San Francisco Path: Belgium-Internet-Verizon_Comm-2->San_Francisco-Broadband-AMI

Cancel Run

Results

Download Copy Clear

```

*****Result of traceroute*****
Trace Route initiated on Virtual Path San_Francisco-Belgium, Path Belgium-Internet-Verizon_Comm-2->San_Francisco-Broadband-AMIS-2.
Please wait while the trace is completed.
Trace Route Results:
Virtual Path: San_Francisco-Belgium
Path: Belgium-Internet-Verizon_Comm-2->San_Francisco-Broadband-AMIS-2
Trace Route to 172.10.10.10, destination was reached after 2 hops, 2 hops attempted.

  hops      rtt 1      rtt 2      rtt 3      mean rtt
  1  172.10.30.1      0.374ms    0.369ms    0.340ms    0.361ms
  2  172.10.10.10     1.546ms    1.517ms    1.511ms    1.525ms
Hops to destination: 2
  
```

- **Packet Capture** – You can intercept the data packet that is traversing over the selected active interface present in the selected site. You can view the source and destination details.

The screenshot shows the 'Packet Capture' configuration window. At the top, there are checkboxes for 'Ping', 'Traceroute', 'Packet Capture' (which is checked), and 'Bandwidth Test'. Below this, the 'Source Site' is set to 'Belgium'. The 'Packet Capture' section includes fields for 'Interface' (set to '2'), 'Filter' (empty), 'Duration (seconds)' (set to '5'), and 'Max no of packets to view' (set to '1000'). There are 'Cancel' and 'Run' buttons. The 'Results' section on the right shows a list of captured packets with details like timestamp, source/destination IP, and protocol. A 'Help' link is visible next to the 'Filter' field.

The **Help** option provides more detail on the **Filter Options**.

- **Bandwidth Test** – You can run a bandwidth test on a specific path of a site to view the maximum, minimum and average bandwidth usage. Enter the source site, destination site, and select the path. Click **Run**.

The screenshot shows the 'Bandwidth Test' configuration window. At the top, there are checkboxes for 'Ping', 'Traceroute', 'Packet Capture', and 'Bandwidth Test' (which is checked). Below this, the 'Source Site' is set to 'Belgium'. The 'Bandwidth Test' section includes fields for 'Destination Site' (set to 'San Francisco') and 'Path' (set to 'Belgium-Internet-Verizon_Comm-2->San_Francisco-Broadband-AMI'). There are 'Cancel' and 'Run' buttons. The 'Results' section on the right shows the results of the bandwidth test, including 'Minimum Bandwidth: 773478 kbps', 'Maximum Bandwidth: 1038753 kbps', and 'Average Bandwidth: 913857 kbps'.

User administration

March 8, 2021

SD-WAN Orchestrator for On-premises supports role-based access control (RBAC). RBAC regulates access to SD-WAN Orchestrator resources based on the roles assigned to individual users. RBAC allows users to access only the data that their role demands and restricts any other data.

A role defines the permissions to view and perform various activities on SD-WAN Orchestrator for On-premises. You can assign a user with a role from the list of predefined roles.

NOTE

Roles can be assigned at the Customer level only.

By default, a user account is created on SD-WAN Orchestrator for On-premises with user name **admin** and password set as **password**. The user is asked to change the default password during initial login.

You can add users who can be authenticated locally and remotely. Users who are authenticated remotely are authenticated through RADIUS or TACACS+ authentication servers.

Customer roles

The following table lists the predefined customer roles:

Role	Description
Customer-Master-Admin	A customer administrator who can view and edit customer information
Customer-Master-ReadOnly-Admin	A customer administrator who can only view customer information

A user with **Customer-Master-Admin** role can perform the following:

- Add users and assign customer roles
- Edit or delete assigned roles

Support roles

For troubleshooting purposes, Customers can assign support roles and provide Support Team members the ability to view and edit their information. Support roles have a validity period that is defined while assigning the role. After the validity period expires, the support user loses access to Customer information. However, the support user details continue to appear under the **Administration > User Administration**. Based on the need, the Customer administrator can either delete or extend the validity of the support role.

Role	Description
Customer-Support-ReadWrite	A support team member who can view and edit the customer information
Customer-Support-ReadOnly	A support team member who can only view the customer information

Authentication types

SD-WAN Orchestrator for On-premises supports the following types of authentication:

- **Single-factor authentication:** Single-factor authentication presents one authentication method to gain access to SD-WAN Orchestrator for On-premises for users.
- **Two-factor authentication (TFA):** Two-factor authentication presents two authentication methods to gain access to SD-WAN Orchestrator for On-premises for users. It introduces an extra layer of security in the login sequence.

The following authentication methods are supported for single-factor and two-factor authentication:

- **Local:** When selected, the user must use the password configured on SD-WAN Orchestrator for On-premises to gain access.
- **RADIUS:** When selected, the user must use the RADIUS server password to gain access.
- **TACACS+:** When selected, the users must use the TACACS+ server password to gain access.

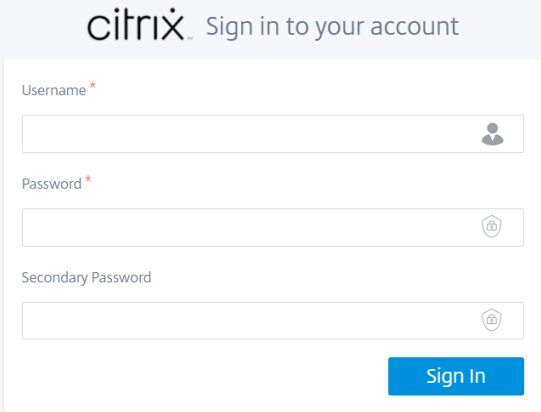
The following table lists the primary and secondary authentication methods supported for users who are authenticated locally:

	Primary Authentication Type	Secondary Authentication Type
Single-factor authentication	Local	-
Two-factor authentication	Local	RADIUS or TACACS+

The following table lists the primary and secondary authentication methods supported for users who are authenticated remotely:

	Primary Authentication Type	Secondary Authentication Type
Single-factor authentication	Local, RADIUS, or TACACS+	-
Two-factor authentication	Local, RADIUS, or TACACS+	RADIUS or TACACS+

If **Two-factor authentication** is enabled and the RADIUS/TACACS+ servers are configured as a secondary authentication type, then the **Secondary password** field is visible at the login page.



The image shows a Citrix login page with the title "citrix Sign in to your account". The form contains three input fields: "Username" with a red asterisk, "Password" with a red asterisk, and "Secondary Password". Each field has a corresponding icon (person, padlock, and padlock) to its right. A blue "Sign In" button is located at the bottom right of the form. Below the form, the text "Copyright(©) Citrix Systems, Inc. All rights reserved." is displayed.

Add a user

Navigate to **Administration > User Administration** > click **+ New** > Enter the following details > click **Add**.

- Enter the user name.
- **Single factor authentication:** Enables only the primary authentication for logging in the users.
- **Two factor authentication:** Enables both primary and secondary authentication for logging in the users. For more information, see [Remote Authentication Servers](#).
- **Primary Authentication Type:** Select Local or the IP address of the remote authentication server.
- **Secondary Authentication Type:** Select the IP address of the remote authentication server.

NOTE

The **Secondary Authentication Type** field is grayed out if Single factor authentication is chosen.

- **Role:** Select a role from the list of the available roles.
- **Expiration Date (MM/DD/YYYY):** The date up to which the support user has access to customer information. The default validity period is for two weeks from the date the role is assigned.

- Enter your password. The length of the password must be between 8–128 characters.

Add User

Username *

user1

☒ Single factor authentication ☐ Two factor authentication

Primary Authentication Type

Local

Role

Customer-Master-Admin

Expiration Date (MM/DD/YYYY)

N/A

Password *

.....

Confirm Password *

.....

Add

Cancel

Using the **Actions** column, you can change the user role, update the password, and edit the authentication type. You can also delete the user if necessary.

Network Administration: User Administration

Users

+ New

User	Role	Expiration	Primary Auth Server	Secondary Auth Server	Actions
admin	Customer-Master-Ad...	N/A	Local	None	...
tac_sdwan1	Customer-Master-Ad...	N/A	10.1.1.98 (TACACS...	None	...
rad_sdwan1	Customer-Master-Ad...	N/A	Local	10.1.1.99 (RADIUS)	...
test	Customer-Master-Re...	N/A	Local	None	...

Page Size: 200

Showing 1 - 4 of 4 items

Page1 of1

Change authentication type

You can change the authentication type of a user from single-factor authentication to two-factor authentication and conversely.

To change the authentication type of a user, in the **Actions** column, click ... and then **Edit Authentication Server**.

Network Administration: User Administration

Users

[+ New](#) [Remote Authentication Servers](#)

User	Role	Expiration	Primary Auth Server	Secondary Auth Server	Actions
admin	Customer-Master-Admin	N/A	Local	None	
rad_sdwan1	Customer-Support-Rea...	02/03/2021	Local	(RADIUS)	
tac_sdwan1	Customer-Master-Read...	N/A	(RADIUS)	(TACACS+)	
tac_sdwan2	Customer-Support-Rea...	02/03/2021	Local	(TACACS+)	
rad_sdwan2	Customer-Support-Rea...	N/A	(TACACS+)	(RADIUS)	

Page Size: 200 Showing 1 - 5 of 5 items Page 1 of 1

If you have currently selected **Single factor authentication**, you can switch to two-factor authentication. Click **Two factor authentication** and select the remote server from **Secondary Authentication Type** drop-down list. Click **Apply**.

Edit Authentication Type

Username

test

☐ Single factor authentication ☒ Two factor authentication

Primary Authentication Type Secondary Authentication Type

Local 1.4 (RADIUS)

Apply Cancel

If you have currently selected two factor authentication, you can choose to change only the secondary authentication type or switch to single factor authentication.

To switch to single factor authentication, click **Single factor authentication**. The **Secondary Authentication Type** drop-down list gets disabled and only the **Primary Authentication type** drop-down list

is enabled.

Primary Authentication Type can only be set at the time of user creation and it cannot be edited later.

Change password

You can change the password of local users. To change the password of a user, in the **Actions** column, click ... and **Update Local Password**.

NOTE

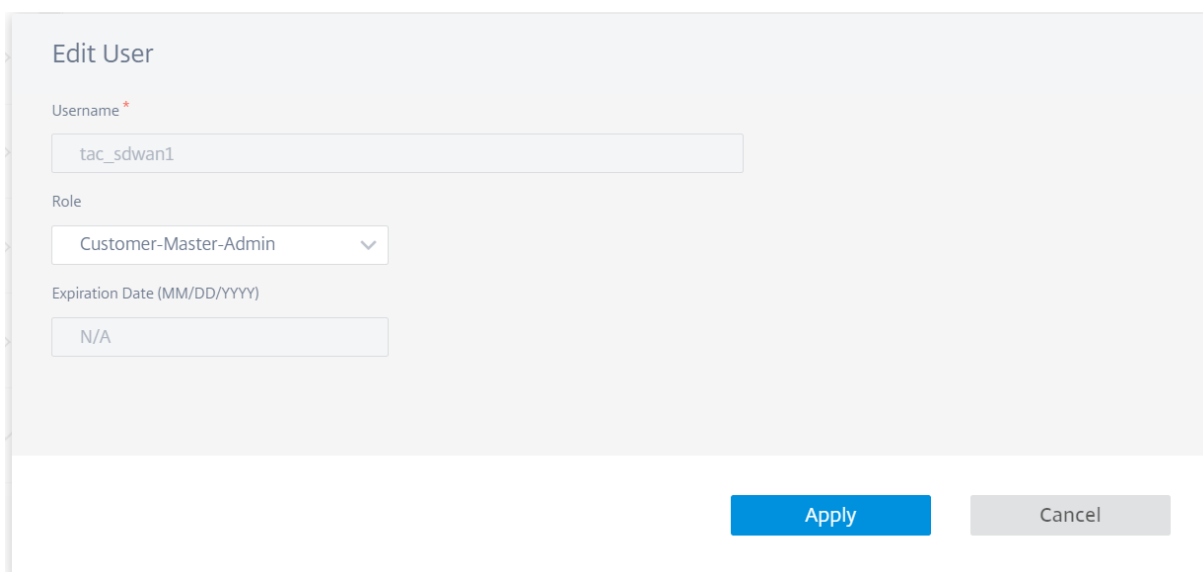
You can modify the password only for local users. For users authenticated remotely, you must update the password on the external server.

Change user role

To change the user role, click the **Edit** icon in the **Actions** column. Select a **Role** and click **Apply**.

NOTE

You cannot edit the role of the default admin user.



The screenshot shows a modal dialog titled "Edit User". It contains three input fields: "Username" with a red asterisk, "Role" (a dropdown menu), and "Expiration Date (MM/DD/YYYY)". The "Username" field contains "tac_sdwan1", the "Role" dropdown shows "Customer-Master-Admin", and the "Expiration Date" field contains "N/A". At the bottom right, there are two buttons: "Apply" (blue) and "Cancel" (gray).

Domain name

March 8, 2021

The domain name is a vanity URL used in the address bar to access SD-WAN Orchestrator for On-premises. Using domain name makes it easier to remember and also allows you to use your company brand name.

To use a domain name ensure that you have a local DNS server configured with a DNS record linking the domain name to SD-WAN Orchestrator for On-premises management IP address. Ensure that the domain name is configured during early configuration. On setting up a domain name, SD-WAN Orchestrator for On-premises reboots and certificates are regenerated automatically. The same domain name must be configured on the individual appliances. For more details, see [On-prem SD-WAN Orchestrator configuration on SD-WAN appliance](#).

It is not mandatory to configure a domain name. If you do not have a domain name and you still want to use DNS Server for IP address resolution, configure DNS records that point to SD-WAN Orchestrator for On-premises IP for the following three FQDNs:

- sdwanzt.citrixnetworkapi.net
- download.citrixnetworkapi.net
- sdwan-home.citrixnetworkapi.net

For example, if SD-WAN Orchestrator for On-premises domain is configured as **citrix.com**, then you must create the DNS record in the DNS Server for the below FQDN and SD-WAN Orchestrator for On-premises IP address:

- download.citrix.com
- sdwanzt.citrix.com
- sdwan-home.citrix.com

In advanced configuration:

For Example: If SD-WAN Orchestrator on-premises domain is configured as **citrix.com**, **Download Management Service Domain** is configured as **download.citrix.com**, and the **Statistics Management Service Domain** is configured as **statistics.citrix.com**, then you must create the DNS record in the DNS Server for the below FQDN and corresponding IP Address:

- download.citrix.com
- sdwanzt.citrix.com
- statistics.citrix.com

Configuring or changing a domain name for an existing configuration affects SD-WAN Orchestrator for On-premises and appliance connectivity. You must manually perform the [certificate authentication](#) process or use the [Site zero-touch deployment settings](#) option.

To configure a domain name, at the network level, navigate to **Administration > Domain Name** and provide a SD-WAN Orchestrator for On-premises domain name.

Custom Domains

☐ Advanced Configuration

On-prem SD-WAN Orchestrator Domain *

xyz.com

Apply

HTTPS certificate

March 23, 2021

HTTPS certificate is required for establishing secure management HTTPS connection to SD-WAN Orchestrator for On-premises. You can use the default HTTPS certificate available on the SD-WAN Orchestrator for On-premises GUI or upload a custom HTTPS certificate generated from any other framework such as OpenSSL or from a trusted authority. Custom HTTPS certificate allows you to have control over the security and the other subject parameters related to the certificate.

To view the default certificate, navigate to **Administration > HTTPS Certificate**.

Network Administration: HTTPS Certificate

[Regenerate](#)

Installed Certificate

Issuer	
Country	US
State/Province	California
Locality	San Jose
Organization	Citrix Systems, Inc.
Organizational Unit	Engineering
Common Name	Citrix
Email	support@citrix.com

Issued To	
Country	US
State/Province	California
Locality	San Jose
Organization	Citrix Systems, Inc.
Organizational Unit	Engineering
Common Name	Citrix
Email	support@citrix.com

Certificate Details	
Certificate Fingerprint	3B:2D:02:7F:8B:7B:6C:9A:07:7D:0B:0B:07:7A:4C:07:0B:4D:4C
Start Date	March 18 08:09:35 2021 GMT
End Date	March 18 08:09:35 2022 GMT
Serial Number	04000007000700070007000700070007000700070007

Upload Certificate

Upload Certificate

Click to select or drag n drop file here.
Allowed file types are .crt

Upload Key

Click to select or drag n drop file here.
Allowed file types are .key

Upload

The **Installed Certificate** section provides a summary of the certificate that is installed on the appliance. The appliance uses this certificate to identify itself in the network.

The **Issued to** section provides details about who the certificate was issued to. The **Common Name** in the certificate matches with the name of the appliance, since the certificate is bound to the appliance name. The **Issuer** section provides the details of the certificate signing authority, who signed the certificate. The Certificate details include the fingerprint of the certificate, serial number, and the validity period for the certificate.

To regenerate the certificate, navigate to **Administration > HTTPS Certificate** and click **Regenerate**.

Note

Regenerating the certificate disconnects any existing connected HTTPS sessions and restarts the HTTPS server. After the certificate is successfully regenerated, the GUI gets refreshed automatically.

You can generate HTTPS certificates from any other framework such as OpenSSL or from a trusted authority and upload it on the SD-WAN Orchestrator for On-premises. Certificate format supported is .crt and key format supported is .key.

To upload a custom HTTPS certificate, click **Upload** or drag the certificate and key files in the **Upload Certificate** and **Upload Key** boxes respectively. After successful upload, the GUI gets refreshed automatically.

Disk space management

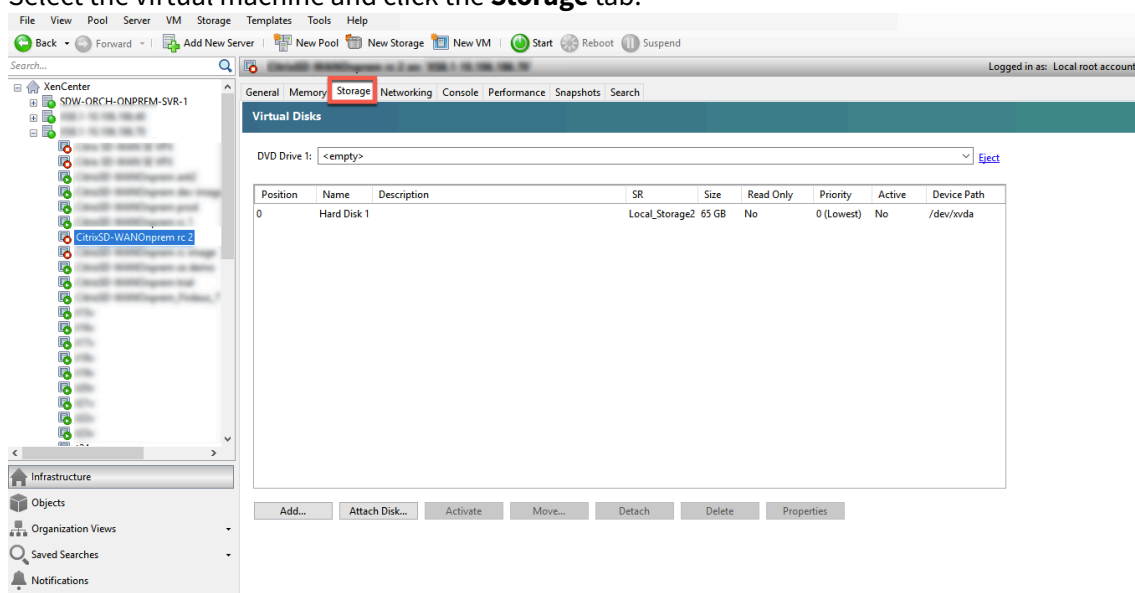
March 8, 2021

You can increase the disk space allocated for Citrix SD-WAN Orchestrator on-premises.

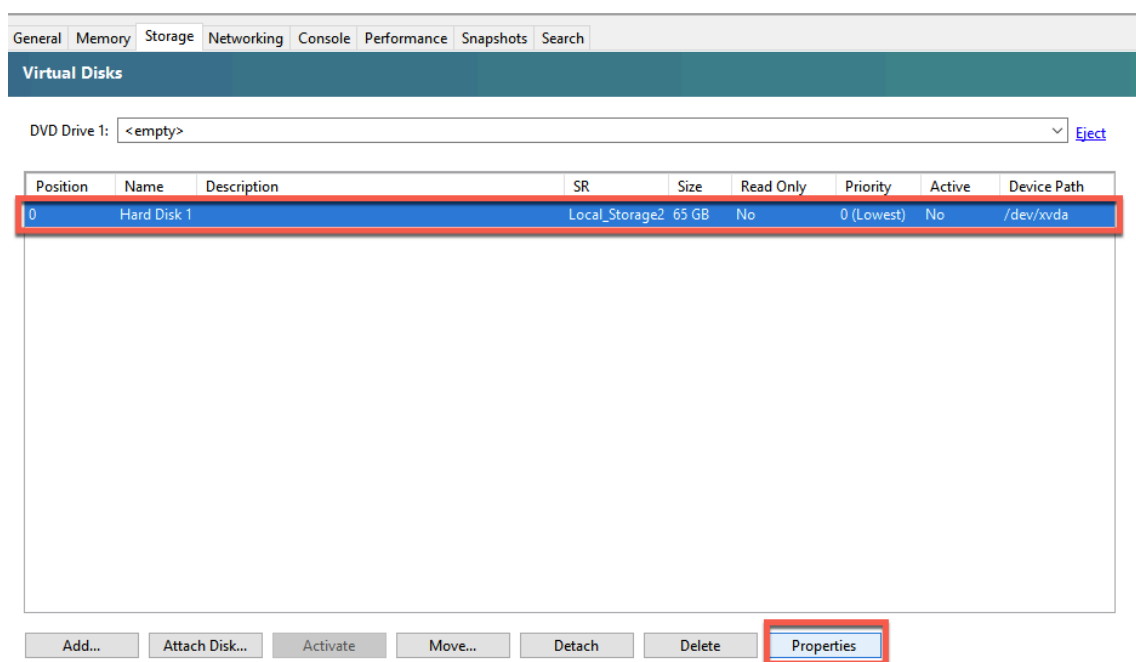
Increase disk space on Citrix Hypervisor

To increase the disk space on Citrix Hypervisor.

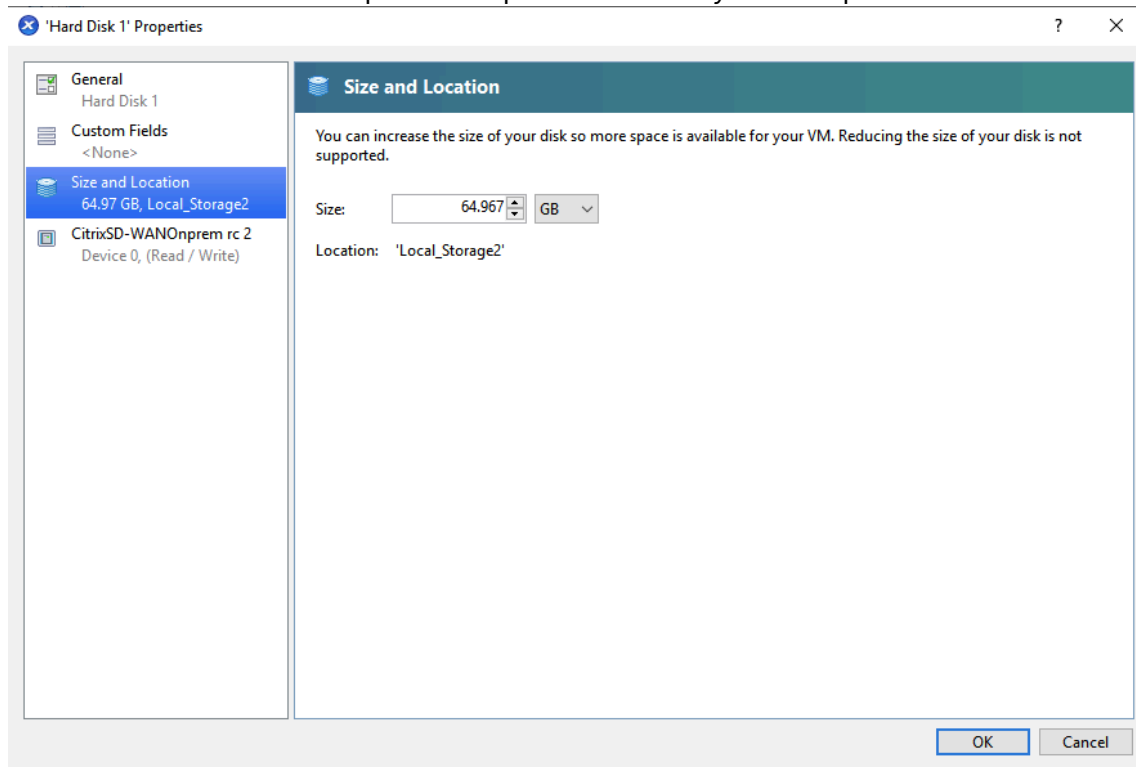
1. Shut down the virtual machine (VM) from the hypervisor.
2. Select the virtual machine and click the **Storage** tab.



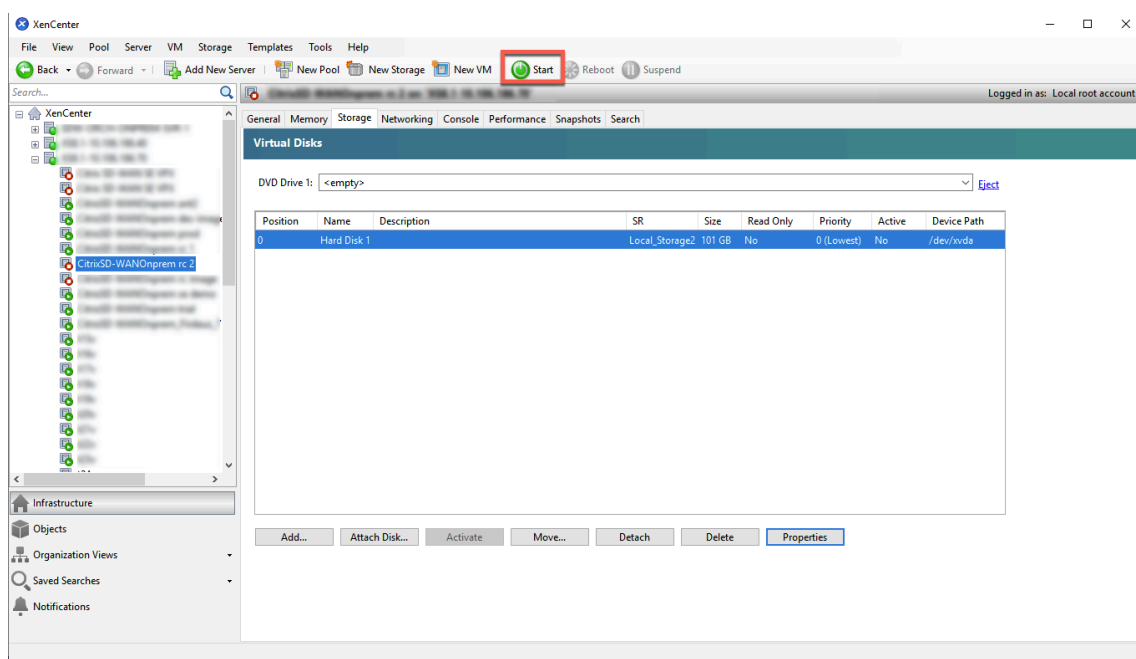
3. Select the hard disk and click **Properties**.



4. Click the **Size and Location** option and update the **Size** of your disk space. Click **OK**.



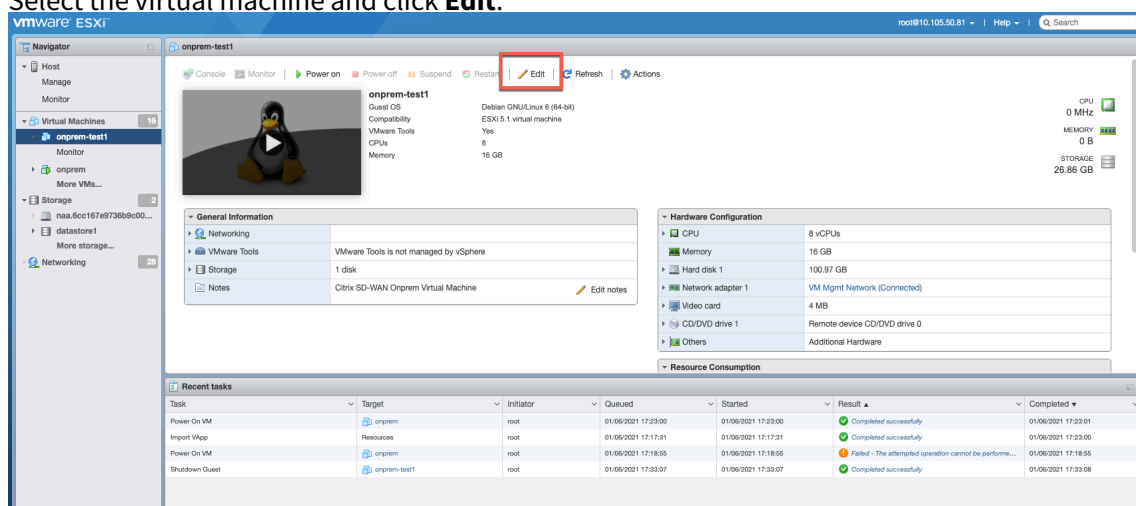
5. Click **Start**.



Increase disk space on ESXi Server

To increase the disk space on the ESXi server.

1. Shut down the virtual machine (VM) from the hypervisor.
2. Select the virtual machine and click **Edit**.



3. Select the **Virtual Hardware** tab.

Edit settings - onprem-test1 (ESXi 5.1 virtual machine)

Virtual Hardware VM Options

Add hard disk Add network adapter Add other device

CPU	8	
Memory	16384	MB
Hard disk 1	100.966791	GB
SCSI Controller 0	LSI Logic SAS	
Network Adapter 1	VM Mgmt Network	<input checked="" type="checkbox"/> Connect
CD/DVD Drive 1		
Video Card	Specify custom settings	

Save Cancel

4. Increase the hard disk space in the **Hard disk** field and click **Save**.

Edit settings - onprem-test1 (ESXi 5.1 virtual machine)

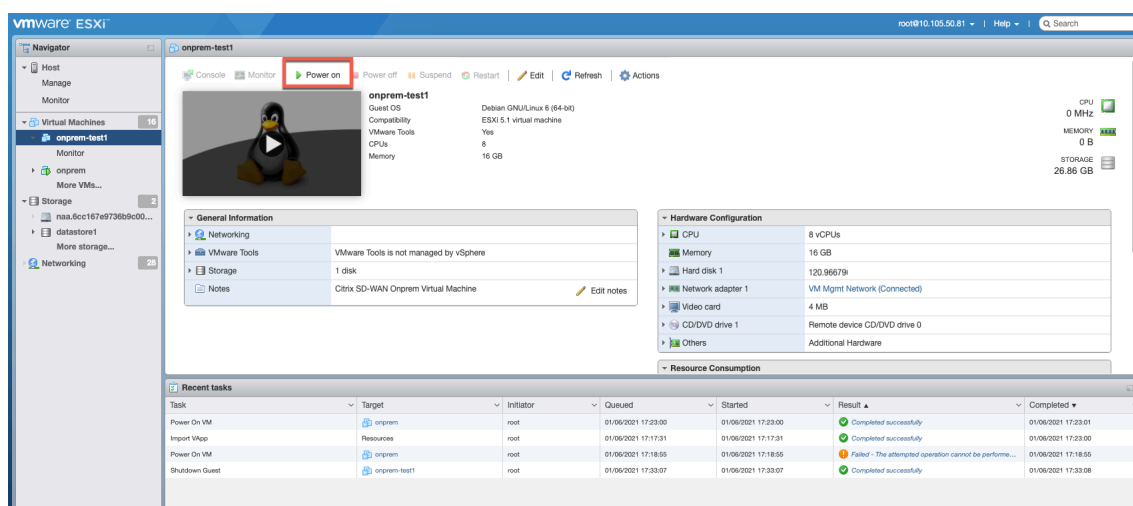
Virtual Hardware VM Options

Add hard disk Add network adapter Add other device

CPU	8	
Memory	16384	MB
Hard disk 1	120.966791	GB
SCSI Controller 0	LSI Logic SAS	
Network Adapter 1	VM Mgmt Network	<input checked="" type="checkbox"/> Connect
CD/DVD Drive 1		
Video Card	Specify custom settings	

Save Cancel

5. Click **Power on**.



March 8, 2021

Replace an affected Citrix SD-WAN appliance

To replace an affected appliance in SD-WAN Orchestrator for On-premises:

1. Log in to SD-WAN Orchestrator for On-premises and select the affected site. At the site level, navigate to **Configuration > Site Configuration > Device Information** and remove the serial number from the **Primary Device Serial Number** field. Click **Save**.

Note

If the appliance is still reachable through SD-WAN Orchestrator for On-premises, then the appliance is in “Factory Reset” state.

Device Information

☒ Enable HA

Primary Device Serial Number

Enter Device Serial (Required for Deployment)

Short Name

Primary

Secondary HA Device Serial Number

H3TM4CXEJV

HA Device Short Name (Optional)

Secondary

Advanced HA Settings

Cancel

Save

Prev

Next

2. Navigate to **Dashboard > Devices** and ensure that the affected appliance is removed from the list.

Site Dashboard

Relative Time Interval: Last 1 Hour

ALERTS [See All](#)
0 Critical

UPTIME [See Details](#)
No Statistics Available

TOP APPS [See All](#)
No Statistics Available

TOP APP CATEGORIES [See All](#)
No Statistics Available

WAN

DEVICES

Device Info

Availability	Cloud Connectivity	Uptime	Short Name	Device Model	Device Edition	Serial No.	Bandwidth	Management IP	Actions
--------------	--------------------	--------	------------	--------------	----------------	------------	-----------	---------------	---------

3. Make a note of the affected appliance's power and cabling setup and then remove the appliance from the rack.

4. Mount the new appliance on the rack and redo the power and cabling as it was for the affected appliance.
5. In the SD-WAN Orchestrator for On-premises UI, at the site level, navigate to **Configuration > Site Configuration > Device Details**. Add the serial number of the new appliance in the **Primary Device Serial Number** field. Click **Save**.

The screenshot displays the 'Device Information' form in the SD-WAN Orchestrator for On-premises UI. The form is titled 'Device Information' and contains several input fields. The 'Primary Device Serial Number' field is highlighted with a red border and contains the value 'HE530CXRDG'. To its right is the 'Short Name' field, which contains the value 'Primary'. Below these are the 'Secondary HA Device Serial Number' field, containing 'H3TM4CXEJV', and the 'HA Device Short Name (Optional)' field, containing 'Secondary'. The form also features an 'Advanced HA Settings' section, which is currently collapsed. At the bottom of the form, there are four buttons: 'Cancel', 'Save', 'Prev', and 'Next'.

6. Configure Zero-touch deployment. For more information, see [Zero-touch deployment](#).
7. Allow a few minutes for the appliance to update cloud connectivity on the site dashboard.

Network Dashboard

Relative Time: Interval: Last 1 Hour Site Group: All

ALERTS [See All](#)

0
Critical

UPTIME [See Details](#)

No Statistics Available

TOP APPS [See All](#)

No Statistics Available

TOP SITES [See All](#)

No Statistics Available

[+ New Site](#) Map List Select Continent Select Country Search

2 Total Sites **2** Critical

Availability	Cloud Connectivity	Site Name	Site Role	Device Model	Serial Number	Bandwidth Tier	Management IP
●	● Online	MCN_VPX	MCN	VPX-SE	6E886BCA-18CF-6C...	1000	10.102.77.106
●	● Online	Client_vpx	Branch	VPX-SE	HE530CXRDG	1000	10.102.77.107

Page Size: 200 Showing 1 - 2 of 2 items Page 1 of 1

8. At the network level, navigate to **Configuration > Network Config Home** and click **Deploy Config/Software**.

9. Click **Stage**.

[Home](#) [Verify Config](#) [Current Deployment](#) [Deployment History](#) [Change Management Settings](#)

Software Version: 11.2.1.56

Stage **Activate**

0/0 **Staged Appliances**

0/0 **Activated Appliances**

Total Appliances	Staged	Activated	Failed
0	0	0	0

Online	Site	Status	HA State	Software Version
--------	------	--------	----------	------------------

10. Click **Activate** after staging is completed.

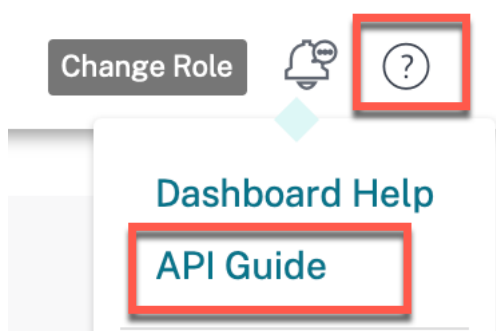
11. Navigate to the site dashboard and verify the successful activation of the appliance.

API guide for SD-WAN Orchestrator for On-premises

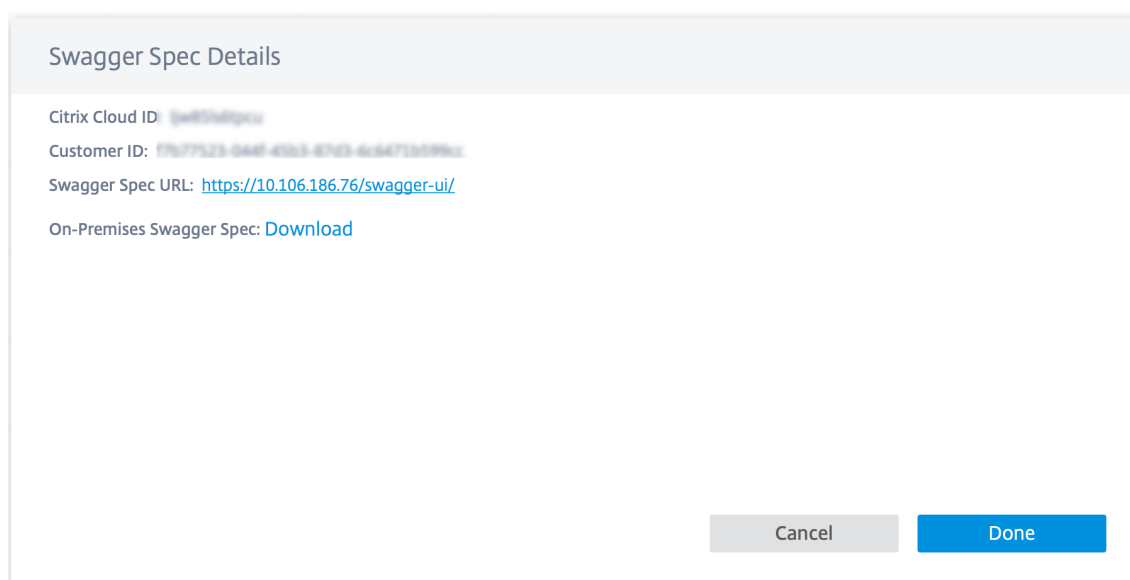
March 8, 2021

To access the SD-WAN Orchestrator for On-premises API Guide on the Swagger UI:

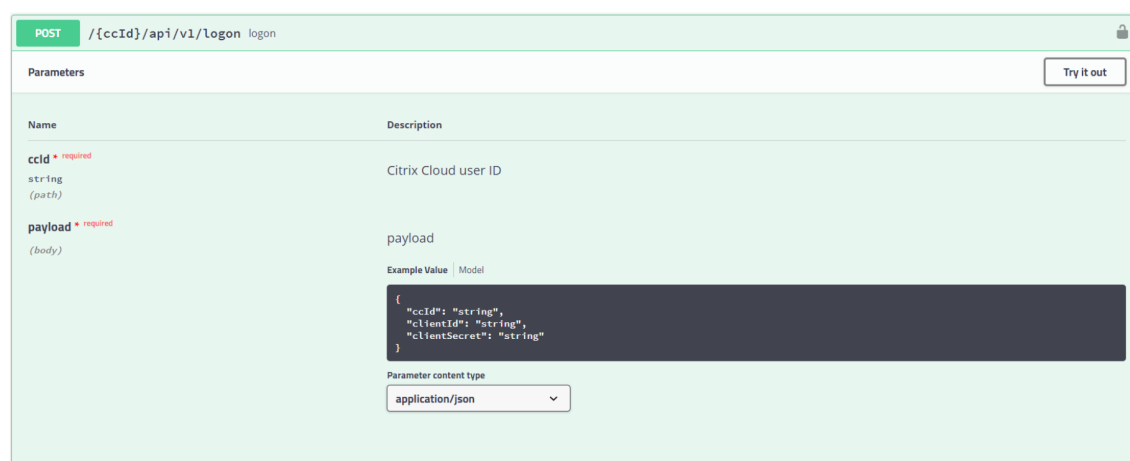
- Log in to the SD-WAN Orchestrator for On-premises and click **?** at the top-right corner of the UI and then click **API Guide**.



The Swagger spec details are displayed.



2. Click the Swagger spec URL to access the API guide.
3. In the API page, navigate to **auth-controller** > **/{{ccId}}/api/v1/logon** > **Try it out**.



4. From the SD-WAN Orchestrator for On-premises **Swagger Spec Details**, copy the **Citrix Cloud ID** and paste it in the textbox under **Citrix Cloud user ID**.

- POST

/{{ccId}}/api/v1/Logon logon

Parameters


Cancel

Name	Description
ccId • required string (path)	Citrix Cloud user ID <div>zbkdfhgls</div>
payload • required (body)	payload Example Value Model <pre>{ "ccId": "zbnkdfhgls", "clientId": "zbnkdfhgls", "clientSecret": "zbnkdfhgls" }</pre>

Cancel

Parameter content type
application/json

- [illegible]

-  swagger

Select a spec


default

SD-WAN Orchestrator API Guide ^{2.0.0}

[Base URL: `sdwan-policy.citrixnetworkapi.net/`]
<https://sdwan-policy.citrixnetworkapi.net/v2/api-docs>

This is an API guide to manage your network through the SD-WAN Orchestrator

Citrix Systems

Authorize 

Available authorizations x

apiKey (apiKey)
Name: Authorization
In: header
Value:

Done Authorize

This completes the authorization process and you must now be able to access and use SD-WAN Orchestrator for On-premises APIs.

Orchestrator administration

January 20, 2021

This section provides you the information on administrative activities that can be performed on the SD-WAN Orchestrator for On-premises platform.

Software

You can download Citrix SD-WAN appliance software version required for all the appliances in your network and stored in SD-WAN Orchestrator for On-premises. Use the stored software to upgrade your SD-WAN Orchestrator for On-premises software to the latest version.

Publish software

SD-WAN Orchestrator for On-premises allows you to download Citrix SD-WAN appliance software version required for all the appliances in your network. The published software is downloaded and stored in SD-WAN Orchestrator for On-premises. You can further deploy the published software to all the appliances managed by SD-WAN Orchestrator for On-premises.

To publish software, at the network level, navigate to **Infrastructure > Orchestrator Administration > Software Images > Appliance**.

Orchestrator

Appliance

Publish New Software

Software Version

11.3.0.119

Publish

Published Software Details

Refresh

Software Version	Status	Details	Actions
------------------	--------	---------	---------

You can choose a software version to be published from a pre-built list of software versions that are supported by the current SD-WAN Orchestrator for On-premises. For newer software versions that are not available in the list, upgrade to the latest SD-WAN Orchestrator for On-premises release which supports the new software version. For information on upgrading SD-WAN Orchestrator for On-premises, see [Software upgrade](#).

Publish New Software

Software Version

11.3.0.119

11.2.2.14

11.2.2.8

11.3.0.112

11.3.0.117

11.3.0.119

11.3.0.4002

11.3.0.5018

11.3.0.5022

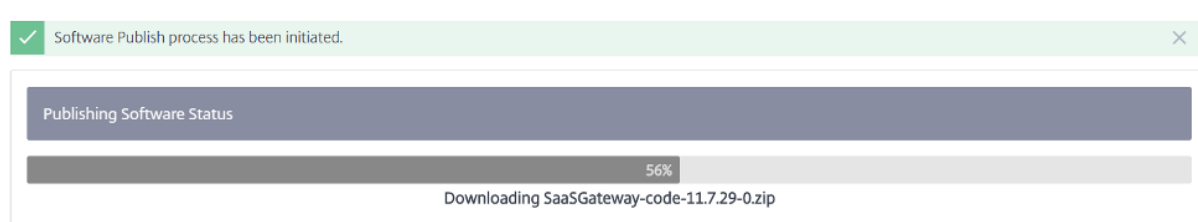
11.3.0.5024

Status

Details

Actions

SD-WAN Orchestrator for On-premises downloads Citrix SD-WAN software of the selected version for all the platforms. A progress bar indicates the progress of the publishing process.



The published software versions are displayed under **Published Software Details**. At any given point SD-WAN Orchestrator for On-premises can store up to three published software versions. If you are intending to publish another software version, delete one of the three versions available before beginning the publishing process.

Published Software Details			
Refresh			
Software Version	Status	Details	Actions
11.2.2.2	FINISHED	Successfully downloaded and published the...	
11.3.0.98	FINISHED	Successfully downloaded and published the...	
11.2.1.56	FINISHED	Successfully downloaded and published the...	

After the publishing is successful you can deploy, stage, and activate the software to all the appliances on the network from the **Network Configuration** page. For more information, see [Network Configuration](#). For a successful deployment, ensure that all the appliances are connected to SD-WAN Orchestrator for On-premises. For more details, see [Connectivity with Citrix SD-WAN appliances](#).

Software upgrade

You can upgrade your SD-WAN Orchestrator for On-premises software to the latest version.

NOTE

Download the appropriate SD-WAN Orchestrator for On-premises software package to your local computer. You can download this package from [Downloads](#) page.

Perform the following steps to upload and install a new version of the SD-WAN Orchestrator for On-premises software:

1. In the SD-WAN Orchestrator for On-premises UI, navigate to **Infrastructure > Orchestrator Administration > Software Images > Orchestrator**.
2. Click inside the box and select the ctx-onprem-1 (latest date).tar.gz binary file that you have downloaded and saved on your local system.

The screenshot shows the 'Orchestrator' tab in the SD-WAN Orchestrator for On-premises GUI. At the top, it says 'Current Software Version : R1_18_11_71_888886'. Below this is a dashed box for file selection with the text 'Click here to select the file or drag and drop the selected file. Allowed file type is .gz'. There is an 'Upload' button. Below the upload area, it says 'Uploaded File Name : none'. At the bottom, there is a yellow warning bar that says 'While upload is in progress, please do not navigate away from this page. Doing so will cancel the software upload.' and an 'Install' button.

3. Click **Upload** to upload the selected software package to the current SD-WAN Orchestrator for On-premises virtual machine.
4. After the upload completes, click **Install**.
5. When prompted to confirm, click **Install**.

Management settings

Management IP and DNS

After SD-WAN Orchestrator for On-premises Virtual Machine (VM) is deployed and a management IP is configured either manually or through DHCP, you can change the **Management IP and DNS** settings through SD-WAN Orchestrator for On-premises GUI. SD-WAN Orchestrator for On-premises stack takes about 3 minutes to restart. Once the management IP address is changed the SSH connections get re-established.

To configure/change the management IP and DNS settings, at the network level, navigate to **Infrastructure > Orchestrator Administration > Management Settings > Management IP & DNS**.

Provide the following details:

- **IP Address:** The IP address for SD-WAN Orchestrator for On-premises VM.
- **Gateway IP Address:** The Gateway IP address that SD-WAN Orchestrator for On-premises use to communicate with external networks.
- **Subnet Mask:** The subnet mask to define the network in which SD-WAN Orchestrator for On-premises is available.
- **Primary DNS:** The IP address of the primary DNS server to which all DNS requests from SD-WAN Orchestrator for On-premises are forwarded to.
- **Secondary DNS:** The IP address of the secondary DNS server to resolve DNS requests if the primary DNS server is not available.

Management Interface IP

IP Address *

Subnet Mask *

Gateway IP Address *

Save

DNS Settings

Primary DNS *

Secondary DNS

Save

NTP settings

You can either set the date and time manually, or use a Network Time Protocol (NTP) server to synchronize the clock time of SD-WAN Orchestrator for On-premises with Coordinated Universal Time (UTC).

To configure NTP server, at the network level, navigate to **Infrastructure > Orchestrator Administration > Management Settings > NTP** and enable **Use NTP server**.

Provide the NTP server IP address or domain name. You can provide up to four NTP servers, but ensure that at least one is configured. If one NTP server is down, SD-WAN Orchestrator for On-premises automatically synchronizes with the other NTP server. If you specify a domain name for an NTP server, ensure that the external DNS server is configured to point the domain name to the IP address.

NTP settings

☒ Use NTP server

NTP server 1

NTP server 2

NTP server 3

NTP server 4

To configure date and time manually, disable the **Use NTP server** option and manually select the date and time.

Date/Time settings

Date

Time

Select the time zone based on your country/city.

NOTE

Reboot the Orchestrator VM after changing the time zone. Some logs continue to use the previous time zone, until the reboot is done. For instructions, see [Reboot Orchestrator VM](#).

Timezone settings

After changing the timezone setting, a reboot will be necessary for the timezone changes to take full effect.

Until then, some logs will continue to use the actual timezone setting in effect at the time of the last reboot, even though events timestamps may reflect the new setting.

Timezone

US/Michigan

Save

Remote Authentication Servers

You can configure RADIUS or TACACS+ servers for the users who are authenticated remotely. To use remote authentication, you must specify and configure at least one authentication server.

NOTE

Ensure that the required user accounts are created on the RADIUS or TACACS+ authentication server.

Remote Authentication Servers

+ New

Name	IP Address	Port	Type	Actions
radiusServer1	10. .99	1812	RADIUS	
tacacsServer1	10. .98	49	TACACSPLUS	
myTacacs	1.2.3.4	1812	RADIUS	

Page Size: 200 Showing 1 - 3 of 3 items Page 1 of 1

Test Remote Server Connection

Username *

Password *

Remote Authentication Server *
10. .99 (RADIUS)

Verify

To configure remote authentication, navigate to **Infrastructure > Orchestrator Administration > Management Settings > Remote Auth Servers**. Click **+ New**. Enter the following details:

- **Enable:** Enables remote authentication server configuration.
- **Server Name:** The name of the remote authentication server.
- **Server Type:** The type of remote authentication server - RADIUS or TACACS+.
- **IP Address:** The host IP address for the remote authentication server.
- **Port:** The port number for the remote authentication server. The default port for the RADIUS server is 1812 and the TACACS+ server is 49.
- **Server Key** and **Confirm Server Key:** A secret key to use when connecting to the remote authentication server.
- **Authentication Type:** (available only for TACACS+ server) Select the encryption method to use to send the user name and password to the TACACS+ server.
 - **PAP:** Uses Password Authentication Protocol (PAP) to strengthen user authentication by assigning a strong shared secret to the TACACS+ server.

- **ASCII:** Uses the ASCII character set to strengthen user authentication by assigning a strong shared secret to the TACACS+ server.
- **Timeout:** The time interval (in seconds) to wait for an authentication response from the remote authentication server.

Add Authentication Server

☒ Enable

Server Name *

radius-server-1

Server Type

RADIUS

IP Address *

10 30

Port *

1812

Server Key

....

Confirm Server Key

....

Timeout

20

Add

Cancel

You can also test the remote server connection. Under **Test Remote Server Connection**, provide your **Username** and **Password**. Select the remote authentication server and click **Verify**.

Database management

You can create backup of the current database running on SD-WAN Orchestrator for On-premises and later use the backed-up file to restore the same database state.

To create database backup, navigate to **Infrastructure > Orchestrator Administration > Database Management**. Click **Backup**.

Click download under the **Actions** column to download the backed-up database.

Click **Upload** to browse and upload the downloaded file. You can also drag the downloaded file and drop it on the screen.

To restore, click **Restore** under the **Actions** column.

NOTE

- You can save only one database backup at a time. To replace an existing backup with the latest, delete the existing backup and click **Backup**.
- Restore of the database must be done to the same release of Citrix SD-WAN Orchestrator

on-premises from where the data backup was taken.

- The database backup only takes the backup of configuration and statistics. It does not back up the platform related data.

Only one backup can exist on the system at a time.

While upload is in progress, please do not navigate away from this page. Doing so will cancel the upload.

Backup

Created At	Status	Actions
Mon, 23 Nov 2020 06:10:19 GMT	Available	

Page Size: 200 Showing 1 - 1 of 1 items Page 1 of 1

Successful Upload of the database backup will immediately restore the backup.

Click here to select the file or drag and drop the selected file.
Allowed file type is .gz

Upload

Orchestrator diagnostics

January 11, 2021

This section provides information on the diagnostic activities that can be performed on SD-WAN Orchestrator for On-premises infrastructure.

Platform events and logs

Any change in platform level attributes, such as CPU, memory, or storage in the system is logged as an event and displayed on the SD-WAN Orchestrator for On-premises.

For example, if CPU usage exceeds the set limit, a platform event is logged and an alarm is triggered. The alarm comes up in the Notifications bar. The notification gets cleared if the CPU usage gets decreased. The **Platform Events & Logs** page maintains the history of all platform related alarms that were triggered. If the CPU usage decreases, the alarm status becomes INACTIVE. If it is still above the limits, the alarm status remains ACTIVE.

To view the platform events, navigate to **Infrastructure > Orchestrator Diagnostics > Platform Events & Logs**.

The following details are displayed for logged platform events:

- **Description:** The description of the platform event.
- **Alarm Status:** The status of the alarm. If the platform attribute exceeds the set limit, then the status is ACTIVE. If the platform level attribute subsides to a value within the set limit, then alarm status is INACTIVE.
- **Resource:** The platform level attribute – CPU, Memory, or Storage.
- **Current Value:** The latest value of the logged platform attribute.
- **Created At:** The time when the platform event occurred.

Description	Alarm Status	Resource	Current Value	Created At
UPPER THRESHOLD EXCEEDED	ACTIVE	Memory	70.1	Sun 22 November, 2020 at ...
UPPER WARNING THRESHOLD EX...	ACTIVE	CPU	51.4	Sun 22 November, 2020 at ...

Page Size: 200 Showing 1 - 2 of 2 items Page1 of1

Platform health

You can view the health of the SD-WAN Orchestrator for On-premises platform. The health information includes real-time values (in percentage) for CPU usage, Memory usage, and free storage available.

To view the platform health, navigate to **Infrastructure > Orchestrator Diagnostics > Platform Health**.

CPU Usage	1%
Memory Usage	74%
Free Storage	35%

Diagnostic info

A diagnostic package consists of System Log files, system information, and other necessary details that assist the Support team in diagnosing and resolving issues with your system.

To create a diagnostic package, navigate to **Infrastructure > Orchestrator Diagnostics > Diagnostic info**. Click **Create**. After the package is created, you can download it to your computer and then share it with the Support team.



NOTE

SD-WAN Orchestrator for On-premises can store a maximum of five diagnostic packages at a time.

These packages contain important real-time system information you can forward to Citrix Support Representatives.

Total five Diagnostic Packages can exist on the system at a time.

Diagnostic Packages *

Create

Restart SD-WAN Orchestrator for On-premises app

You can restart only the SD-WAN Orchestrator for On-premises app without rebooting the Operating System (OS). During restart, SD-WAN Orchestrator for On-premises app goes offline and the all services become unavailable. It takes approximately 6 minutes for the restart to complete. After the restart, SD-WAN Orchestrator for On-premises login page is displayed.

To restart SD-WAN Orchestrator for On-premises app, navigate to **Infrastructure > Orchestrator Diagnostics > Restart Orchestrator App**. Click **Restart** and **Yes, Restart** to confirm.

On-Prem Orchestrator status: UP 

Restart

Reboot SD-WAN Orchestrator for On-premises VM

The Reboot process restarts the Operating System (OS) of SD-WAN Orchestrator for On-premises. During the reboot, SD-WAN Orchestrator for On-premises goes offline and all services become unavailable. It takes approximately 6 to 8 minutes for the reboot to complete. After the reboot, SD-WAN Orchestrator for On-premises login page is displayed.

You can reboot SD-WAN Orchestrator for On-premises as part of a troubleshooting activity or during a maintenance activity.

To reboot, navigate to **Infrastructure > Orchestrator Diagnostics > Reboot Orchestrator VM**. Click **Reboot** and **Yes, Reboot** to confirm.

Network Infrastructure: Reboot Orchestrator VM

Reboot

**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2021 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).