net>scaler

Citrix SD-WAN Orchestrator

Contents

What's new	5
Known issues	13
Onboarding Citrix SD-WAN Orchestrator	16
Licensing	43
Provider level configuration	51
Network home	57
Configuration difference	65
Deployment	68
Inter-link communication	90
DNS and DHCP	92
Site and IP Groups	94
Application settings and groups	104
Profiles and Templates	122
ECMP load balancing	129
Notification settings	133
Network location service	139
Site configuration	140
Wi-Fi Access Point	178
LTE firmware upgrade	186
Address resolution protocol	190
Neighbor discovery protocol	190
Delivery Services	192
Prefix delegation groups	200

Appliance settings	201
In-band management	226
View configuration (Preview)	234
Office 365 optimization	238
Metering and Standby WAN Links	247
Zero touch deployment	253
IP rules	253
Application rules	260
Classes	266
Application classification	268
MPLS queues	274
QoS fairness (RED)	277
QoS policies	279
HDX QoE	283
Routing	297
Dynamic routing	314
SD-WAN Overlay Routing	325
Network address translation	337
Dynamic host configuration protocol	347
Multicast routing	350
Virtual router redundancy protocol	355
Domain Name System settings	360
Virtual Path Route Cost	363
Security	366

Edge security	390
Firewall settings	409
Configure firewall segmentation	411
Link aggregation groups	415
Certificate authentication	420
Inline mode	420
Virtual inline mode	428
Azure Virtual WAN	438
Citrix SD-WAN integration with Google Network Connectivity Center	459
SD-WAN configuration for Citrix Virtual Apps and Desktops Standard for Azure integration	460
Integration of Citrix SD-WAN Orchestrator with Check Point CloudGuard Connect	473
Deploy Citrix SD-WAN Standard Edition instance on Azure	485
Citrix Cloud and Gateway Service optimization	501
PE support: WAN optimization configuration	514
WAN optimization	527
WAN-Optimization settings	528
Provider dashboard	537
Customer/Network dashboard	538
Site dashboard	543
Provider Troubleshooting	546
Network Troubleshooting	549
Site troubleshooting	564
AppFlow and IPFIX	566
Adaptive bandwidth detection	577

Provider reports	578
Customer/Network reports	583
Site reports	634
Diagnostics	675
User settings	677
Role settings	681
IP access list	688
Announcements	689
API guide for Citrix SD-WAN Orchestrator	691
Best practices	695
Routing	696
QoS	696
WAN Links	697
FAQs	698

What's new

October 17, 2022

September 29, 2022

Fixes

- **SDW-23725**: Citrix SD-WAN Orchestrator service failed to process the virtual path route records that did not have a static virtual path to the site.
- **SDWANHELP-2769**: The Rollback banner on the **Change Management Settings** page was not cleared after the SD-WAN appliance was up and auto corrected to the correct version.

September 15, 2022

Configuration

HTTP server configuration

Citrix SD-WAN Orchestrator service now supports Certificate-based authentication for HTTPS push notifications to the server URL. Ensure to upload the client certificate in PEM format and the secret key in PKCS8 format.

[SDW-23898]

Fixes

• **SDW-24143**: On the site level **Configuration**> **Appliance Settings** > **SNMP** page, users were unable to update multiple destination IP addresses as a semi-colon separated list.

August 23, 2022

Miscellaneous

Citrix SD-WAN 11.5 release

Citrix SD-WAN 11.5 release is supported in Citrix SD-WAN Orchestrator service. SD-WAN 11.5.0 release is available only via Citrix SD-WAN Orchestrator service and only on selected geographical POPs. Ensure to get the required approvals and guidance from Citrix Product Management / Citrix Support before deploying 11.5.0 on any production network.

[SDW-24022]

June 30, 2022

Miscellaneous

WAN link template enhancements

When you modify a WAN link template, you now have an option copy the modified WAN link template configuration settings to the site WAN link configuration that is created using the WAN link template.

The following fields are introduced in the **WAN Link Info** section of the WAN link template page:

- Adaptive Bandwidth Detection
- Minimum acceptable bandwidth (%)

The following fields are introduced in the **Metering** section of the WAN link template page:

- Data Cap(MB)
- Disable Link If Data Cap Reached
- Approximate Data Already Used (MB)

The Eligibility field has been introduced in the **MPLS Queues** section of the **Configuration** > **Site Configuration** > **WAN Links** page.

On the **Site configuration** > **WAN links** page, the **Template Name** field is introduced. This field is displayed when a new WAN link is created using a template.

[SDW-23741]

Ethernet interface settings

Citrix SD-WAN Orchestrator service introduces the Ethernet interface settings section on the **Site Configuration** > **Appliance Settings** page of the UI. This section provides information such as connectivity status of the ethernet ports, Interface type, MAC address, auto negotiate, and the duplex setting status.

[SDW-23730]

Fixes

• **SDWANHELP-2706** - Citrix SD-WAN Orchestrator service fails to auto-correct the firmware mismatch when the SD-WAN appliance is factory reset more than once.

June 02, 2022

Fixes

- **SDW-23687**: LTE firmware upload and validation of the uploaded firmware fails intermittently on Citrix SD-WAN Orchestrator service.
- **SDW-23768**: The Citrix SD-WAN Orchestrator service UI allows more than one WAN link to be set as primary WAN link for Intranet services.
- **SDW-23827**: The audit error EC 100 is displayed for sites that do not have the serial number registered and site names that contain more than 25 characters.

May 05, 2022

Dynamic source NAT

The Citrix SD-WAN Orchestrator service UI now displays the auto-created IPv4 outbound Internet dynamic source NAT rules when the following conditions are fulfilled:

- Internet service is enabled on the site.
- IPv4 outbound Internet dynamic source NAT rule is not configured at the site.
- At least 1 WAN link is on an untrusted interface or Internet is enabled on all routing domains.

[SDW-23553]

Minimum and Maximum value in Kbps for WAN link settings: Citrix SD-WAN Orchestrator service allows you to set minimum and maximum upload bandwidth values in Kbps for LAN to WAN as well as WAN to LAN while configuring a WAN link. The minimum/maximum kbps fields are added under the **Configuration> Site Configuration > WAN Links tab > Services** section at the site level. You must provide the value (mandatory to add the minimum value) while adding any new services or editing any existing services.

You can also set the minimum/maximum upload and download bandwidth value for Internet and Intranet services. The same fields are also added under **Configuration>Advanced Settings > Delivery Services > Internet/Intranet Services** at the site level.

[SDW-23408]

Provider-No-Access Role: With the No access role feature, initially a provider administrator can avoid giving the full access role to a newly added user. When the user with a no-access role clicked the Citrix SD-WAN Orchestrator service, the UI gets stuck on loading. The administrator can later decide whether to restrict giving access to the newly added user or add them to a specific tenant.

[SDW-22585]

Deployment enhancements

The **Deployment** home page is enhanced with a new look and feel for a better user experience. The following changes are effective on the new **Deployment** page:

- **Deployment summary:** This section provides a summary of the most recent deployment with such as the date and time (in UTC time zone), and the status of the deployment.
- Switch to Old Deployment View: An option to go back to the old Deployment page is available.
- **Deployment history**: The new **Deployment history** table provides details of the past deployment. If Partial Site Upgrade is enabled, the deployment history table categorizes the details based on the software version that the appliances are configured to run. If the last activation fails, you can even view details of the failure.
- **Site View**: This table includes details about the current deployment status, Orchestrator connectivity, the software version of each appliance, and a timestamp of the running configuration. It also includes options to retry the deployment on individual sites in case of failures.
- **Default network software:** The option to select the software version to be applied to the sites across the network is now available under **Deploy Now** > **Software & Sites**.
- Partial site upgrade: The partial site upgrade option is now available under Deploy Now > Software & Sites.
- Ignore Incomplete: This check box is now available under Deploy Now > Settings.
- Rollback Settings: The Rollback on error option is renamed as Rollback Settings. It is now available under Deploy Now > Settings.
- The 4 main stages of the deployment process are captured in the following screens:
 - Software & Sites
 - Configuration
 - Settings
 - Summary

[SDW-16829]

Site template

Citrix SD-WAN Orchestrator service introduces the option of using a Site template to configure a site. The Site template can be created from **Configuration** > **Profiles & Templates** > **Templates** and a new site can be created using this Site template from **Configuration** > **Network Home.**

You can also clone a branch site in addition to site template. However, if some additional features require any modifications, verify the configuration details after cloning the site or the site template and make the changes as required.

[SDW-14694]

Mobile broadband settings - Manage firmware

Citrix SD-WAN Orchestrator service provides an option to upload a firmware and apply it as part of the mobile broadband configuration. Currently, the firmware can be applied only on SD-WAN SE 210 LTE appliances.

[SDW-23588]

Fixes

- SDWANHELP-2657 Unable to invite a user as there is an interim issue with Citrix Cloud server.
- SDW-23322 The service state of an SD-WAN appliance running a software version of 11.4.2 is displayed as BAD on the Citrix SD-WAN Orchestrator service for On-premises UI. The error message displayed is No Response from Orchestrator URL. This issue occurs when a custom domain is configured in Citrix SD-WAN Orchestrator service.

March 31, 2022

Record device mismatch

Citrix SD-WAN Orchestrator service notifies users when a mismatch is identified between the platform model reported by the appliance and platform model that the users provide while configuring a site. The mismatch details of the platform model and submodel are displayed on the UI in a tabular format.

[SDW-23346]

Platform and systems

Management IP / In-band IP enhancements

The **Management IP** and the **Device Access** columns on the following UI screens are enhanced to display either the in-band IP address or the management IP address based on the type of IP address that the device is using to communicate with Citrix SD-WAN Orchestrator service:

- Provider > Reporting > Inventory > Details
- Customer > Configuration > Network Home > Actions > View Details
- Customer > Security > Hosted Firewall > VM administration
- Customer > Reporting > Inventory > Deployed
- Site > Dashboard > Devices

[SDW-23353]

Mobile broadband settings and Mobile broadband status

You can now connect the Citrix SD-WAN appliance from your site to a network using a broadband Internet connection. This mobile broadband status and configuration support is available for Internal modems. You can also view the status of the broadband configuration of your device and the active SIM.

[SDW-10907]

Fixes

- **SDWANHELP-2619**: In the case of multi-MCN MSP, the audit log for deleting a tenant is missing. With the fix, when user deletes a tenant from the MSP an audit log entry is created.
- **SDWANHELP-2570**: Citrix SD-WAN Orchestrator service UI reflects the actual value of MTU 1350 in Wan links.
- **SDW-23477**: Citrix SD-WAN Orchestrator service sends TCP synchronization packets to the AWS endpoint.

March 03, 2022

Citrix SD-WAN 11.4.3 release is supported in Citrix SD-WAN Orchestrator service.

[SDW-23359]

IP access list

Citrix SD-WAN Orchestrator service allows administrators to configure user IP addresses at a network level. This feature is useful when administrators want to allow the tenant access to users based on the IP address, thereby enhancing IP security. This feature is supported for users that have specific roles assigned as part of a tenant.

The **IP Access List** page is introduced in Citrix SD-WAN Orchestrator service to enable administrators to configure user IP addresses.

[SDW-21393]

Site summary table

A new **Device Status** column has been added at the network home sites summary table.

[SDW-23401]

Fixes

- **SDWANHELP-2609**: Earlier, the user was not able to change the alternate port values after initially configuring it.
- **SDWANHELP-2482**: HA failover was triggered when activation on active and standby appliances did not happen within the predefined freeze time. To avoid unnecessary failovers, the freeze time for failover during Change Management on Citrix SD-WAN 110 appliances has been increased by 10 seconds.
- **SDW-23322**: The service state of an SD-WAN appliance running a software version of 11.4.2 is displayed as *BAD* on the Citrix SD-WAN Orchestrator service UI. The error message displayed is *No Response from Orchestrator URL*. This issue occurs when a custom domain is configured in Citrix SD-WAN Orchestrator service.
- **SDW-23399**: A missing value of 1500 bandwidth for VPX and VPXL has been added.
- **SDW-23310**: To set Access Interface and gateway IPs at WAN links, you have to change the Virtual Interface from the drop-down list > select another Virtual Interface > then back to the original.

January 27, 2022

Restore previous version

Citrix SD-WAN Orchestrator service introduces the Restore previous version functionality. When the **Restore previous version** option is selected, Citrix SD-WAN Orchestrator service initiates a network-wide activation of the previous configuration and restores the previously activated configuration(and/or software) on your network.

[SDW-22042]

QoS Policies

The QoS policies page is revamped to enhance the user experience. The options such as Custom Application Rules, Application Rules, HDX Rules, Application Group Rules, IP Rules, and Default IP-Protocol Rules are enhanced with a new look and feel.

[SDW-11029]

IP Rules

The Override Service option is added under **IP Rules > Virtual Path Traffic Policy** section. When the **Traffic Policy** is selected as **Override Service**, you can select the service type as Intranet, Internet, pass-through, or Discard to which the virtual path service overrides.

[SDW-22213]

Configuration Difference

A **Config Diff** feature is newly added at the Network level under **Configuration**. The **Config Diff** capability helps you to review the difference between any two versions of configuration checkpoints. You can also have the ability to view the configurations both at the global and site levels.

[SDW-4563]

Appliance settings

Citrix SD-WAN Orchestrator service introduces an option to configure the management network priority. You can select **In-Band** or Out-of-Band as the management interface for your network. This option is available only if the SD-WAN appliance is running a software version of 11.4.2 or later.

[NSSDW-35774]

CSV Export Report

With the **Export as CSV** capability, you can download the path graph points (virtual/member path) for any time series (hourly, weekly, and so on) as an excel Comma-separated Value (CSV) file and can plot all distinct points of data for a particular site report.

[SDW-20988]

Certificate authentication

Citrix SD-WAN Orchestrator service supports appliance authentication for static and dynamic virtual paths using Public Key Infrastructure (PKI) as an additional security feature. Enabling the feature extends the existing virtual path authentication mechanism by distributing PKI certificates over the data path, by the appliance initiating the exchange. The PKI enhancement also supports Certificate Revocation List (CRL) management for centralized revocation of compromised certificates.

[SDW-19295]

View Configuration (Preview)

Citrix SD-WAN Orchestrator service introduces the **View Configuration** page at the site level. This page provides a detailed summary of a site's configuration across multiple subsystems.

[SDW-22284]

Real-time statistics

The **Firewall Connection** is now renamed to **Firewall Statistics**. NAT and Filter Policies are newly added under the statistics type drop-down list. Also, the Real-time statistic options are restructured and divided into the following categories:

- Network statistics
- Application statistics
- Route statistics

[SDW-20966]

Fixes

- **SDW-22977**: When a serial number is added to an existing site configuration that is deployed without a serial number, the appliance gets activated with the previously staged configuration.
- SDWANHELP-2536: User was not able to update cc/bcc emails at Network level > Alerts > Notification settings > Notification profile tab.
- **SDW-10178**: On adding more than 9 subinterfaces, the diagram for the LAN segment is not clear.
- **NSSDW-37813**: In Citrix SD-WAN 11.4.2 release, uploading a signed CSR certificate from Citrix SD-WAN Orchestrator service fails for files with .der extension.

Known issues

September 28, 2022

Sep 29, 2022

Citrix SD-WAN Orchestrator service has the following known issues:

Platform and systems

In the Citrix SD-WAN 210 appliance, if you remove the Standard Edition (SE) add-on license, the services get disabled.

Workaround: Before removing the SE add-on license (or) moving from AE to SE license, remove the firewall policies that have the security profile, configure the appliance as out-of-band management (If In-band management is configured) and then proceed with the stage and activation process to convert the appliance to standard edition.

[SDW-18031]

License

When the pooled license's low bandwidth quota is over, the device does not consume any licenses and remains in grace license mode.

Workaround: Add more licenses into pooled licenses and then change the bandwidth in the site configuration to trigger allocation of the pooled licenses. Or, you can change the bandwidth to a higher bandwidth in the site configuration if it is available in pooled licenses.

[SDW-22730]

Currently, there is no indication to the user that the device remains in grace license mode when there are no more licenses to be allocated from pooled licenses while saving the device serial number.

Workaround: Add more licenses into the pooled license and then change the bandwidth in the site configuration to trigger allocation of the pooled licenses.

[SDW-22709, SDW-15001]

Customer with a Secure Internet Access (SIA) entitlement while onboarding to Citrix SD-WAN Orchestrator service, is being onboarded to a different PoP. Whereas the other way, with the customer having SD-WAN entitlement and onboarding to SIA works fine.

[SDW-22672]

Appliance configuration activation fails when the appliance device model is set to Advanced Edition (AE).

[SDW-19067, SDW-15001]

Platform and systems

The GUI of one of the Citrix SD-WAN appliances is not accessible because the network statistics provider is reusing a session and this caused the HTTPD process to behave improperly (in rare cases).

[SDW-23392]

Configuration and Management

On the **Realtime VRRP Site reports** page of the Citrix SD-WAN Orchestrator service UI, the **Enable** and **Disable** operations are not working.

[SDW-24066]

The Applications and Application categories graphs are empty on the **Reports** > **Usage** > **Applications** page of the Citrix SD-WAN Orchestrator service UI.

[SDW-23817]

A mismatch is observed between the agent and appliance scripts while fetching IGMP statistics.

[SDW-23757]

The **Restore previous version** operation fails with the **Activation Failed(ER101)** error message for the sites in PSU when the partial site upgrade list is modified and a change management (stage and activate) is performed on a network.

• **Workaround**: Perform another round of change management before applying the restore previous version action.

[SDW-23227]

Customer is not able to send push notification to their own HTTP Server.

[SDW-23134]

If a site is added to the configuration before performing staging and activation, enabling HA on the site post activation with a new serial number for the secondary appliance triggers auto-deployment of the newly added appliance. The staging fails with the error **Staging Failed (Failed to download script files)**.

Workaround: After enabling HA, do a full network stage and activate to deploy the HA appliance.

[SDW-22567]

The **WAN-OP Settings** > **SSL Profiles** > **Add** section of the UI fails to display the list of newly created WAN optimization rules in the **Service classes** drop-down list.

Workaround: Create an SSL profile without specifying service classes, and then edit the same profile. The list of WAN optimization rules is displayed.

[SDW-21734]

A change in the SSL inspection root Certificate Authority (CA) and the key will not be propagated to the SD-WAN appliance, unless another edge security-related setting is also changed. This results in the SSL inspection being performed with the previous root CA.

Workaround: Change another setting related to edge security, then stage and activate it. This triggers the download and application of the root CA and key.

[SDW-16050]

The static virtual paths that are formed between a transit node and the branch sites are not getting deleted when the transit node configuration is removed.

Workaround: Delete the static virtual paths manually when the transit node configuration is removed.

[SDW-16045]

Scheduling Information of the appliance in **Change Management Settings** might display outdated data, when the appliance reconnects to the Citrix SD-WAN Orchestrator service after a factory reset.

Workaround: In the **Change Management** settings, select the desired scheduled window and apply it. The appliance is updated and the data between the appliance and the Citrix SD-WAN Orchestrator service is synchronized.

[SDW-15169]

Creating the transit nodes for the branches does not form virtual paths.

Workaround: Create the static virtual paths manually between the transit site and the branch nodes.

[SDW-10104]

Onboarding Citrix SD-WAN Orchestrator

April 29, 2022

Here is an overview of the Citrix SD-WAN Orchestrator service onboarding process:

- Onboarding provider and tenants: Our customers can consume a managed SD-WAN service from Citrix partners, enabled by the multitenant Citrix SD-WAN Orchestrator service
- Onboarding "Do It Yourself" (DIY) Enterprises: Citrix SD-WAN Orchestrator service is also available as a self-managed service for enterprises.

Onboarding provider and tenants

This section describes the onboarding process for Citrix partners and their tenants. Here is a summary of the onboarding process:

- 1. A prospective partner sign-up as a Citrix Partner.
- 2. Citrix Partner registers as a Citrix SD-WAN Reseller.
- 3. Partner on boards Customers using one of the following two options:
 - Partner adds a customer who is new to Citrix Cloud.
 - Partner invites an existing Citrix Cloud customer.
- 4. Partner and customers can now access their Citrix SD-WAN Orchestrator service accounts.

Partner signs up for a Citrix partnership program

A prospective partner would need to sign up for the Citrix Service Provider Program (CSP) - CSP signup.

A partner can also sign up for the Citrix SD-WAN Managed Service Provider Program, which has been specially crafted for Citrix SD-WAN partners - SD-WAN MSP Sign Up.

Citrix SD-WAN Orchestrator

\leftrightarrow \rightarrow C \triangleq citrix.c	com/en-in/partner-programs/managed-service-provider.html	* 0 :
citrix r	Products Downloads Support Partners	Q Contact us ∨ EN ∨ &
Partner	with Citrix	1 800 102 2489 Become a Partner
Overview	Partner Programs ^ Partner Insig	yhts
	Solution Advisor	
	Service Provider	
Dali	Citrix SD-WAN Managed Service Provider	ol of
Dell	System Integrator	
busi	Independent Software Vendor	and
aon	Citrix Ready Partner	with SD
gen	Distributor	; with SD-
1AW	Authorized Learning Center)
As enterprises cloud, new bra	with geographically dispersed locations co nch locations are just outside the traditiona	ntinue to migrate applications to the leased-line service footprints.

A Citrix Cloud (CC) account is created for the partner as part of the registration process. For more information, see Signing Up for Citrix Cloud.

Partner registers as a Citrix SD-WAN reseller

Partner logs into the Citrix Cloud account.

Citrix Cloud™	Enter your Citrix credentials. (Citrix.com, My Citrix, or Citrix Cloud)
Move Faster, Work Better, Lower IT Costs	aridexi.kngc/trix.com
A single place to simplify delivery of Citrix technologies. Provide secure access to apps, data and IT tools. Deploy on	
any cloud or infrastructure.	Sign In
	Remember me
	Forgot username? Forgot password?
	Contact Support
Don't have an account? Sign up and try it free	Sign in with my company credentials
English (US)	

A menu of all the available services offered on Citrix Cloud is displayed on the home page. The **Citrix SD-WAN Orchestrator service** tile can be found in the **Available Services** section. The partner clicks



Resell SD-WAN on the tile to register themselves as a Citrix SD-WAN reseller or service provider.

Partner can now access the Citrix SD-WAN Orchestrator service. The **Citrix SD-WAN Orchestrator service** tile now shows up under **My Services**. Click **Manage** to access the Citrix SD-WAN Orchestrator service Provider Dashboard.

My Services (1)	Ó ♪ O Open Tickets Open a Ticket
SD-WAN Orchestrator Centralized cloud management service for SD-WAN	
Manage How to Resell Learn more	

At this point, there are no SD-WAN customers. The partner navigates back to the Citrix Cloud home page to onboard customers.

PROVIDE	customer custom			£ ()
Ø	Provider Dashboard			
ណ៍		Search	Q. Total C	0 0 0 0 0 Dustomers Critical Warning Normal Inactive
Ô				
Z				
L				
>				

Partner on-boards customers using one of the following two options:

- Add a customer who is new to Citrix Cloud.
- Invite a customer who already has a Citrix Cloud account

Partner adds a customer who is new to Citrix Cloud

1. On the Citrix Cloud home page, click **View Details** under the **Customers** icon or click **My Customers** from the hamburger menu.

	L O Customers View Details	Library Offerings	Resource Location Edit or Add New	Domains	Dotifications	Open Tickets Open a Ticket	
Home My Customers My Services Library Licensing	- ts	Library Offerings View Library	Resource Location	Domains	Dotifications	Open Tickets	
Identity and Access Manag Resource Locations Support Tickets Notifications	gement						
Mana How to Resell.	ige Learn more						

- 2. Click Invite or Add.
 - ← Customer Dashboard



3. Select Add a customer and click Continue.

Invite or a	dd customer	×
\bigcirc	Invite a Citrix Cloud customer Customer already exists in Citrix Cloud.	\bigcirc
R	Add a customer Create a new customer in Citrix Cloud.	
	Cancel Continue	

4. Enter the admin and customer details and click **Finish**.

← Add a customer

To add a customer, complete these steps below.

dmin Details		
First Name	Last Name	
Business Email Addre	255	
usiness Details		
Company Name		
Phone Number		
Address		
City	USA	~
AA	✓ Zip or Postal Code	

Note

The company name and email-id used must be associated with only one Citrix Cloud account.

The added customers are visible in the **Customer Dashboard**.

Customer Dashboard

Customer	Trials	Production	Notifications	Open Tickets	
Acres Married	2	5	2	1	••• >
Annual Partner Geoldese	3	2			*** >

5. Partner links their SD-WAN account with the customer SD-WAN account

In the partner's **Customer Dashboard**, the partner selects the customer and clicks **Link Customer's SD-WAN Account**.

~ I	Customer	Dashboard	
-----	----------	-----------	--

Invite or Add		Searc	h by customer name	Q < 1-1 of 1 >
Customer Name 1	Trials	Production	Notifications	Open Tickets
SDWANCustomer1				···· >
		< 1-1 of	1 >	View Details Link Customer's SD-WAN Account View Licensing Manage Offerings Manage Domains Remove Customer Connection

6. Partner requests for Citrix SD-WAN Orchestrator service trial on behalf of the customer.

In the Citrix Cloud dashboard, the partner selects the **Change Customer** option and selects the appropriate customer.

					÷ 0	~.
L 2 Customers View Details	Library Offerings	Resource Location Edit or Add New	Domains	D Notifications	Open Ticke	Account Settings Change Customer
						Sign Out
hestrator gement service for .N						English (US)



The partner navigates to the customer's Citrix Cloud home page, and clicks the Citrix SD-WAN Orchestrator service **Request Trial** button.



The customer's Citrix SD-WAN Orchestrator service account gets provisioned.



The partner can now manage the customer's Citrix SD-WAN Orchestrator service account after switching back to their account using **Change customer** option again.

Partner's dashboard on the Citrix SD-WAN Orchestrator service now reflects the new customers added. Partner can click the customer tile to drill down into the customer's network and manage it.

PROVIDER Citrix Systems Inc Internal Enter	rprise / All Customers V		Change Role 📿 🕐
C dashboard	Provider Dashboard		STILE VIEW
REPORTS >		Search Q	184 Total Customers Critical Warring Normal Inactive
CONFIGURATION >	iغ الم		(点) たいののが シトリックス・シーフィックス・システムス・シーフ クス・システムス・シーフ ・バン用式目的。
\sim troubleshooting >	O O O O O O Critical Alerts	0 0	
$\underline{\Omega}$ administration >		Total Sites Sites Down Critical Alerts	Total Sites Sites Down Critical Alerts
	minash-23705- mi360bbbe	INT4T-	
	O O O Critical Alerts	O O O Total Sites Sites Down Critical Alerts	O O O Critical Alerts
<			

Partner invites an existing Citrix Cloud customer

1. On the Citrix Cloud home page, click **View Details** under the **Customers** icon or click **My Customers** from the hamburger menu.



Home My Customers My Services Library Licensing	~ Is	Library Offerings View Library	도 1 Resource Location Edit or Add New	Domains	ONOTIFICATIONS	Open Tickets	
Identity and Access Managerr Resource Locations Support Tickets Notifications	ient						
Manage How to Resell Lea	n more						

- 2. Click Invite or Add.
 - ← Customer Dashboard

Tent	
It is looking lonely in here Click the Invite Customer button to start making connections.	
Invite or Add	

3. Select Invite a Citrix Cloud customer and click Continue.

\bigcirc	Invite a Citrix Cloud customer Customer already exists in Citrix Cloud.	
	Add a customer Create a new customer in Citrix Cloud.	\bigcirc

4. Copy the link and share it with the customer.



5. The customer clicks the link received and is redirected to the Citrix Cloud login page.



6. Customer logs in and accepts the partner's request to manage their Citrix Cloud account and services.

×	
Citrix Cloud	
would like to learn how you are using Citrix Cloud and help you with your business.	
Read about what type of account information the partner will see. If you approve this request, click the customers you want to allow partner access, and click Accept to continue.	
Decline All Accept	

The partnership between the partner and the customer is established.

	× Great! You have a new partnership with	
	Partner will have access to <u>1 Accounts</u> Manage partner connections from your account settings.	
_		

The customer details show up in the partner's customer dashboard.

≡	citrix				• 0	.~		
4	Customer Dashboa	rd			My Account My Customers			
	Invite or Add			Search by customer name	SDWAN-Customer-I has accepted your invitation to connect.	3 of 3 >		
	Customer Name 1	Trials	Production	Notifications	Open Tickets			
	SDWAN-Customer-1					>		
	REMINCULTURAL C					>		
	Memory	1				•••• >		
			<	1-3 of 3 >				

7. Partner links their SD-WAN account with the customer SD-WAN account

In the partner's **Customer Dashboard**, the partner selects the customer and clicks **Link Customer's SD-WAN Account**.

← Customer Dashboard

Invite or Add		Sear	ch by customer name	Q < 1-1 of 1 >
Customer Name 1	Trials	Production	Notifications	Open Tickets
SDWANCustomer1				>
		< 1-1 o	f1 >	View Details Link Customer's SD-WAN Account View Licensing
				Manage Offerings Manage Domains
				Remove Customer Connection

8. Customer requests for Citrix SD-WAN Orchestrator service trial

Once the partner links the Customer's Citrix SD-WAN Orchestrator service account to their own, the partner or the customer navigates to the customer's Citrix Cloud home page, and clicks the Citrix SD-WAN Orchestrator service **Request Trial** button.



The customer's Citrix SD-WAN Orchestrator service account gets provisioned. The partner can now manage the customer's Citrix SD-WAN Orchestrator service account from within their own account.



The Citrix SD-WAN Orchestrator service option is displayed in the customer's list of the Citrix Cloud services. Clicking it redirects the admin to the customer's Citrix SD-WAN Orchestrator service account.

Partner's dashboard on the Citrix SD-WAN Orchestrator service now reflects the new customers added. Partner can click the customer tile to drill down into the customer's network and manage it.

Citrix SD-WAN Orchestrator

PROVIDER Citrix Systems Inc Internal Enter	prise / All Customers ~		Change Role
C dashboard	Provider Dashboard		
REPORTS >		Search Q	184 0 0 0 184 Total Customers Critical Warning Normal Inactive
CONFIGURATION >	<u>向</u>		
$<\!$	O O O O O O O O O O O O O O O O O O O		
Administration >		Total Sites Sites Down Critical Alerts	Total Sites Sites Down Critical Alerts
	in provide 23750-	Ci 111447-	œ
	O O O O Critical Alerts	O O O O O O O O O O O O O O O O O O O	O O O Critical Alerts
<			

Note

Customers can also choose to add multiple administrators from partner organizations to manage their Citrix SD-WAN Orchestrator service account. For more information, see Add administrators to a Citrix Cloud account

Customer accesses Citrix SD-WAN Orchestrator service

At this point, the **Citrix SD-WAN Orchestrator service** tile also shows up on the customer's Citrix Cloud home page, under **My Services**, click **Manage**.



The customer can now access their Citrix SD-WAN Orchestrator service Network Dashboard. That completes the onboarding process.

Citrix SD-WAN Orchestrator

PROVIDER Citrix Systems IncInternal Enter	CUSTOMER V SITE V Change Rold (C) (Change Rold (C)
🖗 DASHBOARD	Relative Time Interval: Last 1 Hour Site Group: All Y
REPORTS >	Image: Contraction of the see All Image: Contraction of the see All Image: Contraction of the see All Image: Contraction of the see All Image: Contraction of the see All Image: Contraction of the see All
CONFIGURATION >	OverlayUnderlayisakmpUnclasmozillapod5_6100Critical77.8%25.01 MB12.45 MB2.82 MB0 %
() ALERTS >	+ New Site List Select Continent V Select Country V Search Q 10 2 1 7 Total Sites Critical Verming Verming Normal
\ll troubleshooting >	Map Satellite Clustering OFF -
$\underline{\Omega}$ administration >	C Read Sector
	Canada United Canada United Canada United Canada United Un
	North Paolfic Ocean View View View View View View View View

Multi-MCN providers and tenants

A multi-MCN partner network is a network in which each provider network can have multiple MCN sites. If you are a partner or a tenant, and you want to be onboarded as multi-MCN partner, you need to contact your administrator.

A multi-MCN partner can add a tenant directly through Citrix SD-WAN Orchestrator service. While adding the tenant, the partner needs to configure a domain name for each tenant. If the domain name is not configured, any user onboarded through Citrix Cloud (**Identity and Access Management** > **Administration**) is added as a provider-level admin.

The domain name is unique across tenants under that provider. A multi-MCN partner can configure only one domain for each tenant. For example, if Tenant1 is configured with @domain1, no other tenants can have @domain1 configured.

If a multi-MCN network partner grants full access to the tenants while adding them on Citrix SD-WAN Orchestrator service, then the tenant admin can add or remove users through Citrix Cloud (**Identity and Access Management** > **Administration**). If full access is not granted, the tenant admin cannot add or remove other users.

The multi-MCN partner must maintain a mapping of all the tenant names against their domain names. When a multi-MCN partner admin adds a user for a tenant, through Citrix Cloud (**Identity and Access Management** > **Administration**), Citrix SD-WAN Orchestrator service identifies the domain name from the user's email address and adds the user under that tenant.

Note

Domain name mapping is available only for multi-MCN network partners. It is not available for regular partners.
Citrix SD-WAN Orchestrator

enant Details	Tenant Contact Info
company Name* Citrix Cloud ID	Contact Name
AMultiMCNNetwork	Enter Contact Name
ompany Logo (URL)	Contact Email
Enter Company Logo URL	Enter Contact Email
Iomain Name	
Enter Domain Name	

Onboarding DIY Enterprise Customers

This section describes the process to onboard DIY enterprise customers and the procedure to invite administrators to manage their SD-WAN network.

Onboarding DIY customers

1. Customer logs into Citrix Cloud account.



A menu of all the available services offered on Citrix Cloud is displayed on the home page. The **Citrix SD-WAN Orchestrator service** tile can be found in the **Available Services** section.

Note

Ensure that you sign up for Citrix Cloud using only one official account. The company name and email-id used must be associated with only one Citrix Cloud account.

2. The customer clicks **Request Trial**.



The customer's SD-WAN account gets provisioned.



3. The Citrix SD-WAN Orchestrator service tile now shows up under My Services. Click Manage.

	Library Offerings Resou View Library Edit of	1 Domains r Add New Add New	Image: Description Image: Description Notifications Open Ticks View All View All	ets
My Services (2) SD-WAN Orchestrator Centralized cloud management service for SD-WAN Learn more Available Services (15)				
Analytics Security, performance and usage insights. Manage Learn more	Application Delivery Controller Intent based application delivery of Apps or AWS Request Trial Learn more	n Hybrid management ad analytics service for Citrix Networking on-premises and cloud. Manage Learn more	Comprehensive cloud security services for SaaS and Cloud apps Request Demo Learn more	S Content Collaboration Secure data access on any device. Add Service
Endpoint Management Enable subscribers to use corporate or BYO devices.	Gateway SSO to SaaS, web and VDI apps.	ITSM Adapter Provision and manage Virtual Apps and Desktops. Request Trial	Control Contro	Wicroapps Streamline workflows and deliver actionable notifications using behavioral insights Request Demo
Learn more Learn more Secure Browser Protect corporate network from web based attacks.	Learn more	Learn more	Learn more	Learn more
Request Trial	Request Trial	Request Trial	Apps and Desktops from Azure Request Demo	profile management. Request Trial Learn more

The customer can now access their Citrix SD-WAN Orchestrator service Network Dashboard. That completes the onboarding process.

Note

If the customer has Citrix Secure Internet Access subscription as well, then the customer can also click **Manage** on the **Secure Internet Access** tile to view the Citrix SD-WAN Orchestrator service Network dashboard. For information on onboarding Citrix Secure Internet Access, see Citrix Secure Internet Access.

PROVIDER Citrix Systems IncInternal	Enter	customer stre prise / / All Sites V Change Role 🖉 🕐
C DASHBOARD		Relative Time Interval: Last 1 Hour Site Group: All
REPORTS	>	C ALERTS See All O UPTIME See Datalis
CONFIGURATION	>	Overlay Underlay Isakmp Unclas mozilla pod5_6100 Critical 77.8% 77.8% 25.01 MB 12.45 MB 2.82 MB 0 %
1 ALERTS	>	+ New Site Map List Select Continent V Select Country V Search Q 10 2 1 7 Total Sites Critical Warring Normal
	>	Map Satellite
	>	C Final C
		Citata Uning Patta
		North Pacific Ocean North Atlantic Ocean North Atlantic Ocean North Atlantic Ocean North Atlantic Ocean

Adding Administrators

An enterprise customer can invite an administrator to manage their SD-WAN network.

1. Log into Citrix Cloud and navigate to Identity and Access Management.

× citrix					ŧ
Home					
My Services 🗸 🗸		(F) 1	\bigcirc	$\bigcirc 0$	
Library	Library Offerings	토니 Resource Location	Domains	کے V Notifications	Open Tickets
License & Usage	View Library	Edit or Add New	Add New	View All	View All
Identity and Access Management					
Resource Locations					
Support Tickets					
Notifications	°≣				
System Log	for Comprehensive cloud securi SaaS and Cloud a	Access ity services for ipps			
Manage	Trial Request	red			
Learn more	<u>Learn more</u>				

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

÷	Identi	ty and Access I	Vanagement					
	Authentic	ation Administrators	API Access Domains Re	covery				
	Select an Citrix le	identity provider dentity	∽ Invite			C Refresh	Bulk Actions	~
		Туре↓	Display Name	Email	Status	Access	Identity Provider	
		User	10000	100100	Active	Full	Citrix Cloud	•••
		User	Presser Roman	210000-11000-1011-110	Active	Full	Citrix Cloud	•••

3. Select Full access and click Send Invite.

	i	×
	will be added to Orchestrator Dev US	
	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.	
\bigcirc	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	_
	Cancel Send Invite	

The administrator details are displayed.

Identity and Access Management

Citrix mail /	Identity Address	✓ Invite			C Refresh	Bulk Actions	~
	Туре↓	Display Name	Email	Status	Access	Identity Provider	
	User	1000	100100	Active	Full	Citrix Cloud	
	User	Press Turner		Active	Full	Citrix Cloud	
	User	Presser Roman	and a strange of a set	Invite Sent	Full	Citrix Cloud	•••

Once the administrator accepts the request, the status changes to Active.

← Identity and Access Management

Authentic	ation Administrators	API Access Domains Re	ecovery				
Select an Add ad	identity provider ministrators from	~			C Refresh	Bulk Actions	~
	Туре	Display Name 🛧	Email	Status	Access	Identity Provider	
	User	Presser Roman	2000-1470-101-00	Active	Full	Citrix Cloud	•••
	User	10000	100-100-00	Active	Full	Citrix Cloud	•••
	User	1000	a the fire align of cars.	Active	Full	Citrix Cloud	•••

No access role

There are multiple services available under Citrix Cloud including Citrix SD-WAN Orchestrator service. Customers who have a Citrix Cloud account only can access those services. To get access to Citrix Cloud, refer Sign up for Citrix Cloud.

Earlier, at a provider level, all the users had the full administrator access to the Citrix SD-WAN Orchestrator service UI. In this case, a tenant uses a public domain or where the domain is not configured for a particular tenant, any new user added can access to all the tenant accounts and the information which is a potential security risk.

Also, for multiple domains, it is difficult to add/update a user every time. For a multi-MCN setup, multiple users can be added at a time with no access role.

With the **No access role** feature, initially a provider administrator can avoid giving the full access role to a newly added user. When the user clicks the Citrix SD-WAN Orchestrator service, the UI gets stuck

on loading, and you cannot perform any actions. The administrator can later decide whether to restrict access to the newly added user or add them to a specific tenant.

However, the details of a newly added user are available under the **User Settings** page with the **Provider-No-Access** role.

	u .			
Role		Expiration date	Customers	
Provider-Master-Admin-All		NA	NA	-
Provider-Master-Admin-All	\sim	NA	NA	-
Provider-Master-Admin-All	~	NA	NA	-
Provider-Master-Admin Tanant Provider-Master-Admin All Provider-Master-Admin Provider-Statest-Admin Provider-Statest-Admin Provider-Statest-Admin Provider-Statest-Admin Provider-Statest-Admin				
	Role Provider-Master-Admin-All Provider-Master-Admin-All Provider-Master-Admin-All Provider-Master-Admin-All Provider-Master-Admin-All Provider-Master-Admin All Provider-Master-Admin All Provider-Master-Admin ReadOnly All Provider-Master-Admin Provider-Master Admin Provider-Master-Admin Provider-Master Admin Provider-Master-Admin Provider-Support ReadOnly All Provider-Master-ReadOnly All Provider-Master-ReadOnly All Provider-Master-ReadOnly All	Role Provider-Master-Admin-All Provider-Master-Admin-All Provider-Master-Admin-All Provider-Master-Admin-All Provider-Master-Admin-All Provider-Master-Admin-All Provider-Master-Admin-All Provider-Master-Admin-All Provider-Master-Admin-Planet Provider-Master-Admin-Planet Provider-Master-Admin Provider-Master-Admin Provider-Specification Provider-Baser-Radmin-Planet Provider-Baser-Radmin-Planet	Role Expiration date Provider-Master-Admin-All NA Provider-Master-Admin-All Provider-Master-Admin Provider-Master-Master-Admin Provider-Master-Admin Provider-Master-Master-Admin Provider-Master-Admin Provider	Role Expiration date Customers Provider-Master-Admin-All NA NA Provider-Master-Admin-All NA NA

You can add a user under **Identity and Access Management > Administrators**. Select **Citrix Identity** from the drop-down list, add the user's email address, and click **Invite**.

Click the **Custom access** radio button, select the **Provider: No Access** check box, and click Send **Invite**.

Identity and Access Management Authentication Administrators API Access Domains Recov Select an identity provider Citrix identity	×
aparna.swain@citrix.com	aparna.swain@citrix.com will be added to Anil-RJMSP Before sending the invite, set the access for this administrator.
User RJIO NoOpRole	Full access Full access allows administrators management control of Citrix Cloud and its services, as well as adding or removing other administrators.
User Pradeep Kumar Warr	Custom access Custom access allows you to determine the exact part of Citrix Cloud your administrators can manage. witching to custom access will remove management access to certain services.
User Anilkumar Biradar	Select all Deselect All
User Anil RJrole	Provider Admin:Full Access Provider: No Access Provider: Read Only Access When the invite is accepted, all admins × with Full access will be notified by email that this user or group has been added to the account.

At any time, the provider administrator can decide to give read only or full access to the user and by that time the user settings details can be updated to a specific MCN.

A newly added user gets an email notification to accept the invite. Once the invitation is accepted, the user details are verified from back-end and the user is added with a no operational access role under

provider level within Citrix SD-WAN Orchestrator service.

Licensing

September 30, 2021

Citrix SD-WAN Orchestrator service provides licensing options for the following Citrix SD-WAN Orchestrator service users:

- Citrix Service Provider (CSP)
- Non-CSP partners:
 - Citrix Solution Advisor (CSA)
 - Citrix SD-WAN Managed Service Provider (MSP)
- Do It Yourself (DIY) customers Direct Enterprise Customers

Citrix SD-WAN Orchestrator service billing matrix

The billing matrix provides details about the type of billing models that are available to a user.

Orchestrator Users	Prepaid Annual Subscription	Prepaid Perpetual	Post paid
Citrix Service Provider (CSP)	\checkmark	\checkmark	~
Citrix Solution Advisor (CSA)	\checkmark	\checkmark	NA
Citrix SD-WAN Managed Service Provider (MSP)	\checkmark	\checkmark	NA
Do It Yourself (DIY) or Enterprise customers	\checkmark	✓	NA

Trial Mode

Every customer begins the onboarding process by requesting a trial. The customer clicks the **Request Trial** option for Citrix SD-WAN Orchestrator service on Citrix Cloud.

Citrix SD-WAN Orchestrator



The customer Citrix SD-WAN Orchestrator service account is provisioned in trial mode. The trial mode continues for a default period of 60 days.

After the trial period expires, the behavior is as follows:

- **Prepaid Model**: When the trial mode 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 Citrix SD-WAN Orchestrator service changes from Trial to Production when the first valid license is hosted on the Citrix SD-WAN Orchestrator service. 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 Citrix SD-WAN Orchestrator service 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.
- **Postpaid Model**: Postpaid model is supported for CSP partners and their customers only, on trial expiry the partner can choose to upgrade to production. A persistent message "Your Trial has expired. Click "Upgrade to Production" to restore the network functionality and continue the usage" is displayed. Click **Upgrade to Production** to upgrade licenses for all sites and the license details for the same can be viewed under License Usage Insights

Billing Models

Postpaid Billing Model

The postpaid billing model is available for customers of CSP partners. The customer can choose **Postpaid** as the default-billing model for their network. The selected billing model is applied by default to all the appliances in the customer's network.

To select a postpaid billing model, in the Citrix SD-WAN Orchestrator service, at the network level navigate to **Administration** > **Licensing**.

Click Select Billing Model, select Postpaid billing model, and click Submit.

Customer OnBoardir	ng
Please Confirm Billing Model	
Postpaid	\sim
Postpaid	
Prepaid Annual And Perpetual	

Note

If a customer wants to have their postpaid billing model changed to prepaid billing model, a support ticket has to be raised.

In the postpaid billing model, there is no need to upload licenses to the individual sites in the customer network. Each customer's network must be configured with the desired device models and bandwidth tiers. The CSP is billed accordingly for each customer, every month.

Prepaid Billing Model

The prepaid billing model is available for tenants of CSP and non-CSP partners, and DIY - Enterprise 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 Citrix SD-WAN Orchestrator service and the maintenance license are included in the same license 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 Citrix SD-WAN Orchestrator service entitlements and hardware maintenance (SD-WAN entitlements) license must be purchased separately. All the appliances in the customer network have a prepaid perpetual subscription.

• **Hybrid**: With the hybrid billing model, a customer's network can support both perpetual and annual subscription licenses. The appliances on the customer network can have either a prepaid annual subscription or a prepaid perpetual license.

To select a prepaid billing model, in the Citrix SD-WAN Orchestrator service, at the network level navigate to **Administration** > **Licensing**

For a CSP customer, click Select **Billing Model**, select the **Prepaid Annual and Perpetual** billing model, and click **Submit**.

Customer OnBoarding	
Please Confirm Billing Model	
Prepaid Annual And Perpetual	\sim
Postpaid	
Prepaid Annual And Perpetual	

For a non-CSP customer, you can directly retrieve and allocate license entitlements. For more information, see Retrieve and assign entitlements for prepaid billing model.

All prepaid customers, need to upload licenses to Citrix SD-WAN Orchestrator service. These Licenses must be uploaded for every customer site. For more information, see Retrieve and assign entitlements for prepaid billing model.

Retrieve and assign entitlements for prepaid billing model

You need both Citrix SD-WAN appliance entitlements and Citrix SD-WAN Orchestrator service entitlements to perform any configuration changes. You can retrieve the license entitlements using the License Access Code provided by Citrix through email. License Access Code can be specific Citrix SD-WAN Orchestrator service only or Citrix SD-WAN appliance only or both.

Alternatively, the customer can also view the Access Code in the license management portal within Citrix Cloud. The customer can have either **Prepaid Perpetual**, **Prepaid Annual Subscription**, or **Hybrid** billing model in the network.

Prerequisite: Ensure that the Citrix SD-WAN Orchestrator service licenses are not allocated by logging into the license management portal. If the licenses are allocated, release/de-allocate the licenses before using the License Access Codes in Citrix SD-WAN Orchestrator service.

 In the Citrix SD-WAN Orchestrator service UI navigate to Administration > Licensing and click Select Billing Model. Select a billing model and click Submit.

Customer OnBoarding			
Please Confirm Billing Model			
Postpaid	\sim		
Postpaid			
Prepaid Annual And Perpetual			
		Cancel	Subm

2. Click Retrieve Licenses.

Network A	dministratio	n: Licensin	g			I	icensing Model	Prepaid Annual Ar	nd Perpetual
Retrieve L	icenses	Upgrade	to Production						
License Viev	Site View							Search	Q
SDWAN Entitle	ements								
Device Model	Device Edition	Bandwidth	Expiration Date	License Type	License Access Code	Licenses Available	Assigned To Sites	Actions	
					Page Size: 50	✓ Showing	0-0 of 0 item	Page1 of1	• •

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

LILEVE LICENSES			
+ License Access Code			
Enter License Access Coo			
Enter License Access Co			

The Citrix SD-WAN Orchestrator service retrieves the entitlements and populates the license table.

Network Administration: Licensing Model: Prepaid Annual And Perpetual								ual			
Detrievel		Unexade	to Draduction								
Retrievel	licenses	Opgrade	to Production								
License View	Site View										
									Search		0
											~
SDWAN Entitle	ements										
Device Model	Device Edition	Bandwidth	Expiration Date	Software Maintenance	License Type	License Access Code	Licenses Available	Assigned To Sites	Actions		
CB110	SE	100	December 1, 2022 5:30	2022-12-01 00:00:00.0	SD-WAN software Subscript	1617181539	9	0	Assign	Unassign	
CB1100	SE	500	December 1, 2022 5:30	2022-12-01 00:00:00.0	SD-WAN software Subscript	1617181539	9	0	Assign	Unassign	
CB2000	SE	300	December 1, 2022 5:30	2022-12-01 00:00:00.0	SD-WAN software Subscript	1617181539	9	0	Assign	Unassign	
CB210	SE	100	December 1, 2022 5:30	2022-12-01 00:00:00.0	SD-WAN software Subscript	1617181539	9	0	Assign	Unassign	
CBVPX	SE	300	December 1, 2022 5:30	2022-12-01 00:00:00.0	SD-WAN software Subscript	1617181539	19	1	Assign	Unassign	
CBVPX	SE	500	December 1, 2022 5:30	2022-12-01 00:00:00.0	SD-WAN software Subscript	1617181539	9	1	Assign	Unassign	
						Page Size:	50 V Show	ing 1-6 of 6 ite	ms Pa	ge1 of1	

- 4. The licenses get automatically assigned when a new site is added, or when the bandwidth, platform, or software edition of an existing site is modified. Licenses are automatically assigned only when a new site is added and there are unused licenses in the Citrix SD-WAN Orchestrator service. Automatic license assignment does not work on existing sites that were added before the licenses were retrieved.
- 5. Optionally, you can assign licenses manually for each site. To assign licenses manually, 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							
All the unlicensed sites with co	nfigured bandwidth equal to or less	than the license bandwidth ar	e displayed.				
Site	Device	Platform	Configured Bandwidth				
1980_A22	secondary	VPX	200				
	Page Siz	ze: 200 V Showing 1-1	of 1 items Page1 of1				
		Car					

6. Select a site, click **Assign**, and then click **Upgrade to Production**.

Note

While assigning licenses manually, you can select only one site at a time.

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.

Citrix SD-WAN Orchestrator

Details	s of Licensed Si	tes					
View:	• All Licensed /	All Unlicensed					
	Site	Device	Device Model	Configured Bandwidth	Expiration Date		
	MCN_Nort	secondary	CB1100	200	1732838400000)	
	MON_Next	primary	CB1100	200	1732838400000)	
			Page Size: 2	200 V Showing 1-	2 of 2 items	Page1 of1	

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

Cancel

Note

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

License View	Site View										
									Search		Q
Site	License Status	HA Role	Device Model	Device Edition	Configured Bandwidth	Licensed Bandwidth	License Expiration	Software Maintainence	License Type	Action	
100	Inactive	primary	CBVPX	SE	20	500	December	December	SD-WAN s	Unassign	
						Page Si	ze: 50 🗸	Showing 1-1 of	1 items Pa	ge1 of1	• •

Customers with perpetual billing models have Citrix SD-WAN Orchestrator service entitlements displayed under the **License View** table:

Orchestrator Entitlements

Total : 54

Expires :	November	29,	2024	5:30	AM

License Access Code	Licenses Available
LA-0002985185-55496	0
LA-0002685185-55496	9
LA-0002985185-55496	0
LA-0002685185-55496	27
Page Size: 200 V Show	ring 1-4 of 4 items Page1 of1

License Usage Insight

A partner can view the license usage of all the customers under partner level, **Administration** > **License Usage Insights**. Select the customer and period for which you want to view license usage insight.

Provider Administrati	on: License Usage Insig	ghts			
Select Customer: All	V Select Period: 2019-M	ar			Search Q
Customer Name	Site Name	Serial No	Appliance Mode Name	Appliance Software Edition	Max Configured Bandwidth
Abycare Hospitals	London	31:0x3:31a1672567104	CBVPX	SE	200
Abycare Hospitals	NewYork	1407s20 are7-0554-4cc	CBVPX	SE	500
Abycare Hospitals	San Francisco	47547122-35aa 5443-315c	CBVPX	SE	500
Abycare Hospitals	San Francisco	691852ab foot 3/18 b4a5	CBVPX	SE	500
Abycare Hospitals	Belgium	x5x3bc15 x874 4803 dbh	CBVPX	SE	500
Abycare Hospitals	Madrid	4343796: 53% 4:x2-631	CBVPX	SE	500
Creative Enterprises	DAASMCN	0000-0001-0307-4875-011	CBVPX	SE	100
Creative Enterprises	AzureBranch	0000-0009-9954-6380-98.	CBVPX	SE	1000
Creative Enterprises	BranchHA	8000-0010-3881-7804-815	CBVPX	SE	20
			Page Size:	50 🗸 Showing 1-9 of 9	items Page1 of1 🔹 🕨

An individual customer can view the license usage details under network level, **Administration** > **Li-cense Usage Insights**. Select the period for which you want to view license usage insight.

Citrix SD-WAN Orchestrator

Site Name	Serial No	Appliance Mode Name	Appliance Software Edition	Max Configured Bandwidth
London	3%0x3c3 \u06 7356 7104 c5586	CBVPX	SE	500
NewYork	1407623 4447 0554 4110 2044	CBVPX	SE	500
San Francisco	47540122 3baa 5643 315c 4755	CBVPX	SE	1000
San Francisco	691852ab foc0 3/18 b4a5 4/1w8	CBVPX	SE	1000
Belgium	x5x3bc15 x874 4803 dbb8 x1%	CBVPX	SE	500
Madrid	4343790: 53% 4:42 42% 2:06.	CBVPX	SE	500
			Page Size: 50 V Showing 1-6	of 6 items Page1 of1 🔹 🕨

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 virtual paths associated with the sites are brought down.

Email notifications are sent to all the administrators every day before the licenses are about to expire.

For customers with a prepaid annual and perpetual license billing model and upgraded to production, license expiry email notifications are sent 90 days before the license expiry. The license expiry notification contains information about the license access code, details of affected sites, expiry date, and number of days remaining for license expiry. Email notifications are stopped once the licenses are renewed and reassigned to sites.

For customers with a prepaid annual and perpetual license billing model and upgraded to production, grace expiry email notifications are sent 30 days before the expiry of grace licensed appliances. The grace expiry notification contains information about site name, grace period expiry date, and number of days remaining for grace expiry. Email notifications are stopped once the licenses are renewed and reassigned to sites.

For trial customers, email notifications are sent 30 days before trial period expiry. Trial expiry email notifications are stopped once licenses are retrieved, assigned to sites, and upgraded to production.

Provider level configuration

July 16, 2020

Profiles

A profile is a **live configuration template**. A regular template is meant to aid the creation of a new entity. But once the template is created, subsequent changes in the template do not apply to the new entities created using the base template. A profile serves as the live central master entity, which all child entities inherit from, not only during creation but also throughout the life of a profile. All the children 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.

Profile templates for service providers

Partners can create profile templates, which their customers can use while creating profiles.

For example, a provider can create four site profile templates –Small Branch, Medium Branch, Large Branch, and Data Center. These templates are automatically made available to the customer accounts associated with the partner. Customers can use these templates while creating profiles.

For instance, let's say a customer decides to create a profile for small branch configuration. The customer can select one of the templates shared by the partner, made available through a drop-down list as part of the profile configuration. The customer can customize it to their network needs before saving the profile. The profile template is not a live entity. It just aids the creation of profiles at the customer level. Profiles can be created only at a customer level, and are meant to be live entities serving as master configuration records.

The provider can create configuration profiles, which can be shared with some or all customers, as needed. Site and WAN profiles are supported currently.

Site profile templates

Site profile templates are site configuration templates created by service providers, to enable the creation of site profiles at a customer level.

To create profile templates, navigate to **Configuration** > **Site Profile Templates** and click **+ Site Pro-file Template**.

Provider Configuration: Site Profile Templates



To create a site profile template, you need to configure the **Site Details**, **Interfaces**, and **WAN Links**. For detailed description of configuring sites, see <u>Site details</u>.

Provider Configuration: Site Profile Templates

Profile Inform	nation					
Site Profile Templat	te Name *					
Site & Device	Details					
evice Model *		Device Edition *		Sub-Model *	:	Site Role *
210	\sim	SE	\sim	BASE	~	Select Site Role $$

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.

	Ces 03 WAN L	_inks			
Interface Attributes					
Deployment Mode * Interfa Edge (Gateway) \cong Li	ce Type * AN V	Security *	~	Interface Name	
Select Interface*					
Select Interface* 1/1 1/2 1/3 1/4 1/5 Virtual Interfaces					
Select Interface * 1/1 1/2 1/3 1/4 1/5 Virtual Interfaces	Virtual Interface Na	ame	DHC	P Client	
Select Interface* 1/1 1/2 1/3 1/4 1/5 Virtual Interfaces VLAN ID* 0	Virtual Interface Na VIF-1-LAN-1	ame	DHC	P Client	
Select Interface* 1/1 1/2 1/3 1/4 1/5 Virtual Interfaces VLAN ID* 0	Virtual Interface Na VIF-1-LAN-1	ame Firewall Zones	DHC	P Client	
Select Interface * 1/1 1/2 1/3 1/4 1/5 Virtual Interfaces VLAN ID * 0	Virtual Interface Na VIF-1-LAN-1	ame Firewall Zones <default></default>	DHC	P Client	~

Provide **WAN Link Attributes**, **Access Interfaces**, and **Services** with **Advanced Options**. For detailed description of configuring WAN links, see WAN Links.

Provider Configuration:Site Profile Templates

Access Type *	ISP Name *	Custom	Internet Category	
Public Internet V	Verizon Comm	~	Broadband	\sim
Link Name *	Public IP A	ddress Auto De	etect	
Broadband-Verizon_Comm-1				
Egress Speed * 100	Mbps ∨	Ingress Speed * 100		Mbps ∨
Access Interface Name	Virtual Interface *		Virtual Path Mode *	
Access Interface Name	Virtual Interface * VIF-1-LAN-1	~	Virtual Path Mode * Primary	~
Access Interface Name	Virtual Interface * VIF-1-LAN-1	~	Virtual Path Mode * Primary	∽ Save
Access Interface Name AIF-1 Advanced WAN Options	Virtual Interface * VIF-1-LAN-1	~	Virtual Path Mode * Primary	∽ Save
Access Interface Name AIF-1 Advanced WAN Options Enable Metering	Virtual Interface * VIF-1-LAN-1	~	Virtual Path Mode * Primary	✓
Access Interface Name AIF-1 Advanced WAN Options Enable Metering Congestion Threshold (µs)	Virtual Interface * VIF-1-LAN-1 Provider ID	~	Virtual Path Mode * Primary Frame Cost (Bytes)	∽ Save ▲
Access Interface Name AIF-1 Advanced WAN Options Enable Metering Congestion Threshold (µs) 20000	Virtual Interface * VIF-1-LAN-1 Provider ID	~	Virtual Path Mode * Primary Frame Cost (Bytes) 1	Save
Access Interface Name AIF-1 Advanced WAN Options Enable Metering Congestion Threshold (µs) 20000 Standby Mode	Virtual Interface * VIF-1-LAN-1 Provider ID MTU (Bytes)		Virtual Path Mode * Primary Frame Cost (Bytes) 1	Save

WAN link templates

WAN profile templates are WAN link configuration templates created by service providers, to enable the creation of WAN link profiles at a customer level.

Provider Configuration:WAN Link Templates

To create a WAN link template, click **+ WAN Link Template**. You need to fill the WAN link information such as **Profile Name**, **Access Type**, **Internet Category**, **LAN to WAN Rate** and so on. For detailed description of configuring WAN links, see WAN Links.

Network home

May 5, 2022

The **Network Home** page acts as an anchor for network configuration, offers enterprise network level configuration capabilities, and serves as the starting point for configuring the SD-WAN network of an enterprise.

The **Network Home** page displays the total sites within the network and also segregates the sites based on their connectivity status. Select the numbered links to view the sites based on the following status categories:

- **Critical** –Sites that have all the associated virtual paths down.
- Warning Sites that have at least one virtual path down.
- Normal All virtual paths and associated member paths of the site are up.
- **Inactive** Sites are in the undeployed and inactive state.
- **Unknown** Status of the site is unknown.

Clicking the status filters the sites based on their status and displays the details. You can also use the **Search** bar to view the details of a site based on the site name, role, overlay connectivity, model, bandwidth tier, and the serial number parameters.

You can export the filtered results in to a CSV or PDF file by using the **Export as CSV** and **Export as PDF** options. The CSV and PDF file name is prefixed with **SiteList** followed by the date and time when the file is exported.

Configuration	/ Netv	vork Home								Verify Conf	iguration Software Version :	: 11.4.1.9-GA
Network	< Sites								Site Group:	All 🗸	Add Site Mo	ore
5 TOTAL SITES	5 Total sites 1 1 3 0 0 0 INACTIVE UNKNOWN Search Export as CSV Export as C								Q port as PDF			
Site Name						Role	Overlay Connectivity	Model	Bandwidth Tier	Orchestrator Connectivity	Serial No	Actions
myLTE						Branch	CRITICAL	210-SE	20	PRIMARY ACTIVE ONLINE	0	•••
SantaClara						MCN	WARNING	VPX-SE	50	PRIMARY ACTIVE ONLINE	6	
Boston						Branch	NORMAL	VPX-SE	50	PRIMARY ACTIVE ONLINE	6	
Kansas						Branch	NORMAL	VPX-SE	20	PRIMARY ACTIVE ONLINE	G =	•••
Dallas						Branch	NORMAL	VPX-SE	20	PRIMARY ACTIVE ONLINE	0	•••
									Page Size:	50 V Showing 1-5 of 5	items Page1 of1	•

On the top right corner of the screen, you can view the current software version. Click **Verify Configuration** to validate any audit errors. For more details, see Verify Configuration.

You can filter the sites based on the group/region to which they belong by using the **Site Group** dropdown list.

Configuration	/ Netw	ork Home								Verify Con	figuration Software Version :	: 11GA
Network	Sites								Site Group:	All	Add Site Mo	ore
5 TOTAL SITES		1 WARNING	3 NORMAL	0 INACTIVE	O UNKNOWN				Sea	rch		Q
											Export as CSV Ex	port as PDF
Site Name						Role	Overlay Connectivity	Model	Bandwidth Tier	Orchestrator Connectivity	Serial No	Actions
myLTE						Branch	CRITICAL	210-SE	20	PRIMARY ACTIVE ONLINE	C	
SantaClara						MCN	WARNING	VPX-SE	50	PRIMARY ACTIVE ONLINE	Ō	
Boston						Branch	NORMAL	VPX-SE	50	PRIMARY ACTIVE ONLINE	0	
Kansas						Branch	NORMAL	VPX-SE	20	PRIMARY ACTIVE ONLINE	6	•••
Dallas						Branch	NORMAL	VPX-SE	20	PRIMARY ACTIVE ONLINE	0	•••
									Page Size:	50 V Showing 1-5 of 5	items Page1 of1	•

Clicking the site name in the filtered result takes you to the **Site Configuration** screen. If the site is in a high availability setup, then the **Orchestrator Connectivity** column displays the status of both primary and secondary appliances. The **Serial No** column displays the serial number of the appliance.

In a high availability setup, both primary and secondary appliance serial numbers are displayed. You can copy the serial number of the appliance using the copy icon.

Using the **Actions** column, you can view details, edit, clone, delete, reset, and update the password of the site. You can also reboot the devices associated with a site.

Network	Sites								Site Group:	All	Add Site	More
5 TOTAL SITES		1 WARNING	3 NORMAL	O INACTIVE	O UNKNOWN				Sear	ch		Q
											Export	as CSV Export as PDF
Site Name						Role	Overlay Connectivity	Model	Bandwidth Tier	Orchestrator Connectivity	Serial No	Actions
myLTE						Branch	CRITICAL	210-SE	20	PRIMARY ACTIVE ONLINE	C x (C)	(45)
SantaClara						MCN	WARNING	VPX-SE	50	PRIMARY ACTIVE ONLINE	C 414	View Details Edit
Boston						Branch	NORMAL	VPX-SE	50	PRIMARY ACTIVE ONLINE	C 3EBF	Clone
Kansas						Branch	NORMAL	VPX-SE	20	PRIMARY ACTIVE ONLINE	0 75-3	Reboot
Dallas						Branch	NORMAL	VPX-SE	20	PRIMARY ACTIVE ONLINE	ⓐ →450	Reset Update Password
									Page Size:	50 V Showing 1-5 of 5	items Pag	e1 of1 🔹 🕨

You can perform other actions such as upload configuration, add sites in a batch, download JSON, and so on using the **More** ... option.

Network	Sites								Site Group:	All	Add Site	More
-			~	~	~							Deploy config/software
5 TOTAL SITES	CRITICAL	WARNING	3 NORMAL	U	UNKNOWN				Sear	rch		Upload Config
											Eve	Backup Config
											EXP	Download JSON
Site Name						Role	Overlay	Model	Bandwidth	Orchestrator Connectivity	Serial No	Download DB
							Connectivity		Tier			Batch Add Sites
myLTE						Branch	CRITICAL	210-SE	20	PRIMARY ACTIVE ONLINE	C en <mark>x</mark>	Add Region
SantaClara						MCN	WARNING	VPX-SE	50	PRIMARY ACTIVE ONLINE	© .	Add Group
Boston						Branch	NORMAL	VPX-SE	50	PRIMARY ACTIVE ONLINE	G	•••
Kansas						Branch	NORMAL	VPX-SE	20	PRIMARY ACTIVE ONLINE	0	331.7384
Dallas						Branch	NORMAL	VPX-SE	20	PRIMARY ACTIVE ONLINE	6	004-063
									Page Size:	50 V Showing 1-5 of 5 i	items Pa	age1 of1 🔹 🕨

Add sites

To add a single site, navigate to the **Add Sites** drop-down list and click **Add single site**. To add a site using a site template, select **Add New Site Using Template** from the drop-down list.

For more information on site configuration workflow, see Site Configuration.

Clone sites

Citrix SD-WAN Orchestrator service allows you to clone a branch site. Cloning a site streamlines the process of adding and configuring more branch nodes. When a site is cloned, a set of site configurations that require changes are copied and displayed in a single form page. You can then modify the settings according to the requirements of the new site. Some of the original settings can be retained, where applicable. However, most of the settings on the single form page must be unique for each site.

Note

The Virtual WAN appliance models must be the same for both the original and the cloned sites. You cannot change the specified appliance model for a clone. If the appliance model is different for a site, you must manually add the site.

To clone a site, select Clone from the Actions column in the Network Sites section. However, if some features require any modifications, verify the configuration details after cloning the site and make the changes as required.

Deploy configuration and software

The **More > Deploy Config/Software** option takes you to the **Deployment** section that helps verify, stage, and activate the configuration across the network. For more information on deploying configuration and software, see Deployment.

Upload Configuration

The **More > Upload Configuration** option allows you to browse and upload one of the previously saved configurations. The newly uploaded configuration serves as the active configuration for the network.

Load Configura	ation				
Choose File Browse Valid Extension: json	No File Selected				
			Cancel	Proceed	

Back Ups/Checkpoints

The **More > Backup Config** option takes you to the **Back Ups / Checkpoints** page and provides the ability to back-up and restore the configuration, or review the saved checkpoints.

BackUps / Checkpoints ①			
Back Ups / Checkpoints			
Back Up Current Config			
Config Checkpoint Name	Time of Creation	Comments	Actions
Autosaved_Running_Config	2022-4-22 12:27pm	Autosaved_Running_Config	
Autosaved_Running_Config	2022-3-28 3:45pm	Autosaved_Running_Config	
Autosaved_Running_Config	2022-3-25 4:40pm	Autosaved_Running_Config	
Autosaved_Running_Config	2022-3-211:02pm	Autosaved_Running_Config	

Click Verify Configuration to validate any audit error.

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

Citrix SD-WAN Orchestrator

Configuration / BackUps / Checkpoints			Verify Configuration Software Version : 11.5.0.4005-HOTFIX
BackUps / Checkpoints ①			
Back Ups / Checkpoints			
Back Up Current Config			
Config Checkpoint Name	Time of Creation	Comments	Actions
22Dec2021	2021-12-22 1:22pm		
20_Dec_2021	2021-12-20 2:43pm	with the change in firmware to 12.x	
07Dec2021	2021-12-7 2:28pm		
My_Manual_Config	2021-11-25 11:36am		
25Nov2021	2021-11-25 9:22am		
Autosaved_Running_Config	2021-9-7 2:49pm	Autosaved_Running_Config	
Autosaved_Running_Config	2021-9-1 6:08pm	Autosaved_Running_Config	
Autosaved_Running_Config	2021-6-17 4:16pm 🖏	Autosaved_Running_Config	
Autosaved_Running_Config	2021-6-16 10:47pm	Autosaved_Running_Config	•••
Autosaved-Running-Config	2021-6-2 10:15pm	Auto-generated	

Click Load Config (under Actions) to load a saved configuration. Click Proceed.

Load Configuration			
Review the differences between configured, as a quick sanity che	the current configuration and the configu ck. Are you sure you want to load the sele	ration checkpoint you're trying to load, in terms of the site cted configuration checkpoint?	es
Site	Current Config	Saved Checkpoint About To Be Loaded	
BR3	\checkmark	\checkmark	
BR1	\checkmark	\checkmark	
BR2	\checkmark	\checkmark	
HQ	\checkmark	\checkmark	
		Cancel Procee	d

Click **Copy** (under **Actions**) to create a similar copy of an existing configuration. You can also download, edit, and delete the saved configuration checkpoints. These operations are available under **Ac-tions**.

Download JSON

The **More > Download JSON** option allows you to download and export the current configuration in JSON format, for offline review.

Download DB

The **More > Download DB** option allows you to download and export the current configuration in DB format.

Add sites in a batch

The **More > Batch Add Sites** option allows you to quickly add several sites in 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.

Sites 10 + Site Profile : None	∽ Show Lat/Lng			
te Name	Site Address	Site Profile (Optional)		Actio
Enter a Site Name	Search for a Site Address	None	\sim	Û
Enter a Site Name	Search for a Site Address	None	\sim	Ē
Enter a Site Name	Search for a Site Address	None	\sim	Ē
Enter a Site Name	Search for a Site Address	None	\sim	Ī
Enter a Site Name	Search for a Site Address	None	\sim	Ē
Enter a Site Name	Search for a Site Address	None	\sim	Î
Enter a Site Name	Search for a Site Address	None	\sim	Ē
Enter a Site Name	Search for a Site Address	None	\sim	Î
Enter a Site Name	Search for a Site Address	None	\sim	Î
Enter a Site Name	Search for a Site Address	None	\sim	Ē

Add Region

The **More > Add Region** option allows you to create a region and takes you to the **Site & IP Groups > Regions** page. For more information, see Regions.

Add Group

The **More > Add Group** option takes you to the **Site & IP Groups > Custom Groups** page where you can create a region. For more information, see Custom Groups.

Update password

You can change the password of the SD-WAN appliances at different sites, across the network, through the Citrix SD-WAN Orchestrator service.

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

Network	Sites					Site Group:	All ~	Add Site	More
5 TOTAL SITES		3 NORMAL	O INACTIVE	O unknown			Search		Q
								Export	as CSV Export as PDF
Site Name			Role	Overlay Connectivity	Model	Bandwidth Tier	Orchestrator Connectivity	Serial No	Actions
myLTE			Branch	CRITICAL	210-SE	20	PRIMARY ACTIVE ONLINE	(C)	(45)
SantaClara			MCN	WARNING	VPX-SE	50	PRIMARY ACTIVE ONLINE	C 4	View Details Edit
Boston			Branch	NORMAL	VPX-SE	50	PRIMARY ACTIVE ONLINE	10 3F	Clone
Kansas			Branch	NORMAL	VPX-SE	20	PRIMARY ACTIVE ONLINE	6 3	Reboot
Dallas			Branch	NORMAL	VPX-SE	20	PRIMARY ACTIVE ONLINE	۵ ; c	Reset
						Page Size:	50 × Showing 1.5 of 5 i	toma Pag	ol of l
						Fage Size.	Showing 1-5 01 5	rdg	eron

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 for confirmation.

Jser Name *		
admin	\sim	
Current Password *		

New Password *		

Confirm Password *		

	Cancel	Save

Configuration difference

January 27, 2022

The **Config Diff** capability helps you to review the difference between any two versions of configuration checkpoints. The **Config Diff** option is available at the Network level, under **Configuration** > **Config Diff**.

Diff ①	
chal Features Site Features	Config Check Funct 1* Autorspeed-flumning-Config - 2021-06-02 16:45:41 Config Check Funct 2* Config Check Funct 2* Currently Loaded - 2021-12-20 09:15:19
Regions	(
Qo E Configuration	1 regions: (
Qo E Profile	2 { 3 allowExternalVipMatch: false,
Qo S Profiles	4 forceInternalVipNatch: false, 5 isDefault: true,
Config	6 name: **,
Properties	i - "Thirtywary",
Service Allocation	9 + "Thirwother", 10 = "Thirwother",
	11 + "Thirowarur"
	12) 13) 14]

During deployment, you can save a configuration with a suitable name. The saved configurations are known as checkpoints. While comparing the difference between the two configurations, you need to select the required configurations from the **Config Check Point 1/2** drop-down lists.

You can view the list of saved configurations backups/check points under **Configuration** > **Network Home** > select **Backup Config** from the **More** drop-down list.

Network Sites				Site Group:	All V	id Sites 🗸 🗸	More Deploy config/software
2 <u>TOTAL STES</u> O O O O 2 CRITICAL WARNING O O O 2 UNIXCTIVE UNIXOWN			Sea	irch		Exes	Upload Config BackungConfig Download Config
Site Name	Role	Overlay Status	Model	Bandwidth Tier	Orchestrator Connectivity	Serial No	Download DB Batch Add Sites
Thiruvarur	MCN	UNKNOWN	VPX-SE	500 Mbps	PRIMARY) ACTIVE OFFLINE	C DE406C	Add Region
Thiruvothur	Branch	UNKNOWN	VPX-SE	20 Mbps	PRIMARY ACTIVE OFFLINE	© 0A12686	Add Group
							Upload Config DB

When a deployment happens, the configuration is backed up automatically every time. You can also backup the current configuration manually. To do that, click the **Back Up Current Config** option.

Configuration / BackUps / Checkpoints			Verify Configuration Software Version : 11.5.0.4005-HOTFIX
BackUps / Checkpoints ①			
Back Ups / Checkpoints			
Back Up Current Config			
Config Checkpoint Name	Time of Creation	Comments	Actions
22Dec2021	2021-12-22 1:22pm		
20_Dec_2021	2021-12-20 2:43pm	with the change in firmware to 12.x	
07Dec2021	2021-12-7 2-28pm		
My_Manual_Config	2021-11-25 11:36am		
25Nov2021	2021-11-25 9:22am		
Autosaved_Running_Config	2021-9-7 2:49pm	Autosaved_Running_Config	
Autosaved_Running_Config	2021-9-1 6:08pm	Autosaved_Running_Config	
Autosaved_Running_Config	2021-6-17 4:16pm	Autosaved_Running_Config	
Autosaved_Running_Config	2021-6-16 10:47pm	Autosaved_Running_Config	
Autosaved-Running-Config	2021-6-2 10:15pm	Auto-generated	

Provide a name to save your configuration along with comments (optional). Click **Save**.

Citrix SD-WAN Orchestrator

h		
	h	<i>i</i> e

Note

Diff ④

You can save/create a maximum of five configuration backups. Creating a new backup automatically deletes the oldest backup configuration.

There are two types of configurations available:

• **Global level**: Under global category, you can view a list of global features updated such as Regions, Properties, and Configuration.

		Config Dheck Point 1*
	c	20_Dec_2021-202142-20.09:13:54 \lor
		Config Check Point 2*
L,	►	My_backup+2022-01-05 05:45:17 V
Johal Features Site Features		
Site realises		
Regions		(
Config	1	regions: [
Dramatian	2	
Properties	3	allowExternalVipMatchi Talee,
Service Allocation	4	ionenternalipmatchi talme,
	6	Date state
	7	siteNames: [
		"Thiruwarur",
	9 +	"Thiruvothur",
	10 -	"Thiruvothur",
	11 +	"Thiruvarur"
	12	
	13	3

• **Site level**: Under site category, you can select the site from the drop-down list and view the modified details such as Site, WAN Links, and DNS Services.

Citrix SD-WAN Orchestrator

Diff ①	
	Config Check Point 1*
	20_Dec_2021-2021-12-20 09:13:54
	Config Check Point 2*
	My_backup-2022.01.05.05:45:17 ~
Global Enatures Site Easter	
and reactives Site Features	ter m
Jites List *	
Thiruvarur	
Dns Services	(
Site	1 dnsServices: [
one	
	4 P 1
Vrrp	3 dnsServiceType: "dynamic_service",
Vrrp Wan Links	3 dosServiceType: "dynamic_service", 4 serviceInstance: "internet",
Vrrp Wan Links	<pre>3 dnsServiceType: 'dynamic_service', 4 serviceInstance: 'listerset', 5 serviceName: all1', 5 erviceName: all1',</pre>
Vrrp Wan Links	dnaServiceType: 'dysamic service', serviceInstance 'internet', serviceInstance 'all', serviceType: 'internet'
Vrrp Wan Links	<pre>3 dnServiceType: 'dynamic_service', 4 serviceInstance 'Literest', 5 serviceInstance 'silli', 6 serviceOtype: 'Literest' 7 s), 8 </pre>
Vrrp Wan Links	<pre>4 dnServiceType: 'dynamic_service', 4 * serviceInstance 'interset', 5 * serviceInstance 'allil', 6 * serviceType: 'allil', 7 *), 8 * { 9 * dnServiceType: 'state service',</pre>
Virp Wan Links	<pre>> dnServiceType: 'dysamic service', 4 serviceInstance 'internet', 5 serviceInstance 'all', 4 serviceType: 'internet' 5 s), 4 s (5 s (5 s (5 s (5 s)), 5 s (5 s), 5 s (5 s (5 s), 5 s (5 s), 5 s (5 s (5 s), 5 s (5 s</pre>
Virip Wan Links	<pre>4 dnServiceType: 'dynamic_service', 4 serviceInstance 'literast', 5 serviceType: 'literast', 6 serviceType: 'literast' 7 s), 8 serviceType: 'static_service', 9 s dnServiceType: 'static_service', 10 secondaryDes: 's,s,s', 11 secondaryDes: 's,s,s',</pre>
Vrrp Wan Links	<pre>4 dnServiceType: 'dynamic_service', 5 enserviceInstance 'literest', 6 enserviceInstance 'literest', 7 e), 8 enviceType: 'literest' 7 e), 8 dnServiceType: 'static_service', 10 ensecondaryOns: '9,0,0,0', 11 ensecondaryOns: '9,0,0,0', 12 ensecondaryOns: '1,0,0,0', 13 ensecondaryOns: '1,0,0,0', 14 ensecondaryOns: '1,0,0,0', 15 ensecondaryOns: '1,0,0,0', 16 ensecondaryOns: '1,0,0,0', 17 ensecondaryOns: '1,0,0,0', 18 ensecondaryOns: '1,0,0,0', 19 ensecondaryOns: '1,0,0,0', 19 ensecondaryOns: '1,0,0,0', 19 ensecondaryOns: '1,0,0,0', 19 ensecondaryOns: '1,0,0', 19 ensecondaryOns: '1,0', 19 ense</pre>

A deleted value appears in red background with minus symbol and the updated/added value appears in green back ground with plus symbol.

Diff ⁽¹⁾	
C,	Config Check Point 1° V 20_Dec2021-20:21-02:00 0913:54 V Config Check Point 2° V My_backup-2022-01-05 05:45:17 V
Global Features Site Features	
Regions	1
Config	1 = applianceSoftwareVersion: "R12_0_0_100_B88881", 2 = applianceSoftwareVersion: "R13_0_4005_888881",
Properties	3 nato: 'Default Config'
Service Allocation	

Deployment

August 10, 2022

The **Deployment** page allows you to change the software version, stage, and deploy the configuration across your network after the sites are configured. You can upgrade the SD-WAN software version on all the appliances and sites across the network.

The **Deployment** page contains the following sections:

- Switch to old deployment view
- Settings
- Deploy now
- Software and Configuration Deployment

The following sections on the **Deployment** page provide details of the deployment status:

- Sites View
- Deployment History
- Change management settings

Deployment 🐵							
This page has been enhanced with a new look and feel.	If you want to continue using old deploy	vment page, <u>Click</u>	: here				
Software and Configuration Deployment Deploy Now						Now	
1. Staging All Sites	2. Activating standby HA devices 0 / 0 Activating Activating Activating Failed		3. Activating the rest of 3/3 Activate Now	the devices Activating Activated Falled	4. Rollback Device	 Rollback in Progr Rollback complet Rollback failed 	ress ted
Sites View Deployment History Change Mana	gement Settings			Search			٩
Site Name	Role	Model	Orchestrator Connectivity	Status	Software Version	Export as CSV	Actions
mont	MCN	CBVPX-SE	PRIMARY NOT CONFIGURED 0	ACTIVATED	11.2.2.1003.888	2022-4-26 9:41PM	
site1 (HA)	Branch	CBVPX-SE	PRIMARY ACTIVE ONLINE	ACTIVATED	11.4.2.42.888881 11.4.2.42.888881	2022-4-26 9:41PM 2022-4-26 9:41PM	

Switch to old deployment view

Select this option if you want to switch to the old Deployment page. For more information about the old Deployment page, see Old Deployment View.

Settings

The **Stage All Failed Sites** and **Restore Previous Version** options are available under the **Settings...** menu.

Stage All Failed Sites

When some sites are not staged successfully, select the **Stage All Failed Sites** option to reinitiate the staging process. This option is enabled only when staging fails.

Restore previous version

When you restore the previous version, Citrix SD-WAN Orchestrator service initiates a network-wide activation of the previous configuration and restores the previously activated configuration (and/or

software) on your network. To restore the previous version, on the **Deployment** page, navigate to **Settings** and select **Restore Previous Version**.



A confirmation message is displayed. Click **Proceed** to continue.

0	Warning	
Are yo	u sure you want to Restore previous versio	on ?
	Proceed	Cancel

Note

The Restore previous version action can be performed when the network is not in the staged state. This option is disabled for staged networks.

Deploy now

To initiate the software deployment process on your network, click the **Deploy Now** icon. For detailed information about the deployment workflow see Deployment workflow.

Software and configuration deployment

This section provides a summary of the most recent deployment:

- Last Deployment Summary: Displays the date and time (in UTC time zone) of the last deployment.
- **Software version**: Displays the configured software version and the number of sites running the software version.
- **Configuration changes**: Provides information such as the number of global and site-specific features to which changes were made, and the number of sites that were added and deleted. This column is displayed only if the network contains more than 100 sites.

• **Settings**: Displays the status of other deployment settings such as Ignore incomplete and Rollback.

Important information about Citrix SD-WAN 11.5

Note the following points before you upgrade to Citrix SD-WAN 11.5:

- SD-WAN 11.5.0 release is available only via Citrix SD-WAN Orchestrator service and only on selected geographical POPs.
- SD-WAN Configuration Editor and SD-WAN Center are superseded by Citrix SD-WAN Orchestrator service. Citrix SD-WAN Orchestrator service supports all configurations that are currently done through SD-WAN Configuration Editor.
- Citrix SD-WAN 11.5 is a Limited Availability release, recommended and supported only for specific customers/ deployments.
- SD-WAN 11.5.0 release does not support Advanced Edition(AE), Premium Edition(PE), WAN Optimization deployments
- SD-WAN 11.5.0 supports only the platforms mentioned in SD-WAN platform models and software packages.
- SD-WAN 11.5.0 does not support Citrix SD-WAN Center or Citrix SD-WAN Orchestrator for onpremises.
- SD-WAN 11.5.0 firmware is not available on the Citrix Downloads page.
- Ensure to get the required approvals and guidance from Citrix Product Management / Citrix Support before deploying 11.5.0 on any production network.

Auto-correction for configuration and software upgrade

In Citrix SD-WAN Orchestrator service, the auto-correction feature is implemented as part of the change management workflow.

When the staging fails for a site, and if the site is a control node, you need to restage the site after getting the staging failure message. The **Activate now** option will not be enabled if the staging fails for the control nodes. If the site that has failed staging is a branch node, you are still allowed to proceed 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 now** button has been clicked and stops once the next stage is issued from the Citrix SD-WAN Orchestrator service 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:

- On the Citrix SD-WAN Orchestrator service Deployment page, 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 did not come up with the expected software and configuration version, the Citrix SD-WAN Orchestrator service 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 **Change Management Settings**. This check box is used to control if the device needs to be checked for autocorrection or not. Once the maintenance mode check box is cleared, auto-correction brings the appliance in sync with the network software and configuration version.

Sites view	Deployment History	Ghange Mana	Benjent Settings		
Scheduling Int	formation				
Site Name	HA State	Sc	heduling Information	Maintenance Mode	Actions
site1 (Secondar	y) Standby	20	022-04-14 at 21:20:00 (Maintenance window of 1 hours and repeate		1
site1 (Primary)	Active	20	022-04-14 at 21:20:00 (Maintenance window of 1 hours and repeate		1
mcn1	Not Confi	gured 20	22-04-14 at 21:20:00 (Maintenance window of 1 hours and repeate		1

HA near-hitless software upgrade

Cites Manu

Deployment History Change Management Setting

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 Citrix SD-WAN Orchestrator service 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 in the following scenarios:

- The sites that are deployed in High Availability (HA) mode. It is not applicable for non-HA sites.
- Citrix SD-WAN Orchestrator service-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 Citrix SD-WAN Orchestrator service does not perform HA near-hitless software upgrade and continues to upgrade in the earlier fashion (single-step upgrade). All the sites get rebooted at the same time (if a reboot is required) as part of the single-step upgrade.

The upgrade sequence summary is as follows:

- 1. Citrix SD-WAN Orchestrator service checks for the HA state of all the appliances in the network.
- 2. Upgrades all the secondary appliances that are in the 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 SD-WAN 11.1 release, the Citrix SD-WAN Orchestrator service 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 **Sites View**.

Software and Configuration Deploy	yment					Setting	s Deploy	Now
1. Staging All Sites 0 Mr Swind 0 Swi	2. Activating standby HA devices		3. Active	0/0 • Anteres • Anteres • Anteres • Faired atte Now		4. Rollback Devices	 Authoris in Progress Authoris completed Authoris field 	
Sites View Deployment History Change Manager	ment Settings							
Configuration Changes did not affect 6 sites, whi	ich will receive only a timestamp update.							×
				Sear	rch			Q
							Export.es.CSV	Escot as PDF
Site Name		Role	Model	Orchestrator Connectivity ¥	Status	Software Version	Timestamp	Actions
MCN8100_5084		MON	C86100-SE	Massery NOT CONTINUED (D.,	57420	11.4.2.42.888881	2022-4-2912-35/M	
BR5100_50102		Branch	C85100-PE	PREMITY NOT CONTROLNED (D.,	17420	11.4.2.42.888881	2022-4-2912-35/98	
8RT100_50TT		Branch	CETTOD-PE	Maskin NOT CONTINUED (D.,	NPLANNE	11.4.2.42.888881	2022-4-2912.35/98	
8R110_LTEW/6 (HA)		Branch	CETTO-SE	HIMHEY STANDER ONLINE SECONDARY ACTIVE ONLINE	NOT, MEDID	11.4.2.42.888881 11.4.2.42.888881	2022-4-2912:35PM 2022-4-2912:35PM	
R/1000DesktopMount		Branch	C8R/1000	HIMMAY NOT CONTIGUED (8	NUMBER	11.4.2.42.000001	2022-4-2912:35/4	
SilcomR/80008CoreSiteA (HA)		Branch	C8R/1000	PRIMARY (STANDEY (INUME SECONDARY) ACTIVE (INUME	N/LARDED N/LARDED	11.4.2.42.888881 11.4.2.42.888881	2022-4-2912:35PM 2022-4-2912:35PM	
ClonedR/100DesktopSite		Branch	C8R/1000	PREMIT UNKNOWN OFFLINE	C Staging Pending	10.1.0.154	NA	

In the case of a configuration-only update, only the sites that have configuration changes are staged and activated. For the remaining sites, the timestamp is updated and processed. The control nodes will get a package staged even if there is no change to the site configuration.

If the software version is being changed, both configuration and software package are staged and activated on all the sites in the network.

Sites view

The **Sites View** section provides details about all the devices in the network. The table contains the role of each site, the appliance details, deployment status, Citrix SD-WAN Orchestrator service connectivity status, software version of each appliance, and a timestamp of the running configuration. If the staging process fails at any site, use the **Retry Staging (Primary Device)** option, under the **Ac-tions** column, to reinitiate the staging process. For HA appliances, both the options **Retry staging (Primary device)** and **Retry staging (Secondary device)** are available.

You can export the site view details into a CSV or PDF file by using the **Export as CSV** and **Export as PDF** options. The downloaded CSV and PDF file name is prefixed with **Site List** followed by the date and time of the file export.

Sites View	Deployment I	History	Change Manage	ment Settings					
						Search			Q
								Export as CSV Ex	port as PDF
Site Name		Role	Model	Orchestrator Connectivity	Status		Software Version	Timestamp	Actions
mcn1		MCN	CBVPX-SE	PRIMARY NOT CONFIGURED 0	ACTIVATED		11.4.3.53.888881	2022-4-12 12:45PM	
site1 (HA)		Branch	CBVPX-SE	PRIMARY STANDBY ONLINE SECONDARY ACTIVE ONLINE	ACTIVATED ACTIVATED		11.4.3.53.888881 11.4.3.53.888881	2022-4-12 12:45PM 2022-4-12 12:45PM	ø.
site110		Branch			NOT STARTED				

Deployment history

The **Deployment History** section provides the status of the previous deployment operations and results. If a partial site upgrade is enabled, the section categorizes the sites based on the software version that the appliances are configured to run. If the last activation fails, you can even view details of the failure by clicking the number link on the **Failed** column.

Note

The reason for failed sites details can be viewed only for the most recent activation. It is not available for the older entries in the **Deployment History** table.

Sites View	Deployment	History Change	Management S	ettings					
								Export as C	SV Export as PDF
Deployment date	& time	Software version	Selected sites	Deployment status					
				Activated	Staged	Not Needed	Rolled Back	Offline	Failed
May 2nd 2022, 9:4	12 am	R11_2_2_1003_8888881 R11_4_2_42_888881	1 2	0 1	0	0	0	0	1
Apr 26th 2022, 9:	43 pm	R11_2_2_1003_888881 R11_4_2_42_888881	1 2	1 2	0	0	0	0	0
Apr 13th 2022, 5:4	14 pm	R11_4_2_42_888881	3	э	0	2	0	0	•
Apr 13th 2022, 11:	30 am	R11_4_2_42_888881	3	з	0	0	0	0	0
Apr 13th 2022, 11:	10 am	R11_4_3_53_888881	3	3	0	0	0	0	0
Apr 12th 2022, 5:1	0 pm	R11_4_2_42_888881	3	3	0	0	0	0	0
Apr 12th 2022, 1:1	5 pm	R11_4_3_53_888881	3	1	0	0	0	0	2
Apr 12th 2022, 12:	51 pm	R11_4_3_53_888881	3	з	0	0	0	0	0

Once you click the number link in the Failed column, the **Reason for Failed Sites** page is displayed. This page provides details such as site name, software version, appliance edition, and an error message mentioning the reason for the failure.

Reason for Failed Sites	1				×
Total Sites 1			Search		Q
Site Name	Software Versions	Edition		Error Message	
mon1	11.2.2.1003.888881	SE		Activation Timed Out	

You can export the deployment history details into a CSV or PDF file by using the **Export as CSV** and **Export as PDF** options. The downloaded CSV and PDF file name is prefixed with **Deployment History** followed by the date and time of the file is export.

Change management settings

The **Change Management Settings View** section helps to troubleshoot an appliance manually. Enable the **Maintenance Mode** check box. 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.

Sites View Deploymen	nt History Chang	e Management Settings		
Scheduling Information				
Site Name	HA State	Scheduling Information	Maintenance Mode	Actions
site1 (Primary)	Active	2022-04-20 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 day)		1
site1 (Secondary)	Standby	2022-04-20 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 day)		1
men1	Not Configured	2022-04-20 at 21:20:00 (Maintenance window of 1 hours and repeated every 1 day)		1

Verify configuration

Click **Verify Configuration** at the top right corner of the Deployment page to validate the network configuration and check for any audit error or warning. The **Configuration results** page is displayed.

Configuration	/ Deployment	Verify Configuration Software Version :
Deploym	ent ©	

The configuration results display the total number of audit errors and warnings. The results are also filtered based on the audit type (error or warning) and displayed with different color codes. You can click the numbers links to view the filtered results.

The **Type** column displays an icon to indicate whether it is an error or a warning. The **Audit Scope** column specifies if the error or warning is for a site or at the network level. If the error or warning is specific to a site, then the name of the site is displayed. If the error or warning is at the global level,

then a global error or a global warning is displayed. The **Audit Message** column contains the error code and the error message.

You can use the search bar to search for any specific errors or warnings based on the type, error code, site name, or error message.

× **Configuration results** Search Q 4 4 0 TOTAL MESSAGES ERRORS WARNINGS Туре Audit Scope Audit Message (EC723) At Site 'SantaClara'. Dynamically learned routes will not be imported into Virtual WAN route table since no route SantaClara Δ learning filters exist to include routes. (EC450) in Virtual Path Default Set 'Standard' -> add Rule [Src IP:0.0.0.0/0]Dst IP:20.20.20.0/24]: if Protocol is TCP-based or not Global Warning set, cannot set 'Transmit Mode'='Load Balance Paths' and 'Retransmit Lost Packets'=no. 'Retransmit Lost Packets' has been set ⚠ to yes. (EC723) At Site 'Kansas', Dynamically learned routes will not be imported into Virtual WAN route table since no route learning Δ Kansas filters exist to include routes. (EC450) in Virtual Path Default Set 'test' -> add Rule [Src IP:0.0.0.0/0]Dst IP:20.20.20.0/24]; if Protocol is TCP-based or not set, Global Warning cannot set 'Transmit Mode'='Load Balance Paths' and 'Retransmit Lost Packets'=no. 'Retransmit Lost Packets' has been set to ⚠ yes.

When you click **Verify Configuration** for the second time, the **Configuration results** page displays the same results of the previously verified configuration along with the date and time details. If necessary, you can click **Verify Again** to rerun the validation.

Note

The Verify Configuration button does not display the audit information of site templates.

July 28, 2	2021 4:54 PM	Verify Again X
Search		Q
4 TOTAL MES	ISAGES ERRORS	4 warnings
Туре	Audit Scope	Audit Message
Δ	SantaClara	(EC723) At Site 'SantaClara', Dynamically learned routes will not be imported into Virtual WAN route table since no route learning filters exist to include routes.
Δ	Global Warning	(EC450) in Virtual Path Default Set 'Standard' -> add Rule [Src IP:0.0.0.0/0]Dst IP:20.20.20.0/24]: if Protocol is TCP-based or not set, cannot set 'Transmit Mode'='Load Balance Paths' and 'Retransmit Lost Packets'=no. 'Retransmit Lost Packets' has been set to yes.
Δ	Kansas	(EC723) At Site 'Kansas', Dynamically learned routes will not be imported into Virtual WAN route table since no route learning filters exist to include routes.
Δ	Global Warning	(EC450) in Virtual Path Default Set 'test' -> add Rule [Src IP:0.0.0.0/0]Dst IP:20.20.20.0/24]: if Protocol is TCP-based or not set, cannot set 'Transmit Mode'='Load Balance Paths' and 'Retransmit Lost Packets'=no. 'Retransmit Lost Packets' has been set to yes.

Deployment workflow

The deployment process involves the following stages:

- 1. Software & Sites
- 2. Configuration
- 3. Settings
- 4. Summary
- 5. Stage
- 6. Activate Now

Software and sites

When you click **Deploy Now**, the **Start deployment** > **Software & Sites** page is displayed. Select the default software version that you want to apply to all the sites across the network. To upgrade or downgrade selected sites, use the **Partial site upgrade** option.

Default network software Select the software version for the sites across the network. The software version that you select in the **Default network software** drop-down list gets applied to all the sites unless there are specific overrides configured.

Start deployment					
	Software & sites	Configuration	Settings	Summary	
Appliance Software and Site Selection Select the software version for sites across 1 Default network software * 11.4.2.42-0.A Sites: 1/2 Sites	the network. The default	software version is applied	unless there are site speci	fic overrides configured.	
 Partial Site Upgrade Software Version * Partial Site Upgrade Settings will be applied to the site Sites (I) mon1 	ss listed below		v		Select Siles

Partial site upgrade The **Partial Site Upgrade** option is used to upgrade or downgrade the selected sites with a different version. This option provides the ability to test a new software version on a site before deploying it across the entire network.

With the **Partial Site Upgrade** feature, upgrades can be staggered and thereby reducing the impact of software upgrades during business hours.

Note

Partial Site Upgrade can be performed only when all the sites in the network are running Citrix SD-WAN 11.2.2 software version or above.

Any configuration changes for the Partial Site Upgrade need a change management for the changes to take effect. The Partial Site Upgrade picks the lower version and generates the configuration for the same. Any new features cannot be tested while the network is in the Partial Site Upgrade mode.

When you are downgrading from a newer to older version using the Partial Site Upgrade, if a feature which is supported only in the newer version (with the similar configuration present both in the new and older version), audit errors occur. For example, if a new appliance that only supports a newer version is selected, then audit errors are displayed.

To perform the partial site upgrade:

- 1. Navigate to **Software and Configuration Deployment** > **Deploy Now**. The **Start deployment** page is displayed.
- 2. Select the **Partial Site Upgrade** check box, choose the software version on the **Software Version** drop-down list, and click **Select Sites** to add new sites.

Partial Site Upgrade		
Software Version*		
	\sim	
Partial Site Upgrade Settings will be applied to the sites listed below		Select Sites
Sites (1)		
menl		
Cancel		Previous Next

3. Select the sites and click **Save**.

Site Selector		
rowse or search the list of sites, regions an ubset of its members to add/remove.	d groups below. You can add/remove entire Regions a	nd Groups, or click into them and choose a
earch		
		Q
ilter By Region / Custom Groups		
		· · ·
vailable (2 sites)	Selected (1	sites)
Name	Name	
Branch_2	Branch_1	
MCN_1		
	$\left(\leftarrow\right)$	
Save Cancel		

Configuration

The **Configuration change summary** page provides a diff in between the previously activated configuration and the configuration that you want to deploy now. The diff is displayed in JSON format. This change summary displays both global features and site-specific features.

The previous configuration value appears in red background with a minus symbol and the current configuration value appears in green background with a plus symbol.

Note

The **Configuration change summary** page is displayed only if the network contains more than 100 sites.

When you are done validating the details on the **Configuration** page, click **Next**.

🕤 Start deploym	nt
	Software & sites Configuration Settings Summary
Configuration change sun Summary of configuration ch • 3 Global Features Changed	mary nges performed since last deployment
O Sites Deleted and 0 Sites	4dded
Global Features Site Featu	65
Regions	(
QoE Profile	1 regions: [
Firewall Zones	<pre>2 { 3 allowExternalVipMatch: false, 4 forceInternalVipMatch: false, 5 isDefault: true, 6 name: "", 7 siteNames: [8 - "mcn1", 9 + "site1", 10 - "site1", 11 * "mcn1" 12] 13 } 14 1</pre>
Cancel	Previous Next

Settings

This page offers the following additional deployment options such as Ignore incomplete and Rollback settings.

Ignore Incomplete When the **Ignore Incomplete** checkbox is selected, the offline and the inaccessible sites are skipped during the deployment. The **Activate now** button is enabled immediately after all the online control nodes (MCN, RCN, Geo MCN, Geo RCN) are staged. If the user chooses to activate at this state, the remaining appliances are activated once they complete staging.

The online branch appliances that fail to get staged are ignored. To enable the Ignore incomplete feature, navigate to **Deploy Now** > **Settings** and select the **Ignore Incomplete** check box.

Note

The Ignore incomplete feature can be only enabled or disabled before you start with the deployment. The configuration cannot be changed after the deployment process has started.

🕤 Start deployment				
	0		•	
	Software & sites	Configuration	Settings	Summary
Deployment settings This page includes settings that offer a	dditional control over the dep	ployment process.		
Ignore Incomplete				
Skip offline or inaccessible sites. W	hen the site is online, auto-deploy	the configuration using the last	deployed software version.	
Rollback Settings				
Rollback the sites that fail to conne	ct to SD-WAN Orchestrator service	e to the previous version to rest	ore the connectivity.	
Minimum time that Appliance has to be offline	before triggering Rollback (Minutes)*			
30				

Rollback Settings With the **Rollback Settings** feature enabled, sites that fail to connect to Citrix SD-WAN Orchestrator service post performing network activation (as part of deployment), triggers an automatic rollback to the previous version (last staged package) to restore connectivity.

Note

The automatic rollback is only for the site that failed to connect to Citrix SD-WAN Orchestrator service and not for the entire network.

The rollback feature is triggered only when the appliance loses Citrix SD-WAN Orchestrator service connectivity. It is not triggered in scenarios when the virtual path status goes down and so on.

If at least one site in the network initiates a rollback, a warning message displaying a list of sites that are trying to rollback and an option to initiate a network-wide rollback of all the online sites is shown. You can check the progress of these sites and apply the appropriate action. Start deployment

To enable the rollback on error feature, navigate to **Deploy Now** > **Start Deployment** > **Settings** and select the **Rollback Settings** check box.

Software & sites
Configuration
Settings
Summary

Summary
Software & sites
Configuration
Settings
Summary
S

Select the **Rollback Settings** check box to enable automatic rollback of sites that have failed to connect to Citrix SD-WAN Orchestrator service post activation. Rollback settings can be enabled or disabled before you start the deployment.

When the Rollback setting is enabled, the **Rollback Devices** section with details about the status of the rollback devices is displayed.



For a site to trigger automatic rollback, it must stay offline for at least 30 minutes (currently nonchangeable) post activation. If the site can connect to Citrix SD-WAN Orchestrator service within 30 minutes, then rollback does not get triggered.

Note

Rollback on sites is only performed when the site loses connectivity after activation. Rollback is not triggered in cases where site is online, and activation has failed.

Click **Next** once you set the Rollback settings enabled.

Use case 1: Non-hitless Upgrade A site waits for activation to complete for a specified time with the status as **Activating**.

Software and Configuration Deploy	ment					Setting	Deploy I	Now
1. Staging All Sites 5/6 • Net Stated • Descooling • Singed • Failed	2. Activating standby HA (Activating Activating Activated Failed	3. Activat	0/6	ovices Activiting Activitied Failed	4. Rollback Devices	Rollbook in Progress Rollbook completed Rollbook failed	
Sites View Deployment History Change Managem	ent Settings h will roceive only a timestam	o update.		0				×
					Search		Export as CSV	Export as PDF
Site Name	Role	Model	Orchestrator Connectivity	Status		Software Version	Timestamp	Actions
MCN_CWT_50242 (HA)	MCN	CBVPX-SE	PRIMARY ACTIVE ONLINE SECONDARY STANDBY ONLINE	Activating			2022-5-4 6:45PM 2022-5-4 6:45PM	
BRI_CWT_50149	Branch	CBVPX-SE	PRIMARY NOT CONFIGURED D	Activating			2022-5-4 6:45PM	
BR_CWT_50248 (HA)	Branch	CBVPX-SE	PRIMARY ACTIVE ONLINE SECONDARY STANDRY ONLINE	Activating			2022-5-4 6:45PM 2022-5-4 6:45PM	
ChinaPoCSite	Branch	CBVPX-SE	PRIVARY UNKNOWN OFFLINE	Staging Pendi	ing		N/A	

When the appliance is offline, Citrix SD-WAN Orchestrator service waits for another 30 mins (rollback initiation timeout) to give a chance to the site to connect back. At this stage, the status shows as **Activation Timeout, Waiting to Initiate Rollback (remaining time in minutes)**.

Post the 30 minutes waiting period, the appliance triggers an automatic rollback to the previous configuration or (and) software to try to restore Citrix SD-WAN Orchestrator service connectivity. Citrix SD-WAN Orchestrator service waits for 20 mins (non-configurable setting) for the appliance to connect to Citrix SD-WAN Orchestrator service and during this period, status is shown as **Rollback in progress**.

Software and Configuration Deployment Settings Deploy Now									
1. Staging All Sites	2. Activating standby HA devices		3. Activ	vating the rest of the device 4/5 • Acth • Acth • Fair trace New	es Ming Mici d	4. Rollback Devices	Rol/back in Progress Rol/back completed Rol/back failed		
Sites View Deployment History Change Management Settings Image: Configuration Changes did not affect 2 sites, which will receive only a timestamp update. ×									
				s	learch			Q	
							Export as CSV	Export as PDF	
Site Name		Role	Model	Orchestrator Connectivity	Status	Software Version	Timestamp	Actions	
MCN_CWT_50242 (HA)		MCN	CBVPX-SE	PRIMARY ACTIVE ONLINE SECONDARY STANDRY ONLINE	ACTIVATED		2022-5-4 7:35PM 2022-5-4 7:35PM		
BR1_CWT_50149		Branch	CBVPX-SE	PRIMARY UNKNOWN OFFLINE	Rollback_in_progress		2022-5-4 6:45PM		
BR_CWT_50248 (HA)		Branch	CBVPX-SE	PRIMARY ACTIVE ONLINE SECONDARY STANDBY ONLINE	ACTIVATED ACTIVATED		2022-5-4 7:35PM 2022-5-4 7:35PM		
ChinePoCSite		Branch	CBVPX-SE	PRIMARY UNKNOWN OFFLINE	O Steging Pending		N/A		

If the appliance fails to connect back, in this 20 minute, Citrix SD-WAN Orchestrator service marks the rollback operation as failed and status is shown as **Activation Failed** or **Device Rollback Failed**.

Software and Configuration Deployment						Setting	8Deploy	Now
1. Staging All Sites	2. Activiting standby HA devices	3. Activati	ing the rest of the	Activating Activating Activated Feled	4. Rollback I	0/1	 Rollback in Progress Rollback completed Rollback failed 	
Sites View Deployment History Change Management Setti	ngs eive only a timestamp update.							×
				Search				Q
Site Name	N	Role	Model	Orchestrator Connectivity	Status	Software Version	Export as CSV	Actions
AzureMCN	ИĽ	MCN	CBVPX-SE	PRIMARY NOT COMPLEXIED 0	ACTIVITED		2022-5-5 3:41PM	
BR1100_AlteinMifi		Branch	CB1100-PE	PRIMARY LUNINOVIN OFFLINE	ACTIVATION, FAL		2022-5-5 7:53AM	

In the network, if at least one device has initiated the automatic rollback, a banner is presented to the user as follows:

One (or more) Sites in the Network h restore the connection. To view these Site(s) and take appro You can also select the below operat Ignore Network Rollback	ave lost connectivity to Orchestrator after Activatio priate action <u>Click here</u> isons directly. Rollback entire Network	n and are attempting to Rollback to the previous o	onfiguration or(and) software to try and $$\times$$
Software and Configuration	Deployment		Settings Deploy Now
1. Staging All Sites	2. Activating standby HA devices	3. Activating the rest of the devices 4/5	4. Rollback Devices 0/1 Pollback in Progress Rollback completed Rollback tailed

Based on the status of the network Activation, the options displayed perform the following operations:

- Ignore Network Rollback
 - For non-Hitless upgrade scenario: Ends the current deployment.
- Rollback entire Network
 - For non-Hitless upgrade scenario: Triggers rollback on all the online sites of the network.

You can select the **Click Here** hyperlink to view the list of sites for which rollback is in progress or completed and take the above actions for that page.

You can also wait until the sites that have triggered rollback to either succeed or fail before deciding on triggering the network-wide rollback.

6	Deployment Page								
Θ	The following Sites in the Network have lost connectivity to the Orchestrator as part of this deployment and are attempting to Rollback to try and restore the connection. The following options are available for this deployment, depending on the state of Network activation specified operations are performed : I. Ignore Network Rollback : For non-Hitless upgrade scenario This will end the current Deployment. Second step in Hitless upgrade scenario This will on the current Deployment. For step in Hitless upgrade scenario This will on the current Deployment. For step in Hitless upgrade scenario This will trigger Rollback on all Online sites in the network. For step in Hitless upgrade scenario This will trigger Rollback on all Online sites in the network. For step in Hitless upgrade scenario This will trigger Rollback on all Online sites in the network. Second step in Hitless upgrade scenario This will trigger Rollback on all Online sites in the network. Second step in Hitless upgrade scenario This will trigger Rollback on all Online sites in the network. Second step in Hitless upgrade scenario This will trigger Rollback on all Online sites and devices on the network. Second step in Hitless upgrade scenario This will trigger Rollback on all Online Standby devices in the network. Second step in Hitless upgrade scenario This will trigger Rollback on all Online Standby devices on the network. Second step in Hitless upgrade scenario This will trigger Rollback on all Online Standby devices in the network. Second step in Hitless upgrade scenario This will trigger Rollback on all Online Standby devices in the network. Second step in Hitless upgrade scenario This will trigger Rollback on all Online Standby devices on the operation.							s ×	
1	iearch	Q.	Site 0	Status		HA State		Software Vers	ion c
			No rows fo	und					
	Ignore Network Rollback Rollba	ck ent	ine Natuurk		Showing 1-0 of 0 items	Page 1	of 0	< > 5	rows 🗸

If you select the **Rollback entire Network** option, the following confirmation message is displayed.

🖉 Rollba	ck entire Network	
This operation Note: Near-hitl applicable duri	will trigger a Rollback on all (ess software upgrade for HA ng network rollback Proceed	Online Sites. devices will not be Cancel

Note

The Near-hitless software upgrade for high availability appliance is not applicable in this scenario. That is, if there are any high availability sites in the network, triggering a network-wide rollback activates both the high availability appliances of that site at once which can cause some network downtime.

Click **Proceed** to start the network-wide rollback on all the online sites.

Use case 2: Hitless Upgrade In the case of Hitless upgrade, the standby appliances would be activated first followed by the active and non-high availability appliances.

As part of the first step if the standby appliance goes offline post activation and initiates a rollback, the following options are available:

• Ignore Network Rollback

- **For Hitless upgrade scenario**: Ignore the standby appliances which are offline and proceed with the activation of the active appliances.
- First step in Hitless upgrade scenario: Deployment proceeds to second step of Activation.
- Second step in Hitless upgrade scenario: Ends the current deployment.
- Rollback entire Network
 - **For Hitless upgrade scenario**: Rollback all the online standby appliances which have completed the activation and end the ongoing deployment. No activation of active and non-high availability appliance is done in this case.
 - **First step in Hitless upgrade scenario**: Triggers rollback on all online standby devices in the network.
 - Second step in Hitless upgrade scenario: Trigger rollback on all online sites (active and standby). Near-hitless software upgrade for high availability devices is not applicable in this scenario.

The next step of the hitless upgrade that is activation of active and non-high availability appliance, the same rollback on error workflow is followed as mentioned in Use case 1: Non-hitless Upgrade. In this scenario, if you choose **Rollback entire Network**, the rollback triggers for all the (both active and standby) appliance.

Once the site completes rollback and connects back to Citrix SD-WAN Orchestrator service, the status for that site shows **Rolledback** and the sites are online.

Software and Configuration Deployment Settings Deploy Now										
1. Staging All Sites 5/6 • Not Started • Downleading • Stagen • Stagen • Stagen • Stagen • Stagen • Stagen • Started • Started • Downleading • Stagen • Started • Stare	2. Activating standby HA devices			vating the rest of the dev 0 / 1	vices Activating Activated Pailed	4. Rollback Devices 5/5 Rollback in Programs Rollback completed Rollback failed				
Sites View Deployment History Change Management Settings Image: Configuration Changes did not affect 2 sites, which will receive only a timestamp update. ×										
					Search			Q		
							Export as CSV	Export as PDF		
Site Name		Role	Model	Orchestrator Connectivit	y Status	Software Version	Timestamp	Actions		
MCN_CWT_50242 (HA)		MCN	CBVPX-SE	PRIMARY ACTIVE ONLINE SECONDARY STANDBY ONLIN	ROLLEDBACK ROLLEDBACK		2022-5-4 7:35PM 2022-5-4 7:35PM			
BR1_CWT_50149		Branch	CBVPX-SE	PRIMARY NOT CONFIGURED O	ROLLEDBACK		2022-5-4 6:45PM			
BR_CWT_50248 (HA)	Branch	CBVPX-SE	PRIMARY ACTIVE ONLINE SECONDARY STANDBY ONLIN	ROLLEDBACK ROLLEDBACK		2022-5-4 7:35PM 2022-5-4 7:35PM				
ChinaPoCSite	Branch	CBVPX-SE	PRIMARY UNKNOWN OFFLINE	O Staging Pending		N/A				

Limitation Autocorrection for rolling back or rolled back appliances and network is not supported.

Note

Automatic site rollback is only a backup mechanism to try and restore the lost connectivity to Citrix SD-WAN Orchestrator service. If the appliance still fails to connect to Citrix SD-WAN Orchestrator service, check the network configuration of this appliance.

Summary

The **Summary** section provides details of the deployment settings applied on the **Software & Sites**, **Configuration**, and **Settings** pages. When you are done validating the details on the **Summary** page, click **Deploy**. You are redirected to the **Software and Configuration Deployment** section.

Start deployment					
	Software & siles	Configuration	Settings	Summary	
Deployment summary Offers a quick at-a-glance summary of all the	parameters selected for th	e admin to review before initia	ting deployment		
Software version and sites		Configuration chan	ges		Settings
 11.4.2.42-GA (Default) 	2 Sites	 3 Global Feature 0 Sites Deleted a 	is Changed and 1 Sites Added		Rollback: Disabled Ignore Incomplete: Disabled

Stage

Once the verification is successful and you click **Deploy** on the **Summary** page, the staging process where the configuration files are distributed to all the appliances and sites on your network is automatically triggered. By default, Citrix SD-WAN Orchestrator service waits for all the Control nodes (MCN, RCN, Geo MCN, Geo RCN) and the online branch appliances to get staged before allowing the user to activate them. In the **Staging All Sites** section, you can view the progress of the staging. The phases of the staging displayed in this section are **Not started**, **Downloading**, **Staging**, **Staged**, and **Failed**. Each phase is represented with a unique color code. The donut chart provides a real-time update about the status of the staging.

If the staging process fails at any site, use the **Retry Staging (Primary Device)** option, under the **Sites View > Actions** and reinitiate the staging process. For HA appliances, both the options **Retry staging** (**Primary device**) and **Retry staging (Secondary device**) are available.

Software and Configuration	Settings Deploy Now	
1. Staging All Sites	2. Activating standby HA devices 0/0 • Activating • Activated • Failed	3. Activating the rest of the devices 3/3 Activating Activated Failed
Stage		

Activate now

Click **Activate Now** in the **Activating the rest of the devices** section to activate the staged configuration on all the sites across the network.

Each phase of activation is represented with a unique color code.

- Activating standby HA devices: This chart provides a real-time update about the standby appliances for SD-WAN devices that are deployed in High Availability mode. To guard against software failure of the SD-WAN instance, you might choose to deploy the instance in high availability mode which deploys two SD-WAN instances in active standby mode. Citrix recommends deploying instances in high availability mode for production networks.
- Activate the rest of the devices: This chart provides a real-time update about the SD-WAN standalone appliances and the previously active appliances that have switched over to standby mode. In Standalone mode, a single SD-WAN instance is deployed. If the SD-WAN instance fails due to either an issue with the SD-WAN firmware or the underlying Azure infra you cannot reach out to the resources deployed behind the SD-WAN instance in Azure. In other words, the instance behaves in a fail to block mode.

For more information about Standalone and High Availability modes, see Deployment use cases.

When the Rollback settings feature is enabled, an extra section **Rollback Devices** is displayed. For more information on Rollback, see Rollback Settings.



Inter-link communication

March 8, 2022

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 a service provider, and
- Any two Private Intranet links that share a 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.

Defaul	Verify Config Interlink Communica	tion
Delaul	t inter-link communication Groups	
lo	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
Custor	n Inter-link Communication Groups	
Custor PLS Gro	n Inter-link Communication Groups Dups Private Intranet Groups	Internet Communication Override Groups
Custor PLS Gro	n Inter-link Communication Groups <u>pups</u> Private Intranet Groups ne desired MPLS service provider na	Internet Communication Override Groups ames, to enable the corresponding links to talk to each other.
Custor PLS Gro Dup th + M	n Inter-link Communication Groups Private Intranet Groups te desired MPLS service provider na PLS Inter-link Communication Gro	Internet Communication Override Groups ames, to enable the corresponding links to talk to each other.

- 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 the encryption for every custom MPLS Inter-Link Communication Group. In rare cases, to eliminate the overhead of encryption, you can disable this option.
- **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 encryption 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 Interlink 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 dropdown list. The **Enable Encryption** option ensures that the packets of the Inter-Link Communication Group which are sent on the virtual paths are encrypted.

	Verify Config Interlink Communication	
Defau	It 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
з	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
Custo	m Inter-link Communication Groups	
MPLS Grou	ıp Name *	DSCP Tag
+ N	IPLS Provider	
Car	ncel Save	

DNS and DHCP

October 27, 2021

This section enables you to configure DNS and DHCP settings.

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 an internal, ISP, google or any other open source DNS service.

Verify Config	DNS Servers	
DNS Service		
DNS Service Name *	Туре	
Eg: dns_service1	Static	\sim
Primary DNS *		Secondary DNS
Eg: a.b.c.d		Eg: a.b.c.d
Cancel Sa	ve	

Click Verify Config to validate any audit error.

You can also configure DNS server settings for a site. Select a site from the **Select Site** drop-down list and click **Go**. This takes you to the site level DNS server settings page.

DNS 0

+ DNS	Service			
No	DNS Service Name	Primary DNS	Secondary DNS	Actions
Note: DNS F from below	Proxy & Forwarder set dropdown and click G	tings are available as o. This will take you te	part of site config. Plea o site level page	ase choose a site
Select Site:	branchvpx V	Go		

DHCP

You can configure dynamic host control protocol (DHCP) settings for a site by selecting the required site from the drop-down list and clicking **GO**. This takes you to the site level DHCP configuration page. For detailed information on configuring DHCP, see DHCP.

DHCP	<i>(i)</i>		
Note: DHCP	settings are ava	ilable	as part of site config. Please choose a site from below dropdown and click Go. This will take you to site level page
Select Site:	branchvpx	\sim	Go

Site and IP Groups

November 24, 2021

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.

	erify Config Regions		
+ Regio	Region	Sites	Artions
	Default-Region	0	+ m
0	Region-US-WEST	0	+ 🖻
	Region-US-EAST	0	+ 🖻

Currently, a maximum of 1000 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.

Region Attributes		
egion Name: Region- US-WEST		
Description		
	4	
Force Internal VIP Matching	Allow External VIP Matching	
+ Subnets		
Network	Delete	
Eg: a.b.c.d/e	Ŵ	
Import Sites from other Regions	Search Sites Search	
Select Regionish to import nom	Select Sites to be imported	
Select All		
Select All Default-Region		
Select All Default-Region		
Select All Default-Region		
 Select All Default-Region 		
 ✓ Select All ✓ Default-Region 		
 Select All Default-Region 		
 ✓ Select All ✓ Default-Region 		
 Select All Default-Region 		

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.

Verify Config Custom Groups		
+ Custom Group		
Group	Sites	Actions
Group-Large Branch Offices	3	+ 💼
Group-Large Branch Office	3	+ 💼
Group-Europe	3	+ 💼
	2	+ =
Group-G1	2	

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**.

Group Attributes		
Group Name: Group- site1		
Sites		
	Coords	
• + Sites Search Sites	Search	
Select Group(s) to pick from	Select Sites to be Added	
✓ Select All	Select All	
Default-Region	Bangalore	
Region-Main_Office	Belgium	
Region-Sales_office	London	
Group-Large Branch O	Madrid	
Group-Large Branch O	NewYork	
Group-Europe	San Francisco	
Group-G1		
Group-test_group		

Click Verify Config to validate any audit error.

IP groups

Citrix SD-WAN Orchestrator service introduces the option of adding IP groups (network objects). With this option, you can group IP and network addresses by using **IP Groups** while defining a route filter rather than creating a filter for each subnet. These groups can be used in configuration and policies as needed, without necessarily having to key in individual IP addresses each time.

IP Groups ③

+ IP Group	
ie .	Actions
CN-GROUP1	۵
1_GROUP1	
3R2_Group1	÷

You can create IP groups and add network addresses and prefixes. 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.

IP	Gro	oups	Ť
IP	GIC	ups	0

IP Group Identifiers		
IP Group Name "		
IP Addresses		
+ IP Address		
Network Address/Prefix		
	-	
Cancel Save		

Click Verify Config to validate any audit error

The following features utilize the IP groups:

• **Creating an IP route**: You can add a destination network or enable the **Use IP Group** check box to select an existing IP group. For more information, see IP groups.

Verify Config 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 Any Any ✓
Scope
Global Route Site / Group Specific Route
Traffic Steering
Delivery ServiceCost*Internet Breakout5
Eligibility Criteria
Export Route
Cancel Save

• **Import route profiles**: While creating an import filter profile, you can choose from the list of IP groups available on your network.

You can add a destination network or enable the **Use IP Group** check box to select an existing IP group.

For more information, see Import route profiles.

import Profile Name *								
Sample-import-filter	-profile							
Import Filters								
Protocol Routing Dor	nain	Source Router	Destination IP	Use IP Group	Prefix	Next Hop	Route Tag	
Any 🗸 Default_	RoutingDomain	*	*		eq ~ *	*	*	
✓ Include	🖌 Export R	oute to Citrix SD-WAN A	opliances					
Citrix SD-WAN Cost*	Service Type							
6	Local	\sim						
Cancel	Done							
Profile Availability								
			d balance					
mport Filter Profile Se	ettings will be a	pplied to the sites liste	a below				Select Sites	
Sites (2)								
-								

• **Export route profiles**: While creating an export filter profile, you can add a network address mask or enable the **Use IP Group** check box to select an existing IP group.

For more information, see Export route profiles.

Verify Config Export Route Profiles				
Export Filter Profile				
Export Profile Name *				
sample-export-filter-profile				
Export Filters				
Routing Domain Network Address/Mask 🗹 Use IP Group	Prefix	Cost	Service Type	Gateway IP Address
Default_RoutingDomain v ipg1 v	eq 🗸 *	eq 🗸 *	Local 🗸	*
Export OSPF Route Type Export OSPF Route Weight	Include			
Type 5 AS External \checkmark Weight				
Cancel Done				
Profile Availability				
Export Filter Profile Settings will be applied to the sites listed below			Select Sites	
Sites (1)				
Boston				

• **BGP neighbor policies**: While adding a configured BGP policy for neighboring routers, you can add a network address or enable the **Use IP Group** check box to select an existing IP group.

For more information, see BGP.

BGP Import Filters	Export Filters			
Neighbor Information				
Routing Domain*	Virtual Interface*		Neighbor IP *	
Default_RoutingDomain	×	~		
Neighbor AS *	Hold Time *	Local Preference *	Password	
1	180	100		٩
1 IGP Metric Multi Hop Neighbor Policies	180	100		٩
1 IGP Metric V Multi Hop Neighbor Policies Order	180 Network Address Use IP Group	100 Community String list	BC	@ 3P Community(AA:NN)
1 IGP Metric V Multi Hop Neighbor Policies Order 100	Network Address Use IP Group *	100 Community String list Manual	BC ×	@ P Community(AA:NN) *
1 ✓ IGP Metric ✓ Multi Hop Neighbor Policies Order 100 AS Path	180 Network Address Use IP Group * BGP Policy*	100 Community String list Manual	BC V Tirection	@ SP Community(AA:NN)

Application settings and groups

June 8, 2022

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 **Application Groups**, navigate to **Configuration > App Settings & Groups**.

Domains and applications

You can create internal applications based on domain names which are not available in the list of published applications from the **Domains & Apps** page. To create applications based on domain name, at the network level, navigate to **App Settings & Groups > Domains & Apps > Domain Name Based Apps** tab, and click **New Domain Name Based Application**. Enter the application name and add the domain names or patterns. You can either enter the full domain name or use wild cards at the beginning.

2	
	Delete
	Ē
	Ē

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

From Citrix SD-WAN 11.4.2 release onwards, the **Configure Ports** check box option is made available under **Domain Name Based Applications**. When the **Configure Ports** check box is enabled, it presents the flexibility to configure a group of multiple ports, port-ranges, and a protocol (TCP/UD-P/Any) for the domain-based application.

Previously, ports **80** and **443**, and protocol **Any** were supported for domains grouped under an application. You can see the same behavior if the **Configure Ports** check box is cleared. By default, the **Configure Ports** check box is disabled. When you select the **Configure Port** check box, you can edit, add, or delete any port or the port range as required along with the protocol selection as TCP, UDP, or Any. By default, the protocol value is set to **Any** and the ports are set to **80** and **443**.

omain Name Based Apps	Pre-classified Apps	
Domain based App Name *		
Ecommerce		
✓ Configure Ports		
Select Protocol		
ТСР	~	
Add Ports		
Port / Port Range		Delete
20		Ē
80		
443		Ē
500-4000		
Add Domains		
Domain Name/Pattern		Delete
www.amazon.com		Ē
		Ē

You can also view the list of pre-defined applications under the **Pre-classified Apps** tab. You can
search for a specific application using the **Search** bar or filter the list based on the application family.

Domains & Apps ④		
Domain Name Based Apps Pre-cla	ssified Apps	
Filter Based on App Family:		✓ Search C
App Name	App Family	Description
Base virtual protocol	Standard	Base is a virtual protocol, specific to ixEngine, that is always present at the beginning of the protocol path (e.g. ba
Unclassified Protocol	Standard	Unclassified is a virtual protocol created for DPI that represents flows that are not recognized by the system. Mos
Malformed virtual protocol	Standard	A packet belongs to the protocol 'malformed' if the protocol announced by the lower level protocol does not corre
Incomplete virtual protocol	Standard	Incomplete is used when the protocol signature is too long.
802.1Q Ethernet VLAN	Network Service	802.1Q is a protocol which allows sending VLAN membership information of a frame.
AOL Instant Messenger (formerly O	Instant Messaging	AIM (originally AOL Instant Messenger) is an instant messaging application. The protocol name is OSCAR (Open S
Advance Message Queuing Protoco	l Middleware	AMQP (Advanced Message Queuing Protocol) is an open standard application layer protocol for message-oriente
Apollo Domain:XEROX	Routing	Apollo is the routing protocol implemented natively in Apollo workstations.
Address Resolution Protocol	Network Service	The ARP protocol is used to determine the MAC Address of a PC for which the IP address is known.
AppleTalk	Network Service	The AppleTalk Protocol Suite implements services for routing, file transfer, printer sharing and emails in Apple en
		Showing 1-10 of 3585 items Page 1 of 359 4 🕨 10 rows 🗸

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 based on the IP protocol that can be used in multiple policies as needed, without referring the IP address and port number details each time.

To create a custom application, at the network level, navigate to **App Settings & Groups > Custom Apps**, 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.

Verify Config	Custom Apps				
Custom App Name*					
HTTP_SERVER_INT	ERNAL				
Reporting Priority					
Match Criteria					
Add Match Crite	eria				
Application	Protocol	Network IP	Port	DSCP	Actions
Any	TCP (6)		80	DEFAULT	1
Cancel	Save				

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 and application groups. You must select the **Enable Reporting** check box and provide the reporting priority.

When the **Enable Reporting** check box is selected, you can view the IP custom application traffic under **Reports** > **Usage**.

Reporting priority is the order in which IP protocol-based custom applications or application groups are selected for the reporting. It helps to choose the high-priority custom application or application group for reporting, when there are multiple matches with reporting enabled. For example, if the reporting priority of a custom application is set to 1, it means that the custom application gets the highest priority in reporting. Whereas if the reporting priority is set to 100, the custom application takes a much lesser precedence in reporting.

etwork	Reports: Usage	2		Relative	Fime 🗸 Interval:	Last 1 Hour	✓ Site Gro	up: Al	l v
Ap	oplication Usage Ne	twork Usage							
Report Ty	npe Apps ~	Apps All	~						
				Top Applications					
■ нт Тор	TTP_SERVER_INTERN#	AL (94%) 🛑 youtube (6%) 📕 amazon (0%)	salesforce (0%)	STREAMING (0%) 🔳	Others (0%)	Search		Q
	TTP_SERVER_INTERNA	AL (94%) 🛑 youtube (Total Data	6%) 💼 amazon (0%) Upload Data	salesforce (0%)	STREAMING (0%)	Others (0%) Upload Ban	Search	Download	Q. Bandwidth
Top No 1	TTP_SERVER_INTERNA p Applications Applications HTTP_SERVER_IN	AL (94%) 🛑 youtube (Total Data 10.13 GB	6%) a amazon (0%) Upload Data 3.42 GB	Download Data 6.71 GB	STREAMING (0%) Total Bandwidth 82.94 Mbps	Others (0%) Upload Band 26.82 Mbp	Search dwidth	Download 56.12 Mil	Q Bandwidth pps
■ H1 Top Nº 1 2	TTP_SERVER_INTERNA p Applications Applications HTTP_SERVER_IN youtube	AL (94%) voutube (Total Data 10.13 GB 638.21 MB	6%) amazon (0%) Upload Data 3.42 GB 218.21 MB	Download Data 6.71 GB 419.99 MB	STREAMING (0%) Total Bandwidth 82.94 Mbps 1.49 Mbps	Others (0%) Upload Band 26.82 Mbp 510.32 Kb	Search Iwidth DS DS	Download 56.12 Mi 982.19 k	Q. Bandwidth bps
■ H1 Top No 1 2 3	P Applications Applications HTTP_SERVER_IN youtube amazon	AL (94%) youtube (Total Data 10.13 GB 638.21 MB 17.12 MB	6%) ■ amazon (0%) Upload Data 3.42 GB 218.21 MB 6.06 MB	Download Data 6.71 GB 419.99 MB 11.06 MB	STREAMING (0%) Total Bandwidth 82.94 Mbps 1.49 Mbps 129.54 Kbps	Others (0%) Upload Ban 26.82 Mbr 510.32 Kb 47.23 Kbp	Search twidth DS S S	Download 56.12 MI 982.19 K 82.31 Kb	Q Bandwidth bps ps
H1 Top No 1 2 3 4	TTP_SERVER_INTERNA p Applications Applications HTTP_SERVER_IN youtube amazon salesforce	AL (94%) youtube (Total Data 10.13 GB 638.21 MB 17.12 MB 5.49 MB	6%) amazon (0%) Upload Data 3.42 GB 218.21 MB 6.06 MB 2.51 MB	salesforce (0%) Download Data 6.71 GB 419.99 MB 11.06 MB 2.98 MB	Total Bandwidth 82.94 Mbps 1.49 Mbps 129.54 Kbps 12.4 Kbps	Upload Bann 26.82 Mbp 510.32 Kb 47.23 Kbp 5.68 Kbps	Search width ps s	Download 56.12 MI 982.19 k 82.31 KL 6.72 Kbp	Bandwidth pps bps ps ps
► H1 Top No 1 2 3 4 5	TTP_SERVER_INTERNA p Applications Applications HTTP_SERVER_IN youtube amazon salesforce STREAMING	Total Data 10.13 GB 638.21 MB 17.12 MB 5.49 MB 4.27 MB	6%) amazon (0%) Upload Data 3.42 GB 218.21 MB 6.06 MB 2.51 MB 2.05 MB	salesforce (0%) Download Data 6.71 GB 419.99 MB 11.06 MB 2.98 MB 2.22 MB	Total Bandwidth 82.94 Mbps 1.49 Mbps 129.54 Kbps 12.4 Kbps 11.61 Kbps	Upload Bann 26.82 Mbp 510.32 Kb 47.23 Kbp 5.68 Kbps 5.58 Kbps	Search twidth ps s	Download 56.12 MI 982.19 K 82.31 Kb 6.72 Kbp 6.03 Kbp	Q Bandwidth bps bbps bs bs bs
■ H1 Top No 1 2 3 4 5 6	TTP_SERVER_INTERNA p Applications Applications HTTP_SERVER_IN youtube amazon salesforce STREAMING http2	AL (94%) youtube (Total Data 10.13 GB 638.21 MB 17.12 MB 5.49 MB 4.27 MB 1.89 MB	6%) amazon (0%) Upload Data 3.42 GB 218.21 MB 6.06 MB 2.51 MB 2.05 MB 660.48 KB	salesforce (0%) Download Data 6.71 GB 419.99 MB 11.06 MB 2.98 MB 2.22 MB 1.22 MB	STREAMING (0%) Total Bandwidth 82.94 Mbps 1.49 Mbps 129.54 Kbps 12.4 Kbps 11.61 Kbps 24.37 Kbps	Upload Band 26.82 Mbp 510.32 Kb 47.23 Kbp 5.68 Kbps 5.58 Kbps 8.77 Kbps	Search width DS S S	Download 56.12 Mi 982.19 K 82.31 Kb 6.72 Kbp 6.03 Kbp 15.6 Kbp	Q Bandwidth bps bps bps bs bs bs ss ss
Top No 1 2 3 4 5 6 7	TTP_SERVER_INTERNA p Applications Applications HTTP_SERVER_IN youtube amazon salesforce STREAMING http2 ECOMMERCE	AL (94%) youtube (Total Data 10.13 GB 638.21 MB 17.12 MB 5.49 MB 4.27 MB 1.89 MB 1.89 MB 1.85 MB	6%) amazon (0%) Upload Data 3.42 GB 218.21 MB 6.06 MB 2.51 MB 2.05 MB 660.48 KB 660.48 KB	salesforce (0%) Download Data 6.71 GB 419.99 MB 11.06 MB 2.98 MB 2.22 MB 1.22 MB 1.18 MB	Total Bandwidth 82.94 Mbps 1.49 Mbps 129.54 Kbps 12.4 Kbps 11.61 Kbps 24.37 Kbps 95.09 Kbps	Upload Ban 26.82 Mbp 510.32 Kb 47.23 Kbp 5.68 Kbps 8.77 Kbps 12.95 Kbp	Search Width DS S S	Download 56.12 MI 982.19 k 82.31 Kb 6.03 Kbj 15.6 Kbp 81.14 Kb	Q Bandwidth bps bps bs bs bs bs bs bs bs bs bs
Top No 1 2 3 4 5 6 7 8	TTP_SERVER_INTERNA p Applications Applications HTTP_SERVER_IN youtube amazon salesforce STREAMING http2 ECOMMERCE google_accounts	AL (94%) youtube (Total Data 10.13 GB 638.21 MB 17.12 MB 5.49 MB 4.27 MB 1.89 MB 1.89 MB 1.85 MB 1.61 MB	6%) amazon (0%) Upload Data 3.42 GB 218.21 MB 6.06 MB 2.51 MB 2.05 MB 660.48 KB 660.48 KB 667.14 KB 545.11 KB	salesforce (0%) Download Data 6.71 GB 419.99 MB 11.06 MB 2.98 MB 2.22 MB 1.22 MB 1.18 MB 1.07 MB	Total Bandwidth 82.94 Mbps 1.49 Mbps 129.54 Kbps 124.45 Kbps 12.45 Kbps 12.45 Kbps 95.09 Kbps 95.09 Kbps 42.97 Kbps	Upload Ban 26.82 Mby 510.32 Kb 47.23 Kbp 5.68 Kbps 8.77 Kbps 12.95 Kbp 14.53 Kbp	Search twidth ps s s s s	Download 56.12 MI 982.19 K 82.31 Kb 6.03 Kb 15.6 Kb 81.14 Kb 28.44 KI	Bandwidth bps bss bss
■ HT Top No 1 2 3 4 5 6 7 8 9	TTP_SERVER_INTERNA p Applications Applications HTTP_SERVER_IN youtube amazon salesforce STREAMING http2 ECOMMERCE google_accounts google_ads	AL (94%) youtube (Total Data 10.13 GB 638.21 MB 17.12 MB 5.49 MB 4.27 MB 1.89 MB 1.89 MB 1.85 MB 1.61 MB 1.55 MB	6%) amazon (0%) Upload Data 3.42 GB 218.21 MB 6.06 MB 2.51 MB 2.05 MB 660.48 KB 667.14 KB 545.11 KB 667.3 KB	salesforce (0%) Download Data 6.71 GB 419.99 MB 11.06 MB 2.98 MB 2.22 MB 1.22 MB 1.18 MB 1.07 MB 877.85 KB	Total Bandwidth 82.94 Mbps 1.49 Mbps 129.54 Kbps 12.4 Kbps 11.61 Kbps 24.37 Kbps 95.09 Kbps 42.97 Kbps 4.07 Kbps	Upload Bane 26.82 Mbp 510.32 Kb 47.23 Kbp 5.58 Kbps 8.77 Kbps 12.95 Kbp 14.53 Kbp 1.76 Kbps	Search Awidth DS S S S S	Download 56.12 MI 982.19 K 82.31 KE 6.72 Kbp 6.03 Kbp 15.6 Kbp 81.14 Kb 28.44 KI 2.3 Kbp	Bandwidth bps bbps bs ss ss ss ss ss ss ss ss ss ss ss ss

Note

- For you to use a domain name-based application, **Apps & Domains** must be listed as the match criteria while creating the Application Route, QoS policy, and firewall policy.
- For you to use a custom application, **Custom Application** must be listed as the match criteria while creating the Application Route, QoS policy, and firewall policy.

Once you have created the custom application, to perform the application routing, navigate to **Routing Policies > + Application Route**, select **Custom Application** from the **Match Type** dropdown list. Similarly for the domain name-based application, select **Apps & Domains** from the **Match Type** drop-**Type** drop-down list.

st Ranges: Custom Application (1-20)	Application (21-40) App	lication Group (41-60)	IP (1-65535)	
Apps & Domains Match Criteria				
tch Type	Apps & Domains *	<u>+New Domain App</u>	Routing Domain	
Apps & Domains \checkmark	ecom	\sim	Any 🗸	
Scope	DrukNet.bt (Bhutan Telecom) Bhutan Telecom (bt.bt)			
Global Route 🔷 Site / Group Spec	Manx Telecom Cif Chunghwa Telecom			
Traffic Steering	Empresa de Telecomunicacio Earthlink Telecom	nes de Cuba S.A.		
livery Service	Ecommerce			

You can also select a domain name-based application under the match criteria while creating an **IP Protocol** custom application.

Verify Config Cust	tom Apps				
Custom App Name*					
Enable Reporting Reporting Priority					
Match Criteria					
Application	Protocol	Network IP/Prefix	Port	DSCP	
Ecommerce	Any	*	1-2	any	\sim
Cancel Done					

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 **Custom Application** from the **Match Type** drop-down list. To view the domain name-based application, select **Apps & Domains** from the **Match Type** drop-down list.

Firewall Policies

Policy Information	
Policy Name * FIREWALL-12	Active Policy
Firewall Type	
Built-in Firewall	\sim
Match Criteria	
Match Type	Routing Domain
Apps & Domains	\sim Default_RoutingDomain \sim
Apps & Domains * + New Di	omain App
Filtering Criteria	
Source Zone	Destination Zone

You can view the domain name-based custom applications both under **Global or Site/Group Specific Rule**. To view the domain name-based applications, navigate to **QoS > QoS Policies > Global Rules > Application Rule > + Application Rule**, and select the required domain name-based application from the **Apps & Domains** drop-down list. To view custom applications, navigate to **QoS > QoS Policies > Global Rules > Custom Application Rules > + Custom Application Rule**, and select the required custom application from the **Custom Application** drop-down list.

main
~
Src = Dest
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.

App Groups ③	
+ Application Group	
Application Group Name	Actions
O365Optimize_InternetBreakout	â
Citrix_Cloud_and_Gateway_service	Ê
test	Ê

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.

Actions
۵
ė.
ŵ

Click Verify Configuration on the Configuration > App Settings and Groups > App Groups page to validate any audit error.

App Groups ①	
+ Application Group	
Application Group Name	Actions
03650ptimize_InternetBreakout	8
Otrix_Cloud_and_Gateway_service	8
test	

Application quality profiles

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

•	Dashboard	
<u>.11</u>	Reports	>
\$	Configuration	~
	Delivery Services	>
	Routing	>
	Link Settings	>
	QoS	>
	Security	>
	Site & IP Groups	>
	App & DNS Settings	~
	Custom Apps	
	App Groups	
	App Quality Profiles	
	App Quality Config	
	DNS Servers	

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 that 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.

Verify Config	App Quality Config		
Application OoF Cor	nfiguration		
Type *	Application *	QoE Profile *	
Type* Application	Application *	QoE Profile *	>

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.

work Rep	orts: App	lication Qu	ality 🖸							Relative Time \lor	Interval:	Last 30 Mins \lor	Site Group:	All
ation Qoe App / App Gr	oup	Search Applica	tions	Q										
2 Total Apps	2 Good	0 Fair	0 Poor	O No Traffic										View by:
Salesforc	e			Avg QoE: 9,1/10	STREAM	ING			Avg QoE: 9,44/10	1				
2 Total Sites	0 Poor	0 Fair	2 Good	0 Inactive	2 Total Sites	0 Poor	0 Fair	2 Good	O Inactive					

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 Citrix SD-WAN Orchestrator service UI, at the network level, navigate to **Configuration** > **App Setting & Groups** > **Proxy Auto Config** and click + **PAC file profile**.

Verify Config Proxy Auto Config	
Profile Information	
Profile Name *	PAC File URL*
PAC1ht	http://www.testpac.com/test.pac
Select Site(s)	
Proxy Auto Config Settings will be applied to the s	ites listed below Select Sites
Sites (2) Boston Dallas	
Cancel Save	

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.

DPI 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 Settings & Groups > DPI Settings** and clear the **Enable Global DPI** check box option.

Verify Config Application Settings	
Global Application Settings	
Site Overrides Application Settings will be applied to the sites listed below	
Sites (1) Boston	Select Sites

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.

Profiles and Templates

June 28, 2022

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 profiles

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.

	Dashboard	Network Configuration : Profiles & Templates	í.	
<u></u>	Reports >	Profiles Templates		
\$	Configuration 🗸			
	Network Config Home			
	Delivery Services	Site Profiles	<u>@</u>	
	Routing	+ Site Profile		
	Virtual Path Settings	Site Profile Site Count	Actions	
	QoS Policies	test Q / 6	• ^	
	Security	Internetsite Q / 6		
	Region, Site & IP Groups	testdhcp <u>0</u> /6		
	Application & DNS Settings	Test_service <u>0</u> /6		
	Profiles & Templates		~	

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.

:	ite Profile	×
	Create New Use a Profile	
	Cancel Done	

To create a site profile, you need to configure the **Site Details**, **Interfaces**, and **WAN Links**. For detailed description of configuring sites, see <u>Site</u> details.

Provide the device details.

5			Q
			Ø
ice Edition*	Sub-Model *	Site Role *	Q
SE	BASE	∼ Branch	
ni	ce fultion * SE	ce Edition* Sub-Model* SE V BASE	ce Edition* Sub-Model* Site Role * SE V BASE V Branch

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		Ø
Deployment Mode * Interface Type *	Security* Interface Name	
Edge (Gateway) V LAN V	Irusted V LAN-1	
Physical Interface		?
Select Interface 1 2 3 4 5 6 7 8	LSP	
Virtual Interfaces		0
VLAN ID *	Virtual Interface Name	
0	VIF-2-LAN-1	
Routing Domain *	Firewall Zones	
Default_RoutingDomain ~	<default></default>	\sim
		Save
Cancel		

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

For detailed description of configuring WAN links, see WAN links.

WAN Link Attributes					0
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	ı				
Access Interfaces					0
Add Access Interface					
Name	Virtual Inter	face	VIF Path Mode	Actions	
AIF-1	VIF-Bridge	-1-VLAN-0	Primary	Π.	
Advanced WAN Options					
Active MTU detect Enable	Metering				
Longestion Threshold (µs)		Provider ID		Frame Cost (Bytes)	
Standby Mode		Tunnel Header Size		MTU (Bytes)	
	~				
				Standby Heartbeat Interval	
Priority		Active Hearteat Interval		,	

Templates

Citrix SD-WAN Orchestrator service allows you to use templates as a predefined set of fields to configure a new site or a WAN link.

Site template

A site template is a predefined template used for site creation. To configure a site using a predefined site template, at the customer level, navigate to **Configuration** > **Profiles & Templates** > **Templates**. In the **Site Template** section, click **Add Site Template**.

On the **New Site Template** screen that is displayed, provide the details as required and click **Next**.

Note

When you clone a site or create a site using a site template and the source has Wi-Fi configured, the Wi-Fi settings do not get copied to the new site.

SiteTemplate Details		
Site Template Name *		
SiteA		
Site Address *		Lat/Lng
San Francisco, CA, USA		
Notes (Optional)		
Enter Notes for this Site		
		h

WAN link template

WAN link templates help you to configure WAN links easily and quickly. You can create a WAN link template once and reuse it multiple times while configuring WAN links. You can even copy the modified WAN link template configurations to the site WAN link configurations created using the WAN link template.



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.

WAN Link	×
Create New Use a Template	

Cancel Done

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.

Wan Link Info							
Template Name* Acce	ess Type	Internet Categor	У	ISP Name *		Custom	Congestion Threshold (µs)
	Public Internet 🗸 🗸	Broadband	✓ k	E.g. AT	r, Verizon	\sim	20000
Public IP Address Auto Detect	LAN to WAN Rate *	Mbps 🗸	WAN to LAN Rate	*	Mbps 🗸	Provide	r ID
	100		100				
Frame Cost (Bytes)	MTU (Bytes)		Standby Mode				
1	1350		Disabled		\sim		
Enable Metering Adaptive	Bandwidth Detection						
Minimum Acceptable Bandwidth (%)							
30							
Metering							
Data Cap(MB)	Billing Cycle		Starting From				
0	monthly	\sim	MM/DD/YY	ΥY			
	Approximate Data Alread	dy Used (MB)					
Disable Link if Data Cap Reach	ed 0						

Previously, the option to copy the modified WAN link template configurations to site WAN link config-

urations was not available. For example, if a user had already created multiple site WAN links using a WAN link template and had to modify a particular configuration (For example, congestion threshold setting), the user had to do it on every site WAN link individually. From now on, the user can update the WAN link template with the new congestion threshold setting and copy the latest WAN link template configurations to all the site WAN links created using the WAN link template.

When you select one or more WAN link templates and click copy, the updates that you make on the WAN link template get copied to the site WAN link configuration created using the selected templates.

Note

The WAN link site configurations that are created using the Site profile feature do not get updated.

Copy WAN link template configurations to site WAN links

Select either one of the WAN link template or <All> to copy the WAN link configurations from the template to the site WAN link configuration. Note: The site WAN link configurations will be replaced with configurations in the template.

Select Template	
<all> ×</all>	~
Сору	

ECMP load balancing

October 26, 2021

Equal Cost Multi-Path (ECMP) groups allow you to group multiple paths with the same cost, destination, and service. The connections or session data is load balanced across all the paths in the ECMP group depending on the type of ECMP group. For example, consider a network with two WAN links between a branch and a data center having the same route cost. Traditionally, one of the WAN links would be active and the other remains dormant acting as a fallback link. With ECMP Groups, you can group these WAN links together and allow traffic to be load balanced through both the WAN links. ECMP load balancing ensures:

- Distribution of traffic over multiple equal-cost paths.
- Optimal usage of available bandwidth.
- Dynamic transfer of traffic to other ECMP member path, if a route becomes unreachable.

ECMP load balancing is supported on the following services:

- Virtual Paths
- Citrix Secure Internet Access

- Zscaler
- IPsec
- GRE

You can define a maximum of 254 ECMP groups in your network. The maximum number of ECMP eligible routes in an ECMP group depend on your appliance and license type. The following two types of ECMP groups are supported on Citrix SD-WAN:

- Source/destination IP address: Networks where multiple clients try to connect to the same destination, the connections are load balanced across equal cost WAN links.
- Session: Networks where a single client is connected to a destination and multiple sessions are spawned. The session data is load balanced across equal cost WAN links.

To configure an ECMP group, at the Network level, navigate to **Configuration > Routing > ECMP Groups**. Provide a name for the ECMP group and select the type as **Src/Dest IP address** or **Session** as required.

ECMP Groups (i)

ECMP Group		
Name *	Туре *	
ECMP_Group_1	Src/Dst IP Address	/
Save Cancel		

You can associate the ECMP groups to the following services:

- Virtual Paths (at site level)
- Citrix Secure Internet Access
- Zscaler
- IPsec
- GRE

To enable ECMP configuration on Intranet services, at the Network *level, navigate to **Configuration** > **Delivery Channels > Bandwidth allocation > Intranet + Service** and select the **Service Type** as **Intranet**. Select the ECMP group while configuring the Intranet service.

Note

Selecting None will not enable ECMP configuration on the service.

← Edit Intranet Service

Note: Make sure to allocate bandwidth globally or	specific to site				
Intranet Service Info					
Service Name	Routing Domain		ECMP Group	Firewall Zone	
Intranet-service-1	Default_RoutingDomain	~	ECMP_Group_1	<default></default>	\sim
Intranet Subnets Add Network		ļ			
Network IP / Prefix	Co	ost			Actions
Advanced Settings					
Preserve route to Intranet from link even if all associa	ted paths are down				
✓ Enable Primary Reclaim					
Save Cancel					

To enable ECMP configuration on Virtual paths, at the Site level, navigate to **Configuration > Ad-vanced Settings > Delivery Services > Virtual Paths > Static Virtual paths > + Virtual paths**. Select the ECMP group while configuring the Static Virtual paths.

Note

Selecting **None** will not enable ECMP configuration on the service.

Virtual Paths Internet Se	ervice Intranet Serv	ices						
Static Virtual Paths Dyn	amic Virtual Paths							
Static Virtual Paths								
Remote Site *	QOS Profile	Branch Tracking IP		Reverse Trackin	ng IP	ECMP Group		Route Cost
~	Standard					ECMP_Group_1	~	Default
Active Member Paths								
						Restore Defau	ılt Memb	er Paths
Path								Actions
WAN Link Properties								
Name	UDF	Port	Alternate Port		Port Switching Interv	al (min) Tunnel Heade	r Size	Action
Cancel Save								

To enable ECMP configuration on Zscaler services, at the Network level, navigate to **Configuration** > **Services & Bandwidth**. Click the **Settings** icon next to Zscaler listed under the **Delivery Services** column. Authenticate and click + **Site**. Select the **Enable ECMP** check box while adding sites.

NOTE

Zscaler service supports only session-based ECMP load balancing.

th		
	Primary ZEN *	
\sim	Singapore IV	~
	Secondary ZEN *	
\sim	Denver III-2	~
tes listed b	Denver III-2	Select Sites
ites have	been Selected	
	th tes listed b ites have	Primary ZEN* Singapore IV Secondary ZEN* Denver III-2 tes listed below

To enable ECMP configuration on Citrix Secure Internet Access service, at the Network level, navigate to **Configuration > Services & Bandwidth**. Click the **Settings** icon next to **Secure Internet Access Service** and click **+ Site**. Select the **Enable ECMP** check box after selecting the sites.

NOTE

Citrix Secure Internet Access service supports only session-based ECMP load balancing.

Verify Config Service & Bandwidth	
Tunnel Type* Regions*	~
Site Name Home210	Enable ECMP
Back Save Cancel	

To enable ECMP configuration on fixed IPsec tunnels with third-party peers on the LAN or WAN side,

navigate to **Configuration > Services & Bandwidth > Intranet + Service** and select the **Service Type** as **IPsec**. Select the **Enable ECMP** check box and choose a type from the **ECMP Type** drop-down list.

Service Details				
Service Name * S	Service Type *	Routing Domain	Firewall Zone	
zscaler210	Intranet	✓ Default_RoutingDomain	· · ·	\sim
Enable ECMP Tunnel End Points Across Network + End Point	CMP Type * Session Session Source Destination	→ IP		
Name	Peer IP	IPsec Profile		Actions
ep1	101.071.040.40	zscalerprofile		<u>ا</u>
ep2	114.021.081.79	zscalerprofile		Ē
Map Sites to Tunnel End Points				
+ End Point Mapping				
Name		No of Sites		Actions
ep1		1		1
0		1		Ī

Notification settings

September 14, 2022

You can configure Citrix SD-WAN Orchestrator service to identify alert conditions based on your network and priorities, generate alerts, and receive notifications via email.

Alert configuration

An alert for an event type is triggered by the trigger and clear state or severity.

To configure alerts at the network level, navigate to **Alerts** > **Notification Settings** > **Alert Configuration** and click **Add**. Provide a name for the alert and enter values for the following parameters:

- **Event Type**: The SD-WAN appliance can trigger alarms for particular subsystems or objects in the network, these are called event types. The available event types are SERVICE, VIRTUAL_PATH, WANLINK, PATH, DYNAMIC_VIRTUAL_PATH, WAN_LINK_CONGESTION, USAGE_CONGESTION, FAN, POWER_SUPPLY, PROXY_ARP, ETHERNET, DISCOVERED_MTU, GRE_TUNNEL, and IPSEC_TUNNEL.
- **Frequency**: The frequency with which the alert notifications are sent. The selected frequency is the time interval between two alert notifications. All the alerts occurring within the interval are cumulatively sent as a single notification.
- **Notification profile**: Defines the notification mechanism to send the alert notification. For more detail, see Notification profile.

Trigger rules

- **Severity**: Select the severity level about which you have to be notified. You can choose multiple severity levels.
 - Trigger Duration: The duration in seconds, this determines how quickly the appliance triggers an alarm. Enter a value between 0-600 seconds. By default, the trigger duration is set to 10 seconds. Alarms are not triggered, if more events occur on the same object within the trigger duration period. More alarms are triggered only if an event persists longer than the trigger duration period.

Alert Configuration Notification Profile			
Alert Configuration			
Name* Config_Update			
Event Type*	F	requency*	Notification Profile*
Trigger Rules Severity Custom Criteria Severity Type'	Trigg	instantly 5 minutes 15 minutes 30 minutes	roat_ndl3
Sites All Sites Specific Sites		1 hour	

- **Custom Criteria**: Trigger rule, provide the following details.
 - **Trigger State**: The event state that triggers an alarm for an Event Type. The available Trigger State options depend on the chosen event type.
 - **Trigger Duration**: The duration in seconds, this determines how quickly the appliance triggers an alarm. Enter a value between 0-600 seconds. By default, the trigger duration is

Alert Configuration Notification Profile

set to 10 seconds. Alarms are not triggered, if more events occur on the same object within the trigger duration period. More alarms are triggered only if an event persists longer than the trigger duration period.

- **Clear State**: The event state that clears an alarm for an Event Type after the alarm is triggered. The available Clear State options depend on the chosen Trigger State.
- Clear Duration: The duration in seconds, this determines how long to wait before clearing an alarm. Enter a value between 0-600 seconds. By default, the clear duration is set to 10 seconds. The alarm is not cleared, if another clear state event occurs on the same object within the specified time.

Alert Configuration							
Name *							
CustomCriteriaConfig							
Event Type *		Frequency			Notification Profile	•	
Virtual Path		S minutes		~	TestProfile_	1	~
Trigger Rules O Severity	n Criteria						
Trigger State	Trigger Dura	tion *	Clear State			Clear Duration	
disabled \checkmark	10		good		\sim	10	
Sites All Sites Specific Sites							
Cancel Save							

Sites

- All Sites: The event is by default set for all sites (global level).
- **Specific Sites**: You can set the event for specific sites. Select the Specific Sites radio button and click **Select Sites**.

Alert Configuration		
Name "		
Config_Update		
Event Type *	Frequency*	Notification Profile *
Config Update	✓ 5 minutes ✓	Test_Alerts ~
Trigger Rules Severity Custom Criteria		
Seventy Type Low Medium High	Trigger Duration " 10	
Alert Configuration will be applied to the sites listed below		Select Sites
	No Sites have been Selected	
Cancel Save		

You can search for a site by name or can select sites by region/custom groups from the drop down list.

iearch		C
ilter By Region / Custom Groups		
Available (3 Sites)	Selected (1 Sites)	
Name	Name	
London_MCN Test_110_Office Test_VPX_Inband	→ Spain_Branch1	

Click **Save**. The selected site reflects under **Site**.

Alert Configuration		
Name*		
Config_Update		
Event Type *	Frequency*	Notification Profile *
Config Update	✓ 5 minutes	V Test_Alerts
Trigger Rules Severity Custom Criteria		
Severity Type' 🖌 Low 🖌 Medium 🗌 High	Trigger Duration * 10	
Sites All Sites Specific Sites		
Alert Configuration will be applied to the sites listed below		Select Sites
Sites (1) Spain_Branch1		

The created alert configurations are listed under **Alert Configuration**. Click to view more details.

	Alert C	onfiguration Notification	n Profile					
A	bb	Edit Delete						
Q	Click h	ere to search with Key:Valu	ue format					:
		NAME 0	EVENT TYPE:	FREQUENCY	ALERT TRIGGER RULES	NOTIFICATION PROFILE	NOTIFICATION MECHANISMS	+
>		CustomCriteriaConfig	Virtual Path	5 minutes	Trigger State: disabled, Trigger Duration: 10, Clear St	TestProfile_1	EMAIL	
>		SeverityConfig	Virtual Path	5 minutes	Severity: HIGH, MEDIUM, LOW	TestProfile_1	EMAIL	
					Showing 1	-2 of 2 items Page 1	of 1 🚽 🕨 10 rows	s ~

Notification profile

You can create a notification profile and set-up the email notifications. The notification profiles are further used to create alert configuration. For more details, see Alert configuration.

To create a notification profile, at the network level, navigate to **Alerts** > **Notification Settings** > **No-tification Profile** and click **Add**. Provide a name for the notification profile.

You can receive the Citrix SD-WAN alerts to your email address. You can use the default SMTP server provided by Citrix SD-WAN Orchestrator service or use a custom SMTP server to send email notifications.

Click **Enable email Alerts** and provide the email ids to which notifications have to be sent in the **To**, **Cc**, and **Bcc** fields. You can enter multiple email ids separated by a comma. The **To** field is mandatory, the **Cc** and **Bcc** fields are optional.

You can enter custom text which is appended at the end of the email notification. The custom text limit is 200 characters. Custom text can be used to filter and search specific alert emails.

Customize email notifications settings by providing your SMTP server details. You can also secure messaging by enabling HTTPS messages. Provide the HTTPS server URL and credentials, the server is used as a secure base server to transport messages. The HTTPS server uses the SSL certificate for security.

You can send push notifications to the HTTPS server by either using the username and password or uploading the secret certificate and key files. Ensure to upload the client certificate in PEM format and upload the secret key file in PKCS8 format.

Network Alerts : Notification Settings (Preview) Alert Configuration Notification Profile Certifications			Site Group: All ~
Notification Profile			
Profile Name *	1		
profile_1			
Email Configuration			
C Enable Email Alerts			
To:*	Ce:	Bcc:	
johndoe@xyz.com, alex@xyz.com	aton@xyz.com	nathan@xyz.com	
Custom Text	1		le
Critical events			
Use Custom SMTP server			
SMTP Server IP*	SMTP Server Port*		
turbo-smtp.com	25		
SMTP User Name "	SMTP Password *		
john⊕xyz.com			
Source Email Address *			
noreply@xyz.com			
HTTPS Server Configuration			
Enable HTTPS Messages			
Server URL:*			
https://sdwan/nito/v1/config			
User Name / Password Client Certificate			
Client Certificate			
internal.crt ~			

To upload the client certificate and secret key files, navigate to the Certifications tab. In the Upload Cert and Key Files section, upload the files.

Alert Configurat	ion Notification Profile	Certifications
oload Cert and	Key Files *	
Browser	No File Selected	

Network location service

June 27, 2024

Important update:

This feature is deprecated in the Citrix SD-WAN Orchestrator service deployment. However, you can still enable NLS using Citrix Cloud. For details, see Optimize connectivity to workspaces with Direct Workload Connection.

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 customer level, navigate to **Configuration > Network Location Service**.

Verify Config Network Location Service	
C Enable	
Network Location Service Settings will be applied to the sites listed below	Select Sites
No Sites have been Selected	
Deploy	

Select **Enable** if you want to enable NLS for all sites in the network. To enable NLS for specific sites, click **Select Sites**. Choose the **Region** and select the sites accordingly. Click **Save** and then **Deploy**.

	Site Selector
Verify Config Network Location 5	Browse or search the list of sites, regions and groups below. You can add/remove entire Regions and Groups, or click into them and choose a subset of its members to add/remove.
Z Enable	Search
Network Location Service Settings will be a	Q
	Filter By Region / Custom Groups
Doplay	
Deploy	Name Name
	Kansas Boston SantaClara □ Dallas
•.	
	Save

Site configuration

July 27, 2022

You can add new sites from the **Network Home** page or from the **Profiles & Templates** section to configure your SD-WAN network.

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

Site Name *		
Bengaluru		
On-Premises Cloud Site		
Site Address *		✓ Lat/Lng
Bengaluru, Karnataka, India		
Latitude *	Longitude *	
12.9715987	77.5945627	

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.

ie Name * SiteA I* Sub-Model* BASE	Site Address* 1239 Henderson Device Ed	Lat/Lng		
SiteA	1239 Henderson Device Ed	Ave, Sunnyvale,		
I* Sub-Model*	Device Ed			
BASE		lition [*]		
	 ✓ SE 	~		
ndwidth Tier (Mbps) *	Select Tag	Create New		
20 ~		\sim		
_				
				SiteA SDWAN-210 (Primary)
k even if all associated paths a	re down			
k even if all associated paths a	re down			
	20 ~ Default Routing Domain Default_RoutingDomain k even if all associated paths a	additional field (Mopps) Select rag 20 V Default Routing Domain Default_RoutingDomain V	Default Routing Domain Default_RoutingDomain v v	Default Routing Domain

When you configure sites using a site template, the following screen is displayed.
Citrix SD-WAN Orchestrator

G Site Details	Device Details	Interfaces	😢 WAN Links 🛛 🔞	Routes 🛛 💿 Sum	mary	
Template Information						
Template Name*						
test						
Region*	Device Model*	Sub-Model	Device Edition			
Default-Region 🗸	210	BASE	↓ SE	~		
Site Role*	Bandwidth Tier (N	fbps)*	Select Tag	Create New		
Branch	~ 100	~		~		
				_		
Default Routing Domain						
Global Default Advanced Settings Enable Source MAC Lea	- Defaul	It_RoutingDomain	~			
Preserve route to Intern	et from link even if all asso	ciated paths are dow	'n			
Preserve route to Intran	et from link even if all asso	ciated paths are dow	'n			test SDWAN-21
Contact Details						
ontact Name		Contact Email				
Enter Contact Name for	this Template	Enter Contac	t Email for this Template			
lotes						
Enter Notes for this Site				<i>t</i> e		
Cancel Save			P	rev Next		

Site/Template 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

Citrix SD-WAN Orchestrator service 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. 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. 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.

Routing support for LAN segmentation

The SD-WAN Standard and Enterprise Edition (SE/PE) appliances implement LAN segmentation across distinct sites where either appliance is deployed. The appliances recognize and maintain a record of the LAN side VLANs available, and configure rules around what other LAN segments (VLANs) can connect to at a remote location with another SD-WAN SE/PE appliance.

The above capability is implemented by using a Virtual Routing and Forwarding (VRF) table that is maintained in the SD-WAN SE/PE appliance, which keeps track of the remote IP address ranges accessible to a local LAN segment. This VLAN-to-VLAN traffic would still traverse the WAN through the same pre-established Virtual Path between the two appliances (no new paths need to be created).

An example use case for this functionality is that a WAN administrator might be able to segment local branch networking environment through a VLAN, and provide some of those segments (VLANs) access to DC-side LAN segments that have access to the internet, while others might not obtain such access. The configuration of the VLAN-to-VLAN associations is achieved through the Citrix SD-WAN Orchestrator service web interface.

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.

				Verify Configuration	Software Version : 11.3.1.53-G
O Site Details O Device Details	3 Interfaces 🛛 🚳 WAN Links	05 Routes	06 Summary		
Device Information					
Enable HA					
Primary Device - Serial Number : 338D8622-6416-C527-C69D-4 - Short Name : MB-Branch1-Primary Secondary Device - Serial Number : Not configured Add - Short Name :	1E631D113803 Delete				
Advanced HA Settings		•			
Advanced HA Settings Failover Time (ms)	Shared Base MAC	*			
Advanced HA Settings Failover Time (ms) 1000	Shared Base MAC AA:AA:AA:00:00:00	^			
Advanced HA Settings Failover Time (ms) 1000 Primary Reclaim	Shared Base MAC AA:AA:AA:00:00:00	•			
Advanced HA Settings Failover Time (ma) 1000 Primary Reclaim HA Fail-to-Wire Mode	Shared Base MAC AA:AA:AA:00:00:00	•			
Advanced HA Settings Failover Time (ms) 1000 Primary Reclaim HA Fail-to-Wire Mode Disable Shared MAC	Shared Base MAC AA:AA:AA:00:00:00	•		LAN-1 1	WAN-1 2Broadband-Verizon
Advanced HA Settings Failover Time (ma) 1000 Primary Reclaim HA Fail-to-Wire Mode Disable Shared MAC Cancel Save	Shared Base MAC AA:AA:AA:00:00:00	Prev Next	-	LAN-1 1	WAN-1 2Broadband-Verizon

Note

Serial numbers are not configurable using the site templates.

Device information

Enable HA and enter the serial number and a short name for the primary and the secondary appliances. Click **Add** and provide the serial number along with the site short name.

	0 Site Details	02 Device Details	03 Interfaces	04 WAN Links	05 Routes	06 Summary	
Device Ena Prima - Ser - She	e Information able HA ary Device rial Number : <i>Not col</i> ort Name :	nfigured Add					
Can	icel Save					Prev Nex	t

Click **Add**.

Add Device		
Serial Number *		
33808622 64% C327 C880 404310113803		
Short Name		
MB-Branch1-Primary		
	Cancel	Add

• 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.

Click the **Delete** option if you want to delete the serial number.

Note Updating serial number requires deleting the existing serial number and readding a new one.

O Site Details O2 Device Details	ils 03 Interfaces	04 WAN Links	05 Routes	06 Summary
Device Information				
Enable HA Primary Device - Serial Number : - Short Name : <i>MB-Branch1-Primary</i>	80-408210112802	Delete		

On clicking the **Delete** option, a pop-up appears to confirm if you want to delete the serial number or not.

A Serial Number Delete	
Are you sure you want to Delete the Seria ?	l Number
Confirm	Cancel

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.

Verify Config 01 Site	Details 02 Device Details	03 Cloud Details 04 Interfaces	65 WAN Links 66 Routes 77 Summary
nterface Attributes			
eployment Mode * Interfac Edge (Gateway) >> LAI	e Type* Security* N Trusted	Interface Name	
hysical Interface			
elect interface* 1 2 3 4 5 6 7 8 //rtual Interfaces	1		
'LAN ID*	Virtual Interface Name *		
0	VIF-1-LAN-1	Enable HA Heartbeat	
touting Domain *	Firewall Zones	Client Mode	_
Default_RoutingDomain $~~$	Internet_Zone ~	PPPoE Static V	
C Name	Service Name	Reconnect Hold Off (s)	LAN-1 8
test-ac-name	test-service-name	0	
Isername *	Password *	Auth	
test-user		Auto ~	
lote : Converting Virtual Interfa uddress (in case of PPPoE Dyna DHCP DHCP IPv6 Client Client	ace to PPPoE will clear any Gatew amic only) associate with it under SLAAC Dii Br	ay IP Address and Virtual IP. access interfaces rected padcast	SDWAN-VPX (Primary)
+ IP V4 Addresses	+ IP V6 Addresses		
Type IP Addres	Identity Prive	te Link Delete Local	
IPv4 Eg: a.b.c.d/e	•	N/A 🗊	
		Done	

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 management 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 the 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.

Earlier, the DHCP client was only supported on Fail-to-block port. With the Citrix SD-WAN 11.2.0 release, the DHCP client capability is extended on fail-to-wire port for the branch site with serial High Availability (HA) deployments. This enhancement:

- * Allows the DHCP client configuration on untrusted interface group that has fail-to-wire bridge pair and serial HA deployments.
- * Allows DHCP interfaces to be selected as part of Private Intranet WAN links.

Notes

- * Inline (Fail-to-Wire) option is available only on hardware appliances and not on virtual appliances (VPX / VPXL).
- * DHCP client is now supported on the private intranet link.
- * A LAN interface must not be connected into the fail-to-wire pair as packets might be bridged between the interfaces.



* **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 acts as a PPPoE client. For IPv4, SD-WAN obtains the dynamic IPv4 address or uses the static IPv4 address. For IPv6, it obtains the link local address from the PPPoE server. For the IPv6 unicast address, Static IP, DHCP, or SLAAC can be used.

- **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, for example; Citrix SD-WAN. PPPoE allows users to share a common Digital Subscriber Line (DSL), cable modem, or wireless connection to the Internet. PPPoE combines the Point-to-Point Protocol (PPP), commonly used in dialup connections, with the Ethernet protocol, which supports multiple users in a LAN. The PPP protocol information is encapsulated within an Ethernet frame.

Citrix SD-WAN appliances use PPPoE to support ISP to have ongoing and continuous DSL and cable modem connections unlike dialup connections. PPPoE provides each user-remote site session to learn each other's network addresses through an initial exchange called "discovery". After a session is established between an individual user and the remote site, for example, an ISP provider, the session can be monitored. Corporations use shared Internet access over DSL lines using Ethernet and PPPoE.

Citrix SD-WAN acts as a PPPoE client. For IPv4, SD-WAN obtains the dynamic IPv4 address or uses the static IPv4 address. For IPv6, it obtains the link local address from the PPPoE server. For the IPv6 unicast address, Static IP, DHCP, or SLAAC can be used.

The following is required to establish successful PPPoE sessions:

- Configure virtual network interface (VNI).
- Unique credentials for creating PPPoE session.
- Configure WAN link. Each VNI can have only one WAN link configured.
- Configure Virtual IP address. Each session obtains a unique IP address, dynamic, or static, based on the provided configuration.
- Deploy the appliance in bridge mode to use PPPoE with static IP address and configure the interface as "trusted."
- Static IP is preferred to have a configuration to force the server proposed IP; if different from the configured static IP, an error can occur.
- Deploy the appliance as an Edge device to use PPPoE with dynamic IP and configure the interface as "untrusted."
- Authentication protocols supported are, PAP, CHAP, EAP-MD5, EAP-SRP.
- Maximum number of multiple sessions depends on the number of VNIs configured.
- Create multiple VNIs to support Multiple PPPoE sessions per interface group.

Note

Multiple VNIs are allowed to create with the same 802.1Q VLAN tag.

Limitations for PPPoE configuration:

- 802.1q VLAN tagging is not supported.
- EAP-TLS authentication is not supported.
- Address/Control compression.
- Deflate Compression.
- Protocol field compression negotiation.
- Compression Control Protocol.
- BSD Compress Compression.
- IPX protocols.
- PPP Multi Link.
- Van Jacobson style TCP/IP header compression.
- Connection-ID compression option in Van Jacobson style TCP/IP header compression.

• PPPoE is not supported on LTE interfaces.

From Citrix SD-WAN 11.3.1 release, an extra 8 bytes PPPoE header is considered for adjusting TCP Maximum Segment Size (MSS). The extra 8 bytes PPPoE header adjusts the MSS in the synchronize packets based on the MTU. The supported MTU ranges from 1280 bytes to 1492 bytes.

PPPoE configuration On an MCN, you can configure only PPPoE static. On a branch, you can configure either PPPoE static or PPPoE dynamic.

To configure PPPoE, at the site level configuration, navigate to **Configuration > Site Configuration > Interfaces** tab. In the **Virtual Interfaces** section, select the appropriate PPPoE option from the **Client Mode** drop-down list.

Note

- A VNI configured with multiple interfaces can have only one interface used for PPPoE connectivity.
- If a VNI configured with multiple interfaces and a PPPoE connectivity is changed to a different interface, then the **Reports > Real Time > PPPoE** page can be used to stop the existing session and start a new session. The new session can then be established over the new interface.
- If PPPoE Dynamic is selected, the VNI is required to be "Untrusted."

Citrix SD-WAN Orchestrator

Deployment Mode* Inte Edge (Gateway)	wan ~	Security*	Interface Name
Physical Interface			
Select Interface*			
Virtual Interfaces			
VLAN ID*	Virtual Interface Name*		
0	VIF-2-WAN-1		Enable HA Heartbeat
Routing Domain *	Firewall Zones		Client Mode
Default_RoutingDomain	✓ <default></default>	~	PPPoE V4 Dynamic + V6 🗸 🗸 🗸
AC Name	Service Name		Reconnect Hold Off (s)
test_ac	pppoe_service		0
Username *	Password *		Auth
user1	•••••	۲	Auto ~
Note : Converting Virtual Interface to Address (in case of PPPoE Dynamic o	PPPoE will clear any Gatewa only) associate with it under a	ay IP Address and Virtu ccess interfaces	al IP.

- 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.

Only one WAN link creation is allowed per PPPoE static or dynamic VNI. The WAN link configuration varies depending on the VNI selection of the Client Mode.

If the VNI is configured with PPPoE dynamic client mode:

• IP address and Gateway IP address fields become inactive.

- Virtual path mode is set to "Primary."
- Proxy ARP cannot be configured.

By default, Gateway MAC Address Binding is selected.

If the VNI is configured with PPPoE static client mode, then configure the IP address.

Note

If the server does not honor the configured static IP address and offers a different IP address, an error occurs. The PPPoE session tries to re-establish connection periodically, until the server accepts the configured IP address.

PPPoE Monitoring and Troubleshooting At the site level, navigate the **Reports > Real Time > PP-PoE** section to view information about the configured VNIs with the PPPoE static or dynamic client mode. It allows you to manually start or stop the sessions for troubleshooting purposes.

Site Reports: Real Time PPP	oE 🛛		Relative Time	✓ Interval:	Last 1 Hour 🖂		
Retrieve Latest Data Start	Retrieve Latest Data Start Stop						
$\ensuremath{\mathbb{Q}}$ Click here to search or you can enter	r Key : Value format				0 0 0		
VIRTUAL INTERFACE		GATEWAY IP	SESSION ID	STATE	÷ +		
VirtualInterface-2			0	Dialling			
VIF-2-LAN-1		10.00.00.0	3	Ready			
		Showing 1-2 of	2 items Page 1	of 1 🔹 🕨	10 rows 🗸 🗸		

When there is a problem in establishing a PPPoE session:

- Hovering the mouse over the failed status shows the reason for the recent failure.
- To establish a fresh session or for troubleshooting an active PPPoE session, restart the session.
- If a PPPoE session is stopped manually, it cannot be started until either it is manually started and a configuration change is activated, or the service is restarted.

A PPPoE session might fail due to the following reasons:

- When SD-WAN fails to authenticate itself to the peer due to an incorrect username/password in the configuration.
- PPP negotiation fails negotiation does not reach the point where at least one network protocol is running.
- System memory or system resource issue.
- Invalid/bad configuration (wrong AC name or service name).
- Failed to open serial port due to operating system error.
- No response received for the echo packets (link is bad or the server is not responding).
- There were several continuous unsuccessful dialing sessions with in a minute.

After 10 consecutive failures, the reason for the failure is observed.

- If the failure is normal, it restarts immediately.
- If the failure is an error then restart reverts for 10 seconds.
- If the failure is fatal the restart reverts for 30 seconds before restarting.

LCP Echo request packets are generated from SD-WAN for every 60 seconds and failure to receive 5 echo responses is considered as link failure and it re-establishes the session.

- If the VNI is up and ready, the IP and Gateway IP columns shows the current values in the session. It indicates that these are recently received values.
- If the VNI is stopped or is in failed state, the values are the last received values.
- Hovering the mouse over the Gateway IP column shows the MAC address of the PPPoE Access Concentrator from where the Session and IP is received.
- Hovering the mouse over the "state" value shows a message, which is more useful for a "Failed" state.

PPPoE session type	Status Color	Description
Configured	Yellow	A VNI is configured with PPPoE. This is an initial state
Dialing	Yellow	After a VNI is configured, the PPPoE session state moves to
		dialing state by starting the PPPoE discovery. Packet information is captured.
Session	Yellow	VNI is moved from Discovery state to Session state, waiting to receive IP, if dynamic or waiting for acknowledgment from the server for the
Ready	Green	IP packets are received and the VNI and associated WAN link is ready for use
Failed	Red	PPP/PPPoE session is terminated. The reason for the failure can be due to invalid configuration or fatal error. The session attempts to reconnect after 30 seconds.

PPPoE session type	Status Color	Description
Stopped	Yellow	PPP/PPPoE session is manually stopped.
Terminating	Yellow	An intermediate state terminating due to a reason. This state automatically starts after certain duration (5 seconds for normal error or 30 secs for a fatal error).
Disabled	Yellow	The SD-WAN service is disabled.

The *SDWAN_ip_learned.log* file contains logs related to PPPoE. Navigate to **Troubleshooting > Device Logs** to view or download the *SDWAN_ip_learned.log* file.

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 410 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 profiles 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.

Wired 802.1X Configura	ation	
Enable 802.1x		
(i) When enabled 802	2.1x Configura	tion will be applied to supported ports only.
RADIUS Profiles		
Primary RADIUS Profile *		Secondary RADIUS Profile
PiFreeRADIUS	\sim	Select Radius Profile 🗸
Create Radius Profile		Create Radius Profile
Virtual Interfaces		
Authenticated VIF*		Unauthenticated VIF
101	\sim	100 ~
MAC Address Bypas	S	
MAC Address Bypass Value		
Enter a MAC Adress	o byapss	Add
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 template to configure WAN link attributes quickly. If you have already used a site profile, the **WAN link** attributes auto-populate.

Citrix SD-WAN Orchestrator

WAN link attributes

WAN Link Attribu	tes					
iamplate Name O	Acces	s Type	ISP Name	* Custo	m Internet Categor	/
International a	P	ublic Internet	→ Hath	iway	✓ Broadband	~
	ite					
Link Name *		Tracking I	P Address			
Broadband-Hat	thway-1					
	Public IPv4 Add	ress	Public IPv6 Address	3		
Auto Detect	E.g. a.b.c.o	ł	E.g. 2001:0db	8:85a3:0000:0000:8	a2e:0370:7334	
Egress			Ingres	S		
Speed *		Mbps	✓ Speed*			Mbps 🗸
97			97			
Permitted Rate	AL	ito Learn 🗹 Physical	Rate Permitte	d Rate	Auto Learn	Physical Rate
97			97			
Access Interfaces	s					
+ Accord Int	torfago					
· Access Int		10.7	12.1.1.	0.1		A. 15.
Name	Virtual Interface	IP Type	IP Address	Gateway IP	VIF Path Mode	Actions
AIF-1	VIF-1-WAN-1	V4	10.40.3.10	10.40.3.1	Primary	
AIF-2	VIF-1-WAN-1	V6	f::3	f::1	Primary	İ
ervice Bandwidt	h Settings : Link	Specific 🗸				
ervice Bandwidt	h Settings : Link	Specific 🗸				
+ Service						
Service Name	Allocation %	Actions		Servio	ces Allocation	
Service Name	Allocation %	Actions		Servio	ces Allocation	
Service Name internet Virtual Path	Allocation % 10% 90 %	Actions		Servic	ces Allocation	
Service Name internet Virtual Path	Attocation % 10% 90 %	Actions P D C		Servic	ces Allocation	
Service Name internet Virtual Path	Altocation % 10% 90 %	Actions		Servic	ual Path (90%)	
Service Name internet Virtual Path	Attocation % 10% 90 %	Actions	Inte	Servic	ual Path (90%)	
Service Name internet Virtual Path firtual Path Settin	Attocation % 10% 90 %	Actions	Global Default	Servic	ual Path (90%)	
Service Name internet Virtual Path firtual Path Settin telative Bandwidt	Attocation % 10% 90 %	Actions P D C S S S S S S S S S S S S S	Global Default	s v	ual Path (90%)	
Service Name internet Virtual Path firtual Path Settlin telative Bandwidd dvanced WAN O	Attocation % 10% 90% 90% rest for the Link th Provisioning across ptions	Actions Actions Description Description Adaptive Bandwidth Partners	Global Default	s virt	ual Path (90%)	•
Service Name internet Virtual Path firtual Path Settin telative Bandwidd telative Ba	Attocation % 10% 90% 90% Provisioning acro ptions	Actions Act	Global Default	ernet (10%) Virtu	ual Path (90%)	*
Service Name internet Virtual Path Virtual Path Virtual Path Settin Relative Bandwidd C Enable Metering Jinimum Acceptable I 30	Attocation % 10% 90% 90% Provisioning acro ptions	Actions Actions Image: Constraint of the second	Global Default	ernet (10%) Virtu	ual Path (90%)	*
Service Name internet Virtual Path Virtual Path Virtual Path Settin telative Bandwidd telative Bandwidd telative Bandwidd advanced WAN O telative Bandwidd advanced WAN O a	Attocation % 10% 90% 90% Provisioning acro ptions	Actions Act	Global Default	ernet (10%) Virtu	ual Path (90%)	*
Service Name internet Virtual Path Virtual Path Settin Relative Bandwick Advanced WAN O Enable Metering Itinimum Acceptable I 30 Congestion Threshold	Attocation % 10% 90% 90% 90% Units of the Link th Provisioning across the provisioning across the provision of the Link the provision of the the provision of the provision	Actions Actions Actions Actions Actions Actions Actions Actions Actions Provider ID	Global Default	ernet (10%) Virtu s Frame (ual Path (90%)	•
Service Name internet Virtual Path Virtual Path Virtual Path Settin Relative Bandwidd Congestion Threshold 3000	Attocation % 10% 90% 90% solution solut	Actions Actions Actions Actions Actions Actions Provider ID Actions	Global Default	ernet (10%) Virtu s Frame I 1	ual Path (90%)	*
Service Name internet Virtual Path Virtual Path Settin Relative Bandwich Celative Ba	Attocation % 10% 90 % 90 % Units Provisioning across Provisioning	Actions Actions Actions Actions Actions Provider ID TU(Bytes)	Clobal Default	ernet (10%) Virtu s Frame (1	Lat Path (90%)	•
Service Name internet Virtual Path firtual Path Settin clattice Bandwidd clattice Ba	Altocation % 10% 90 % 90 % 10% Provisioning acro ptions	Actions Actions Actions Actions Actions Provider ID TU (Bytes) T350	Global Default	Servic	Les Allocation	
Service Name internet Virtual Path Path Virtual Path Virt	Altocation % 10% 90 % 90 % Units Provisioning across Pathons P	Actions Actions Actions Actions Actions Actions Actions Provider ID TU (Bytes) T350	Clobal Default	Servic	Les Allocation	
Service Name internet Virtual Path Path Virtual Path Settin Relative Bandwidd Advanced WAN O Enable Metering Minimum Acceptable I 30 Congestion Threshold 30000 Standby Mode Disabled Eligibility	Altocation % 10% 90 % 90 % 90 % 90 % 90 % 90 % 90 % 90	Actions Actions Actions Actions Actions Actions Provider ID TU (Bytes) I350	Global Default	Servic	cost (Bytes)*	
Service Name internet Virtual Path Virtual Path Virtual Path Settin Relative Bandwidd Advanced WAN O Enable Metering Minimum Acceptable I 30 Congestion Threshold 30000 Standby Mode Eligibility	Altocation % 10% 90 % 90 % Units Provisioning across Units U	Actions Actions Actions Actions Actions Provider ID Provider ID TU (Bytes) T1350	Ciobal Default	Servic	Cost (Bytes)*	
Service Name internet Virtual Path Virtual Path Virtual Path Settin Relative Bandwidd Advanced WAN O Congestion Threshold 300 Congestion Threshold 30000 Eligibility Eligibility	Altocation % 10% 90 % 90 % 90 % 90 % 90 % 90 % 90 % 90	Actions ctions Actions	Ciobal Default	Servic	Les Allocation	
Service Name internet Virtual Path Virtual Path Settin Relative Bandwidd Advanced WAN O Congestion Threshold 300 Congestion Threshold 30000 Etigibility Etigibility	Altocation % 10% 90 % 90 % 90 % 90 % 90 % 90 % 90 % 90	Actions ctions Actions Actions Actions Actions Actions Actions Act	Cilobal Default	Servic	Les Allocation	

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

- **Template Name**: The name of the WAN link template used to create the WAN link. The WAN link template name cannot be modified after the creation of WAN links. Once WAN links are created using a WAN link template, you cannot edit the Access Type, ISP Name, or Internet Category.
- Access Type: Specifies the WAN connection type of the link.
 - Public Internet: Indicates that the link is connected to the Internet through an ISP.
 - **Private Intranet**: Indicates that 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.
- **Internet category**: The type of WAN link Internet access technology service (Broadband, Satellite, Fiber, LTE, and so on) enabled on the WAN link.
- 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 information about adding MPLS queues, see MPLS queues.

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 addressWANK 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) 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.

Citrix SD-WAN Orchestrator

Access Interfaces		
Access Interface Name	Virtual Interface*	Virtual Path Mode "
BRANCH_UTM-WL-1-AI-1	WANT	Primary
IP Address'	● V4 ○ V6 Gates	way IP Address
Bind Access Interface to Gateway MAC Enable Internet Access on Routing	Enable Proxy ARP	
All		
78 V		Cancel Done

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.
- Tunnel Header Size: The size of the tunnel header, in bytes.
- LAN to WAN Tag: The DHCP tag to apply to LAN to WAN packets on the service.
- LAN to WAN Delay: The maximum time, to buffer packets when the WAN Links bandwidth is exceeded.
- LAN to WAN Min Kbps: The minimum upload bandwidth value that is reserved for the service. The Min Kbps is a mandatory field.
- LAN to WAN Max Kbps: The maximum upload bandwidth value that is reserved for the service. The Max Kbps field is optional and the value cannot be lesser than the configured minimum upload bandwidth value. The value must be greater than or equal to the minimum upload bandwidth value.
- 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.
- WAN to LAN Min Kbps: The minimum download bandwidth value that is reserved for the service. The Min Kbps is a mandatory field.
- WAN to LAN Max Kbps: The maximum download bandwidth value that is reserved for the service. The Max Kbps field is optional and the value cannot be lesser than the configured min-

imum download bandwidth value. The value must be greater than or equal to the minimum download bandwidth value.

• WAN to LAN Grooming: If enabled, packets are randomly discarded to prevent WAN to LAN traffic from exceeded the Service's provisioned bandwidth.

Note

The minimum and maximum Kbps fields are not available for the Virtual Path.

Services			
Service Bandwidth Settings :	Link Specific \smallsetminus		
Service Name *	Allocation % *		Mode *
internet ~	50		primary ~
Tunnel Header Size (bytes)			
0	Access Intefa	ce Failover	
LAN to WAN			
Tagging	Max Delay (ms)		
None ~	500		
Min Kbps *		Max Kbps	
100			
WAN to LAN			
Tagging	Matching		
None ~	None	~	Grooming
Min Kbps *		Max Kbps	
100			
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 Path Enable Auto-Bandwidth Provisioning across all Virtu Max to Min Virtual Path Bandwidth Ratio for the Link 10 Minimum Reserved Bandwidth for each Virtual Path (Kbps) 80	IS: Link Specific v			
Custom Bandwidth Allocation for Virtual Paths Dynamic Virtual Paths Virtual Path	Bandwidth Allocation (Upload)	Bandwidth Allocation (Download)	Action	*
<				÷
Virtual Paths Remote Site Branch2	~			
Virtual Path MCN_PRIMARY_test - Branch2	Bandwidth Allocation (Upload)	Bandwidth Allocation (Download)	Action	*
			²	-

To customize the bandwidths for the virtual paths associated with a WAN link:

- 1. Clear the Enable Auto-Bandwidth Provisioning across all virtual paths associated with the link check box.
- 2. In the **Custom Bandwidth Allocation for Virtual Paths** section, select a remote site. You can provision bandwidths for the virtual paths to the remote site.
 - **Minimum Bandwidth (Kbps)**: The minimum bandwidth reserved for the virtual path. The minimum bandwidth that you can set for a virtual path is 80 Kbps.

- **Maximum Bandwidth (Kbps)**: The maximum bandwidth that the virtual path can utilize from the WAN link. If the maximum bandwidth is not set, the site utilizes all of the available bandwidth.
- **Bandwidth Allocation (Relative Measure)**: The bandwidth share allocated to a virtual path out of its group's eligible bandwidth. For example, if a WAN link group of 3 virtual paths is eligible for 30 Mbps bandwidth and you want to allocate equal bandwidth for each virtual path, update 10 as the bandwidth allocation on the remote site.

Upload			
Minimum Bandwidth (Kbps)			
80			
Maximum Bandwidth (Kbps)			
Bandwidth Allocation (Relative Measure)			
10	Weight		
Download			
Minimum Bandwidth (Kbps)			
80			
Maximum Bandwidth (Kbps)			
Bandwidth Allocation (Relative Measure)			
10	Weight		
		Cancel	Done

3. Click Done.

Note

Citrix SD-WAN Orchestrator service retains the previously configured custom bandwidth settings even after the previously configured dynamic virtual paths are disabled between two sites. Ensure to update the custom bandwidth settings manually when you reconfigure the dynamic virtual paths.

Points to consider for bandwidth provisioning

- By default, all branches and WAN services (Virtual Path/Internet/Intranet) receive a weightage of 1 each.
- Bandwidth customization is required when there is a high disparity in terms of bandwidth requirement.
- When dynamic virtual paths are enabled between the available sites, the WAN link capacity is shared between the static virtual path to the data center and the dynamic virtual paths.

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. The standby mode of a WAN link is disabled by default. For more information on standby mode, see Standby mode.

Advanced WAN Options	;	•
Enable Metering	Adaptive Bandwidth Detection	
Congestion Threshold (µs)	Provider ID	Frame Cost (Bytes)
20000		1
Standby Mode	MTU (Bytes)	
Disabled	✓ 1350	

• **Enable Metering**: Tracks usage on a WAN link and alerts the user when the link usage exceeds the configured data cap. For detailed information on metering, see Metering and Standby WAN Links.

Citrix SD-WAN Orchestrator

Advanced WAN Options		•
Enable Metering	ptive Bandwidth Detection	
Congestion Threshold (µs)	Provider ID	Frame Cost (Bytes)
20000		1
Standby Mode	MTU (Bytes)	
Disabled ~	1350	
Data Cap(MB)	Billing Cycle	Starting From
	monthly ~	MM/DD/YYYY
	Approximate Data Already Used (MB)	
Disable Link if Data Cap Reached	d O	

 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%.

For more information, see Adaptive bandwidth detection

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.

	erify Config 01 Site	Details 02 Device	e Details 03 Interfaces	04 WAN Links	05 Routes	06 Summary	
Applicat	tion Routes IP Rou	utes					
st Range	es: Custom Application	n (1-20) Application (2	21-40) Application Group (41-	60) IP (1-65535)			
+ App	lication Route		Search for Route		Q		
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	Ē
3	Application Group	Default SIA App	Secure Internet Access	Any	Global	45	1
4	Application Group	03650ptimize_In	Internet Breakout	Any	SiteA	50	1
5	Application Group	03650ptimize_In	Internet Breakout	Any	Global	50	Ī

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

Verify Config 0 Site Det	tails 02 Device Details	03 Interfaces	04 WAN Links	05 Routes	06 Summary
Application Routes IP Routes					
Cost Ranges: Custom Application (1-2	20) Application (21-40)	Application Group (41-60)) IP (1-65535)		
Application Match Criteria					
Match Type	Application *	Ro	outing Domain		
Application \lor	Gazeta.pl(gazeta)	~	Any	\sim	
Traffic Steering					
Delivery Service	Cost *				
Internet Breakout \lor	21				
Eligibility Based on Path					
Add Path					
Site Name	From Wan Link		To Wan Link		Actions
Cancel Save					

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.

Application 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 Any Default_RoutingDomain
Traffic Steering
Delivery Service Cost* Internet Breakout ✓ 5
Eligibility Criteria
Export Route
Eligibility Based on Path
Add Path
Site Name From Wan Link To Wan Link Actions
Cancel Save

Summary

This section provides a summary of the site configuration to enable a quick review before submitting the same.

Citrix SD-WAN Orchestrator

Verify C	config 01 Site	e Details 02 Device	e Details 🛛 🔞 Interfaces	04 WAN Links	05 Routes	06 Summary	
Site & Device D	etails						
Site Name	Device Model	Site Role	Serial Number	Bandwidth Tier			
mymcn	VPX	MCN	3065cea3-f6b8	1000 Mbps			
Interfaces LAN-1-1 • VLAN0-V WAN-1-2 • VLAN0-V	IF-1-LAN-1-Defa IF-2-WAN-1-Def	ault_RoutingDomain -1 fault_RoutingDomain -	92.168.1.1/24 172.16.1.2/24				
WAN Links						LAN-1 1	WAN-1 2Broadband-OTE-1
• AIF-1-VIF	I-OTE-1-1000 -2-WAN-1-172.16) Mbps↑ 1000 Mbp 6.1.2 -172.16.1.1 - primar	s↓ y			mymcn SDWAN-VPX (f	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.

Wi-Fi Access Point

January 15, 2021

You can configure a Citrix SD-WAN appliance that supports Wi-Fi as a Wi-Fi Access Point. Citrix SD-WAN appliance configured as a Wi-Fi access point eliminates the need to maintain an extra access point appliance to create a WLAN. The devices on your LAN can connect to Citrix SD-WAN appliance through Wi-Fi.

Note

Ensure that a DHCP server is available on the network to assign IP addresses to the host machines. If another DHCP server is not available on the network, you can configure the SD-WAN appliance as a DHCP server. For instructions, see DHCP server.

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 information about the platforms, see Citrix SD-WAN 110 SE.

Note

Wi-Fi feature does not support High Availability (HA) in Citrix SD-WAN 11.3 release.

You can configure and manage Citrix SD-WAN appliances that are configured as Access Points through Citrix SD-WAN Orchestrator service.

To configure Wi-Fi capabilities on a Citrix SD-WAN 110 appliance, ensure that the appropriate device model and submodel are selected on the **Configuration** > **Site Configuration** page.

Verify Config	01 Site Detail	5 02 Device Details	03 Wifi Details	04 Interfaces	05 WAN Links	06 Routes	07 Summa
Site Information							
Site Profile		Site Name *			Site Address *		Lat/Lng
None		✓ Branch1			Greece		
Region *	c	Device Model *	Sub-Mod	iel*	Device	Edition *	
Default-Region	~	110	✓ LTE-	WiFi	↓ SE		\sim
Site Role *	_	Bandwidth Tie	er (Mbps) *		Select Tag		Create New
Branch		~ 20		\sim			~
Advanced Settings							
Gateway ARP Timer (ms)		Host ARP Tim	er (ms)		Grable Cer		
1000 Preserve route to In	ternet from link e	1000 ven if all associated path	s are down		Enable Sou	irce MAC Learning	
Preserve route to In	tranet from link e	ven if all associated path	s are down				

Site Configuration:Basic Settings

Select **Enable Wi-Fi** on the **Wi-Fi Details** page, to make the Citrix SD-WAN 110 appliance act as a Wi-Fi Access Point.
Citrix SD-WAN Orchestrator

Verify Config	01 Site Details	02 Device D	0etails	03 Wi-Fi Detai	ls 04 Interface	es 05 W/	AN Links	06 Routes	07 Summary
Enable Wi-Fi									
Wi-Fi Settings: Radio									
Country			Band		Protocol				
Australia		~	2.4 0	GHZ 💿 5 GHZ	● 802.11n ○	802.11ac			
Channel			Channel W	idth					
Auto		\sim	20			\sim			
Australia Channel		~	Channel W	GHZ 💿 5 GHZ	● 802.11n ○	802.11ac			

Configure Wi-Fi radio settings

Configure the Wi-Fi radio settings by providing the following details.

• **Country**: The country where the appliance is deployed. The country determines the allowed wireless radio settings for that country.

Note

The **Country** field is locked to **USA and Canada** for appliances sold to USA and Canada. For appliances sold to other countries, the **Country** field is set to **Worldwide** by default, allowing you to choose the appropriate country.

- **Band**: The Citrix SD-WAN 110 appliance supports 2.4 GHz and 5 GHz frequency bands. The 5 GHz band provides greater performance than the 2.4 GHz band, but is not compatible with all wireless devices. Select the band and protocol based on the devices that connect to the Citrix SD-WAN appliance. The Citrix SD-WAN 110 appliance does not support dual band, you can only choose one band at a time.
- **Protocol**: Select the protocol based on the selected band. The 2.4 GHz band supports 802.11n protocol, whereas the 5 GHz band supports both 802.11n and 802.11ac protocol.

Note

The 802.11ac protocol is backwards compatible to 802.11n. It is recommended to use 802.11ac protocol, if 5 GHz band is selected.

• **Channel**: The available channels depend on the selected country and wireless protocol. By default, the channel is set to **Auto**. The Citrix SD-WAN appliance selects a channel with the least interference from the list available for the band. While not recommended, you can also manually select a channel, if necessary.

• **Channel Width**: You can configure the channel to use a channel width of 20 MHz, 40 MHz, or 80 MHz (for certain 5 GHz channels only). By default, the channel width is set to the maximum available channel width for the band and channel selected.

Configure SSID

The Service set identifier (SSID) is used to identify a wireless network profile to establish and maintain wireless connectivity. You can configure up to four SSIDs on the Citrix SD-WAN appliance. SSIDs help you to configure your wireless network with different security levels, serving different type of users such as corporate users, home users, or guests.

Note

The Wi-Fi radio settings are common to all the SSIDs.

Wi-Fi Settings: SSID		
SSID 1 SSID 2 SSID 3 SSID 4		
SSID Type Corporate Home SSID Name	Corporate SSID Profile No profile, start afresh ✓ SSID Broadcast Client Isolation	🔊 Reset
SSID1	● Enable ○ Disable ● On ○ Off	
Security WPA2 Enterprise	VLAN ID	
Primary Security Profile	Secondary Security Profile	
RADIUS-Profile1 V	RADIUS-Profile2 🗸	
Create Radius Profile Create Radius Save As Profile	Profile	
Cancel Save		Prev Next

To configure SSIDs, provide the following details:

- **SSID Type**: Citrix SD-WAN Orchestrator allows you to configure two types of SSID **Corporate** and **Home**. For a Corporate SSID it is recommended to create and use a Corporate SSID profile. For more details, see SSID profiles.
- **SSID Name**: A unique identifier for the wireless network profile. The SSID names are case sensitive and can contain up to 32 alphanumeric characters. Do not include leading or trailing spaces in your SSID name.

- **SSID Broadcast**: Enabling SSID broadcast makes the SSID name visible to all the devices in your network, allowing them to easily identify and connect to the Wi-Fi network. Disabling SSID broadcast makes the SSID name invisible to other devices. However, it only hides the name, not the network itself. Users that know the SSID name can still connect to your Wi-Fi network.
- **Client Isolation**: Client isolation prevents clients connected to the same SSID from communicating with each other. For open authentication, where untrusted clients may connect, it is recommended to set **Client Isolation** to **On**.
- Security: Citrix SD-WAN supports the following types of Wi-Fi security protocols:
 - **Open**: The Wi-Fi network is unsecure and anybody can connect to the wireless network. It is recommended to isolate open SSIDs to their own routing domain, to prevent untrusted clients from compromising personal (home) or corporate networks.
 - WPA2 Personal: The Wi-Fi Protected Access (WPA) 2 protocol, pre-shared key mode, commonly referred to as "personal", is used to secure the Wi-Fi network. With this protocol, you can configure a passphrase as a pre-shared key (PSK). Anybody that knows the SSID and passphrase can connect to your Wi-Fi network. This is typically used for home networks. It is recommended to isolate home SSIDs to their own routing domain, to prevent untrusted clients from compromising the corporate network.
 - WPA2 Enterprise: The Wi-Fi Protected Access (WPA) 2 protocol, enterprise version is used to provide enterprise-grade authentication to access your Wi-Fi network. A user name and password is required to log in. A RADIUS server authenticates the user name and password. You can select the Primary and Secondary RADIUS profiles, which point to a primary and secondary RADIUS server respectively. If the primary RADIUS server is down, the secondary server is used for authentication. For more information on creating RADIUS profiles, see RADIUS server profiles.

Note

Each site can have up to two RADIUS server profiles assigned on each WPA2 enterprise SSID.

- **WPA3 Personal**: Similar to WPA2 Personal, you use a PSK to connect to the network. It uses the latest version of the Wi-Fi Protected Access protocol. Only the devices that support WPA3 can connect to this network.
- WPA3 Transition: Allows WPA3 capable devices to connect using the new WPA3 security protocol, and the unsupported devices to continue to use the WPA2 security protocol. Devices that use WPA3 or WPA2 Personal version can use the same PSK to connect to this network.
- VLAN ID: Associates the SSID with a VLAN identifier. The VLAN identifier can be reused

when the SSID is assigned to a virtual interface, to associate it with an external VLAN or associate it with a distinct routing domain.

You can also save the Corporate SSID configuration as an SSID profile. It allows you to easily reuse and manage SSID configuration across multiple sites. For more details, see SSID profiles.

The SSIDs configured are reflected as virtual interfaces while configuring Interfaces. It further allows you to use the SSIDs in your SD-WAN configuration or enhance network security. For example, you can have a configuration to mark all the traffic over a particular SSID to belong to a particular routing domain or assigned to a specific VLAN. This routing domain can further be configured to have access to specific network and resources. If a combination of corporate, home, and guest wireless networks are configured, it is critical to associate them with different routing domains, to ensure tenant isolation and prevent rogue or compromised clients in one network from compromising the others.

Verify Config 01 Site Details 02 Device Details 03 Wi-Fi Details 04	Interfaces os V	VAN Links	06 Routes	07 Summa
Interface Attributes				
Deployment Mode * Interface Type * Security *		Interface Na	ame	
Edge (Gateway) V V Trusted	~	LAN-1		
Physical Interface				
Select Interface*]		<u>Link Aggreg</u>	ation Group
Virtual Interfaces				
VLAN ID * Virtual Interface Name * 0 VIF-1-LAN-1	Enable	e HA Heartbea	at	
+ IP V4 Addresses + IP V6 Addresses				
Type IP Address	Private	Link Local	Delet	е
IPv4 Eg: a.b.c.d/e		N/A		•

Site Configuration:Basic Settings

RADIUS server profiles

The WPA2 Enterprise protocol provides enterprise-grade authentication to your wireless network. A user name and password is required to log in into the wireless network using the WPA2 enterprise protocol. The user name and password is authenticated by a RADIUS server, which is configured using

RADIUS profiles. The RADIUS profiles can be applied to multiple sites while configuring SSIDs. For more details, see Configure SSIDs.

The RADIUS profiles are dynamic in nature. Any changes made to the RADIUS profile, will reflect across all the different sites where the RADIUS profile is used. Each WPA2 enterprise SSID can have up to two RADIUS server profiles assigned to it.

To manage RADIUS profiles, at the network level, navigate to **Configuration** > **Security** > **RADIUS Profiles**. A list of all the available RADIUS profiles are listed, you can edit or delete the profiles.



To create a RADIUS profile click **Add** and provide the following details:

- Radius Profile Name: A unique name to identify the RADIUS server profile.
- Auth Server IP: The IP address of the RADIUS authentication server. The authentication server might be located at the Data Center, accessible through the management interface or in-band management.
- Auth Server Port: The port number of the RADIUS authentication server. The default port number is 1812.
- Auth Server Secret: The secret passphrase to connect to the authentication server. Only the authorized clients that know the secret key can connect to the authentication server and send authentication requests.
- **NAS-identifier**: Configure the same Network Access Server (NAS) identifier on the RADIUS server and Citrix SD-WAN appliance. It allows the RADIUS server to identify the correct RADIUS client and perform the authentication. It is a Fully Qualified Domain Name. A special tag {SITENAME} is used. The tag is replaced in the NAS identifier with the respective site name for each site.

The RADIUS accounting server optionally collects network monitoring and statistics data. The accounting process starts when access to the RADIUS server is granted and if the Acct-Interim-Interval AVP is present in the RADIUS Access-Accept message. In this case, the Citrix SD-WAN RADIUS client reports session details such as total time, total data and packets transferred for every Acct-Interim-Interval seconds. The accounting server can be the same as the authentication server or a different server. To enable the optional RADIUS accounting capability select **Configure RADIUS accounting** and provide the following details.

- Account Server IP: The IP address of the accounting server.
- Account Server Port: The port number of the accounting server. The default port number is 1813.
- Account Server Secret: The secret passphrase to connect to the accounting server. Only the authorized clients that know the secret key can connect to the accounting server and send accounting requests.

← Create Radius Profile		
Radius Profile Name		
New Radius profile		
Auth Server IP/URL	Auth Server Port	Auth Server Secret
10.102.29.220	1812	
NAS Identifier		
{SITENAME}		
Configure Radius Accounting		
Account Server IP/URL	Account Server Port	Account Server Secret
120.202.3.29	1813	
Save		

You can also create a RADIUS profile directly from the **Wi-Fi details** page, while configuring sites. You can also perform operations such as edit, clone, and delete.

SSID profiles

The Service set identifier (SSID) is used to identify a wireless network profile to establish and maintain wireless connectivity. You can configure up to four SSIDs on the Citrix SD-WAN appliance. SSIDs help you to configure your wireless network with different security levels, serving different type of users such as corporate users, home users, or guests.

In large deployments, that uses corporate SSIDs, it is expected that the same SSID settings be replicated across numerous appliances. The commonly used settings can be stored as an SSID profile. The SSID profiles are dynamic in nature. Any changes made to an SSID profile, reflects across all the different sites where this SSID profile is used.

To manage SSID profiles, at the network level, navigate to **Configurations** > **Security** > **SSID Profiles**. A list of all the available SSID profiles are listed.

Citrix SD-WAN Orchestrator

🛞 CONFIGURATION 🗸 📩	Network Configuration Home / Security / Ssid Profiles				
Network Config Home Delivery Services > Routing >	Manage SSID Profiles This page is reserved to manage WiFi SSID Profiles across all si WiFi SSID Profiles Add	tes.			
Clink Secongs >					
Qos >	Profile	Created On	Actions		
Security V	Home network	November 10, 2020	1 😑		
Network Security	Office network	November 10, 2020	1 🗎		
Ssid Profiles	Guest network	November 10, 2020	N 🗎		
Radius Profiles	citrix	November 9, 2020	1		
Firewall Zones					
Firewall Defaults				Page Size: 25 V Showing 1 - 4 of 4 items	Pagel of 1 🔹 🕨
Firewall Profiles					

To create a new SSID profile click **Add**. For more details on configuring SSID, see Configure SSIDs. You can also perform operations such as edit, clone, and delete.

Wi-Fi diagnostics

To capture Wi-Fi traffic details, at the network level, navigate to **Troubleshooting > Diagnostics** and select the **Packet Capture** check box. Choose the appropriate Wi-Fi interface.

NOTE

Traffic between wireless clients is isolated from the data path in Citrix SD-WAN 110 platform and therefore is not part of the packet capture.

For detailed information on packet capture, see Diagnostics.

LTE firmware upgrade

December 16, 2020

Citrix SD-WAN Orchestrator service 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**.

Verify Config	01 Site Details	02 Device Details	03 Interfaces	04 WAN Links	05 Routes	06 Summary
Site Information						
Site Profile	Site Name *		Site Address *	Lat/Lng		
None	✓ Site_2	10	Kolkata, West B	engal, India		
Region *	Device Model *	Sub-Model *	Device E	dition*		
Default-Region $$	210	✓ LTE	∽ SE	~		
Site Role *	Bandwidth T	ïer (Mbps) *	Select Tag	Create New		
Branch	~ 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	Configuratio	on: Home						Site Group:	All		\sim
Software Ve	ersion : 11.2.2.	1005 🗸									
+ Add Si	ite Batch Add	Sites Deploy Config/Sof	tware Back	< Up/Review Ch	eckpoints	More Actions		Deployment Tracker	Searc	h	Q
Availabilit y	Cloud Connectivity	Site Name	Site Role	Device Model	Serial No		Bandwidth Tier	Management IP	Actio	ns	
•	Inactive	Branch_Azure_VPXL	Branch	VPXL-SE			200	Unknown	ø	Ō	•••
•	Inactive	RajanCube_210	Branch	210-SE			200	Unknown	ø	Ō	•••
•	Inactive	Siva_1100_Branch	Branch	1100-SE			300	Unknown	ø	Ō	•••
•	Inactive	Siva_2100_Branch	Branch	2100-SE			1000	Unknown	ø	Ô	•••
•	Online	Site_210	Branch	210-SE			200	Unknown	ø	Ō	•••
•	Online	Branch_VPX_Azure	Branch	VPX-SE	2867ACC5-D	DFD-4105	50	10.105.173.229	ø	Ō	•••
•	Online	MCN_Azure	MCN	VPX-SE	0000-0017-0	293-3041	1000	172.20.0.4	ø	Ō	•••
_	Online	Azure VPX Branch test	Branch	VPX-SE	0000-0015-9	237-3615	500	172.18.0.4	ø	n	
•	Online	Site_210	Branch	210-SE	V GF04KD	3EGW	100	10.140.3.67	ø	Ō	
					Page Size	e: 200 ∨	Showing 1-	9 of 9 items Pa	ge1 of1		• •
С											

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 filed is non-editable. Once you click **Stage**, it downloads all the appropriate LTE firmware for the selected software version.

	rify Config Current Deployme	nt Deployment History Chang	ge Management Settings		
oftware V	arsian : 11.2.2.1005				
Jitware ve	1.2.2.1005				
Stage	- Activ	vate 🗸 🗌 Ignore Inc	omplete		
					4/
		Sta	ged Appliances		
					4/
		Activ	vated Appliances		
Total Appliar	nces	Activ	vated Appliances	Failed	
Total Appliar 4	nces	Activ Staged 4	Activated Appliances	Failed O	
Fotal Appliar 4 Dnline	nces Site	Activ Staged 4 Status	Activated Appliances	Failed O HA State	Software Version
Fotal Appliar 4 Online Yes	Site MCN_Azure	Activ Staged 4 Status Activation Complete	Activated Appliances Activated 4	Failed 0 HA State Not Configured	Software Version
Total Appliar 4 Online Yes Yes	Site MCN_Azure Azure_VPX_Branch_test	Activ Staged 4 Status Activation Complete Activation Complete	Activated Appliances Activated 4	Failed 0 HA State Not Configured Not Configured	Software Version 11.2.2.1005.888881 11.2.2.1005.8888881
Total Appliar 4 Donline Yes Yes Yes	Site MCN_Azure Azure_VPX_Branch_test Branch_VPX_Azure	Activ Staged 4 Status Activation Complete Activation Complete Activation Complete	Activated Appliances	Failed 0 HA State Not Configured Not Configured Not Configured	Software Version 11.2.2.1005.888881 11.2.2.1005.888881 11.2.2.1005.888881
Total Appliar 4 Daline Yes Yes Yes Yes	Site MCN_Azure Azure_VPX_Branch_test Branch_VPX_Azure Site_210	Activ Staged 4 Status Activation Complete Activation Complete Activation Complete	Activated Appliances Activated 4	Failed 0 HA State Not Configured Not Configured Not Configured	Software Version 11.2.2.1005.888881 11.2.2.1005.888881 11.2.2.1005.888881 11.2.2.1005.888881

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.

- 5. Once the staging is completed, click **Activate** button to activate the software.
- 6. 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.

	erify Config	Current Deployment	Deployment History	Change Management Settings		
Scheduling	g Informatio	ı				
Site Name		HA State	Scheduling Informa	ation	Maintenance Mode	Actions
Azure_VPX_	_Branch_test	Not Configured	2021-01-04 at 21	1:20:00 (Maintenance window of 1 hours and repeated every 1		ø
Site_110		Not Configured	2021-01-04 at 21	1:20:00 (Maintenance window of 1 hours and repeated every 1		Ø
MCN_Azure	e	Not Configured	2021-01-04 at 21	1:20:00 (Maintenance window of 1 hours and repeated every 1		Ø
Branch_VPX	X_Azure	Not Configured	2021-01-04 at 21	:20:00 (Maintenance window of 1 hours and repeated every 1		Ø

In the scheduling window, a specific time frame is specified to complete the LTE software upgrade.

7. 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 Citrix SD-WAN Orchestrator service 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

December 16, 2020

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 (i)			
Gateway ARP Timer (ms	;)		
1000			
Host ARP Timer (ms)			
1000			
Save			

Neighbor discovery protocol

April 7, 2021

In an IPv6 network, Citrix SD-WAN appliances periodically multicast router advertisement messages to announce their availability and convey information to the neighboring appliances in the SD-WAN network. The router advertisements include the IPv6 prefix information. Neighbor Discovery protocol (NDP) running on Citrix SD-WAN appliances use these router advertisements to determine the neighboring devices on the same link. NDP also determines each other's link-layer addresses, finds neighbors, and maintains active neighbors reachability information.

To configure the NDP router advertisement, navigate to **Configuration > Advanced Settings > NDP** and click **+ NDP**.

Choose one of the configured virtual interfaces from the **Virtual Interface** drop-down list. Select **Enable Advertisement** to enable sending periodic router advertisements and responding to Router Solicitations for the selected virtual interface.

Specify the maximum, minimum, and router lifetime intervals.

- **Max Interval**: The maximum time (in seconds) allowed between sending periodic unsolicited multicast router advertisements.
- **Min Interval**: The minimum time (in seconds) allowed between sending periodic unsolicited multicast router advertisements.
- **Router Lifetime**: The time (in seconds) the router is considered valid by the hosts. 0 indicates the router cannot be used as the default router

Select **Managed Flag** if IP addresses are available through the DHCPv6 protocol. Select **Other Flag** if the configuration information (other than the IP addresses) is available through the DHCPv6 protocol.

Specify the following values for the selected interface.

- Link MTU: The recommended Maximum Transmission Unit (MTU) for the interface.
- **Reachable Time**: The time (in milliseconds) the NDP protocol stays in the **Reachable** state.
- **Retransmit Timer**: The time (in milliseconds) between retransmission of Neighbor Solicitation messages when resolving an IP address or probing a neighbor.
- Hop Limit: The maximum number of hops to be included in the router advertisement.

Click +Prefix List and enter the following values:

- **Prefix**: The prefix and prefix length in Classless Inter-Domain Routing (CIDR) notation.
- **Valid Lifetime**: The time in seconds up to which the prefix is valid. -1 represents infinity which means the prefix remains forever.
- **On-link**: When selected the prefix is considered as local to the network.
- **Autonomous Flag**: When enabled the prefix is used by the host's Stateless Address Autoconfiguration (SLAAC) to generate the IP address.
- Prefix Lifetime: The time (in seconds) up to which the prefix is considered as preferred.

NDP (i)

Virtual Interface *					
VIF-1-LAN-1		~	Enable Advertisement		
Max Interval (sec)	Min Interval (see	:)	Router Lifetime (sec)		
600	200		1800		
Link MTU					
0	Managed	Flag Othe	er Flag		
Reachable Time (ms)	Retransmit Time	er (ms)	Hop Limit		
0	0		0		
Prefix List					
+ Prefix List					
prefix	Valid Lifetime(Sec)	On-Link	Autonomous Flag	Preferred Lifetime (sec)	Actions
	2592000	Disabled	Disabled	604800	▣

Delivery Services

April 29, 2022

Delivery Services are delivery mechanisms available on Citrix SD-WAN to steer different applications or traffic profiles using the right delivery methods based on the business intent. The delivery services are defined globally and applied to WAN links at individual sites, as applicable.

Citrix SD-WAN Orchestrator service offers the following delivery Services at the site-level:

- Virtual paths
- Internet services
- Intranet services

Virtual paths

A virtual path is a logical link between two WAN links. It comprises 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 state of the reverse path.

To configure static virtual paths, from the site level, navigate to **Configuration** > **Advanced Settings** > > **Delivery Services** > Virtual Paths > Static Virtual Paths.



You can assign a route cost to the virtual path, for more information, see Virtual Path Route Cost

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 (%)**: This specifies the percentage of loss threshold before a path is marked BAD, as measured over the specified time. By default, the percentage is based on the last 200 packets received. When the packet loss exceeds the set percentage over the configured time, the GOOD Path state changes to BAD.

- **Over Time (ms)**: When the packet loss exceeds the set percentage over this configured time, the path state is marked as BAD.
- **Silence Period (ms)**: This specifies the duration (in milliseconds) before the path state transitions from GOOD to BAD. The default is 150 milliseconds. The path state transitions from GOOD to BAD when no packets are received within the specified amount of time.
- **Path Probation Period (ms)**: The period to wait before changing the path state from BAD to GOOD. The default is 10000 milliseconds.
- Instability Sensitive: Latency penalties due to BAD state and other spikes in latency are considered.

IP DSCP Tagging					
Any	\sim				
Bad Loss Sensitive		Percent Loss (%)		Over Time (ms)	
Enable	\sim	DEFAULT	\sim	1000	\sim
Silence Period (ms)		Path Probation Period (ms)			
DEFAULT	\sim	10000		✓ ✓ Instability Sen	sitive
				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 NATprotected client sites.

JDP Port	UDP Port V6	
4980	4980	
Alternate Port	Alternate Port V6	
Port Switch Interval (min)	Port Switch Interval V6 (min)	
1440	1440	
Funnel Header Size in Bytes		
0	Active MTU Detect	
Enable UDP Hole Punching	Enable UDP Hole Punching V6	

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 Set**tings > **Delivery Services**> Virtual Paths > **Dynamic Virtual Paths**.

Select **Site Specific Override** to override the virtual path settings inherited from the global wan link auto-path settings. The **Site Specific Override** option only allows you to enable or disable the dynamic virtual paths. You cannot create, remove, or configure the dynamic virtual paths from the site level.

Select **Enable Dynamic Virtual Paths** to allow the dynamic virtual paths between the configured site and other sites connected through an intermediate node. Using this option, you can enable both, dynamic virtual paths and member paths. Set the maximum allowable dynamic virtual paths for the site.

Citrix SD-WAN Orchestrator

Delivery Services ③						
Virtual Paths Internet Service Intranet Services						
Static Virtual Paths Dynamic Virtual Paths						
Dynamic Path Override Settings						
Site Specific Override \lor						
✓ Enable Dynamic Virtual Paths						
Max limit for Number of dynamic virtual paths						
3						
Active Member Paths						
Link	UDP Port	Alternate Port	Interval (min)	Actions		
Broadband-ATMNet-1	4980	0	1440	Ø		
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			
4980	1025			
Alternate Port	Alternate Port V6			
0	0			
Interval (min)	Interval V6			
1440	0			
LAN to WAN Throughput (Kbps) Throughput (pps)		WAN to LA Throughput (Throughput (AN	
			Cancel	Done
			ounoot	

Internet Service

An Internet service provides a 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 Internetbound traffic across multiple Internet links. You can set up only one Internet service for a site.

To configure Internet settings, from the site-level, navigate to **Configuration > Advanced Settings > Delivery Services > Internet Service**.

You can configure the Internet service globally for all the sites in the network, or specific to individual sites. By default, every site inherits the global Internet service settings and the **Internet Override Settings** drop-down list displays the **Global Default** option. If you want to override the global settings with site-specific settings, select the **Site Specific Override** option from the drop-down list. This option overrides the global Internet settings for a specific site by keeping the network with the default global configurations intact.

To configure site-specific Internet service settings, select **Enable** from the **Internet Service** dropdown list. You can further choose between global defaults and site-specific override settings for the following services:

- Override cost: Flag to override the Internet cost.
- **Internet cost**: The route cost used for the default Internet route added to the appliance. The route cost ranges from 1 to 65534.
- **Override Preserve Route**: Flags to override the Internet preserve route.
- Internet Preserve Route: When enabled, packets destined for the Internet service choose this service even if all the WAN links for this service are unavailable.
- **Override Primary Reclaim**: When enabled, the usage associated with the Internet service on a WAN link forcefully reclaims status as the active service on that WAN link.

You can configure the following ICMP services at site level and at network level:

- Determine Internet reachability from link using ICMP probes
- IPv4 ICMP endpoint address
- Probe interval (in seconds)
- Retries

For more information about ICMP probing, see Internet service.

Citrix SD-WAN Orchestrator

Delivery Services @			
Virtual Paths Internet Service Intranet Services			
Internet Settings			
Internet Override Settings	Internet Service		
Site Specific Override 🗸	Enable	~	
Override Cost	Internet Cost		
Site Specific Override 🗸 🗸	5		
Override Preserve Route	Internet Preserve Route		
Site Specific Override 🗸 🗸	Disable	~	
Override Primary Reclaim	Internet Primary Reclaim		
Site Specific Override 🗸	Disable	~	
Override Global Internet ICMP Probes Settings			
Determine Internet reachability from link using ICMP probes			
IPv4 ICMP endpoint Address *			
Enter ICMP endpoint Address			
Probe interval()n seconds) Retries			
5 3			
WanLinks Settings			
WanLink Name	Ν	Aode	Actions
Internet-ATT-2	В	lalance	•••

WAN link settings

To update the **WAN link** settings for an Internet service:

- 1. In the **WanLinks Settings** section, navigate to **Actions** > **Edit**. The **Update Wan Link Settings** page is displayed.
- 2. Update the fields as required. This page provides a complete list of services and the bandwidth allocation of the services configured for the site. You can modify the bandwidth allocation of the Internet service by updating the **Allocation%** column. The total allocation percentage of all the services put together cannot exceed 100%.
- 3. You can set the minimum/maximum upload and download bandwidth value for Internet services. The **Min Kbps** is a mandatory field. The **Max Kbps** field is optional and the value cannot be lesser than the configured minimum download/upload bandwidth value. The value must be greater than or equal to the minimum download/upload bandwidth value.
- 4. Click Done.

Note

If an Internet WAN link is in the **Global Default** mode, you cannot update the service allocation. This allocation is applicable only if the WAN link is in the **Site Specific Override** mode.

Intranet Service

An Intranet service provides an underlay link-based connectivity from an SD-WAN site to any non-SD-WAN site. The traffic is unencapsulated or you can use any non-virtual path encapsulation such as IPsec, GRE. You can set up multiple Intranet services for a site.

To configure the **Intranet** settings, from the site-level, navigate to **Configuration** > **Advanced Settings** > **Delivery Services** > **Intranet Service**.

You can configure Intranet settings for a specific site. The **Site Specific Override** option on the **In-tranet Override Settings** drop-down list configures Intranet settings for a specific site.

When you enable the **Intranet Service** option for a specific site, you can further choose between global defaults and site-specific override settings for the following services:

- **Override Preserve Route**: Flags to override the Intranet preserve route.
- Intranet Preserve Route: When enabled, packets destined for the Intranet service choose this service even if all the WAN links for this service are unavailable.
- Override Primary Reclaim: Flag to override primary reclaim.
- Intranet Primary Reclaim: When enabled, the usage associated with the Intranet service on a WAN link forcefully reclaims status as the active service on that WAN link.

Configuration / Advanced Settings / Delivery Services		Verify	Configuration Software Version : 11.4.1.27-GA
Delivery Services ①			
Virtual Paths Internet Service Intranet Services			
Service Name			
Intranet1 ~			
Intranet Override Settings	Intranet Service		
Site Specific Override 🗸 🗸	Enable	~	
Override Preserve Route	Intranet Preserve Route		
Site Specific Override 🗸 🗸	Enable	\sim	
Override Primary Reclaim	Intranet Primary Reclaim		
Site Specific Override 🗸 🗸	Enable	~	
WanLinks Settings			
WanLink Name		Mode	Actions
Internet-ATT-2		Primary	
Intranet-ATT-1		Primary	
Cancel Save			

WAN link settings

To update the **WAN link** settings for an Intranet service:

- 1. Navigate to the WANLinks Settings section.
- Select an Intranet service and click Actions > Edit. The Update Wan Link Settings page is displayed.
- 3. Update the fields as required. This page provides a complete list of services and the bandwidth allocation of all the services configured for the site. You can modify the bandwidth allocation of the Intranet service by updating the **Allocation%** column. The total allocation percentage of all the services put together cannot exceed 100%.
- 4. You can set the minimum/maximum upload and download bandwidth value for Intranet services. The **Min Kbps** is a mandatory field. The **Max Kbps** field is optional and the value cannot

be lesser than the configured minimum download/upload bandwidth value. The value must be greater than or equal to the minimum download/upload bandwidth value.

5. Click Done.

Note

- The WanLinks Settings section under Intranet Services displays both, Internet and Intranet service settings configured for a specific site. It does not display just the Intranet settings.
- If an Intranet WAN link is in the Global Default mode, you do not have an option to update the service allocation. This allocation is applicable only if the WAN link is in the Site Specific Override mode.

Update Wan Link Set	tings-Intranet-ATT-	1				
Service Name*		Mode *				
Intranet2		Select mode 🗸 🗸				
Tunnel Header Size (bytes)						
0		Access Inteface Failover				
-LAN to WAN						
Tagging		Max Delay (ms)				
None	~	500				
WAN to LAN	Matching V None	Grooming				
Service Name	Allocation %	Services Allocation				
Intranet1	20					
Intranet2	0					
Virtual Path	80					

Prefix delegation groups

April 7, 2021

Citrix SD-WAN appliances can be configured as a DHCPv6 client to request a prefix from the ISP using the configured WAN port. Once the Citrix SD-WAN appliance receives the prefix, it uses the prefix to create a pool of IP addresses to cater to the LAN clients. The Citrix SD-WAN appliance then behaves as a DHCP server and advertise the prefix on the LAN ports to the LAN side clients.

To configure prefix delegation, navigate to **Configuration > Advanced Settings > Prefix Delegation Groups** and click **+ Prefix Delegation Groups**.

Choose a configured WAN Virtual Interface on which the prefix is requested from the ISP and provide the following details:

- LAN Virtual Interface: Select one of the configured LAN virtual interfaces for which the prefix is requested.
- Prefix Length: The number of bits of a Global Unicast IPv6 address that are part of the prefix.
- Interface IP Host Portion: The host portion to be used for the interface IP address.
- **Prefix ID**: A unique identifier to identify the prefix delegation requests for the LAN interface.

Prefix Delegation Groups ③

Prefix Delegation Group				
WAN Virtual Interface *				
Select WAN Virtual Interface		\sim		
Prefix Delegation List				
LAN Virtual Interface *			Prefix Length	
Select LAN Virtual Interface		\sim	64	
Interface IP Host Portion	Prefix ID			
Save Prefix Delegation List	Cancel			

Appliance settings

June 28, 2022

Citrix SD-WAN Orchestrator service 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.

Note

The option to configure appliance settings is not available while creating or editing a site template.

If HA is configured, select the primary or secondary appliance for which you want to change the appliance settings.

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.



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		\sim
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 Passwo	ord		
User Name *				
admin		\sim		
Current Password	l			
•••••				
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.

G	Administrator Interface	NetFlow Host Settings	Network Adapters	AppFlow Host S	ettings	SNMP	Fallback Configuration
User Accounts	RADIUS TACACS+						
Radius Setting	gs						
✓ Enable RAI	DIUS						
Server 1:	IP Address 10.102.72.41		Authentication Port* 1812				
Server 2:	IP Address 10.102.72.56		Authentication Port 1812				
Server 3:	IP Address		Authentication Port				
Server Key:							
Confirm Serve	r Key:						
Timeout:	10						
Save	l						

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 RAD	DIUS TACACS+	
Tacacs Settings		
Enable TACACS		
	IP Address*	Authentication Port*
Server 1:	10.102.75.41	49
	IP Address	Authentication Port
Server 2:	10.102.75.46	49
	IP Address	Authentication Port
Server 3:		
Authentication Type:	• PAP ASCII	
Server Key:		
Confirm Server Key:	•••••	
Timeout:	10	
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 <u>Multiple NetFlow Collector</u>. 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 S	Settings		
✓ Enable NetF	low		
	IP Address*	Port*	
NetFlow Host 1:	10.102.72.41	2055	
	IP Address	Port	
NetFlow Host 2:			
	IP Address	Port	
NetFlow Host 3:			
Save			

Network adapters

For Citrix SD-WAN appliances, you can manually change the management network preference, 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.
- The In-band option works only if you have configured a data port as the In-band management port and Internet service is configured. Ensure that you have the configuration to support In-band management for the SD-WAN appliance, prior to setting the management preference.
- The Management Network Preference (In-band and Out-of-band) section is visible if the appliance is running a software version of 11.4.2 or later.

To configure the network adapter settings, navigate to **Configuration** > **Appliance Settings** > **Network Adapter**.

Administrative NetFlow NetFlow SNN	P Falback DateTime Systeg Overlay Soft-Reset Actions Ce	tificate Authentication Mubile Broadband Status Mobile Broadband Settings
Management Network Proference		
Out-Of-Band In-Band		
P Address		
tPr4 Protocol ⊘ Dratis Pr4 Dratis Pr4		
V Endta DHCP P Ablivia	Submit Weak	Category P. Address
Brvd Protocol Cruster Brvd		
Dividia SILARC		
Pril Address		Pode
DNS Settings		
Prenary Drds	Secondary Onli	
See		

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.

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**

Citrix SD-WAN Orchestrator

UDP Port: 161 System Description: Citrix Virtual WAN Appliance System Contact: support@citrix.com System Location: Citrix System Location: Citrix System Location: Citrix ShMP v1/v2 Pable v1/v2 Agent Community String: public Impose Impose Impose ShMP v3 Impose	NMP
161 System Description: Citrix Virtual WAN Appliance System Contact: support@citrix.com System Location: Citrix ShMP v1/v2 Enable v1/v2 Agent Community String: public Enable v1/v2 Traps Destination IP Address(es): 162 SNMP v3 Enable v3 Agent User Name: Image: Authentication: MD5 Enable v3 Traps Destination IP Address(es): Image: Image: Sume: Image: Sume: Image: Image: Sume: Image: Sume: Image: Image: Sume: Image: Sume: Image: Sume: Image: Sume: Image: Sume: Image: Sume: Image: <td>DP Port:</td>	DP Port:
System Description: Citrix Virtual WAN Appliance System Contact: Support@citrix.com System Location: Citrix SNMP v1/v2 Citrix SNMP v1/v2 Community String: public Community String: public Community String: public Community String: public Community String: public Community String: public Community String: public Community String: public Community String: public Community String: Community String: Port: 162 SNMP v3 Community String: Community String: Co	161
Citrix Virtual WAN Appliance System Contact: Support@citrix.com System Location: Citrix ShMP v1/v2 Enable v1/v2 Agent Community String: public public Destination IP Address(es): Enable v3 Agent User Name: ShMP v3 Password: Import Interference MD5 Enable v3 Traps Destination IP Address(es): Import Interference ImportInter Import	vstem Description:
System Contact: support@cltrix.com System Location: Citrix SIMP v1/v2 Enable v1/v2 Agent Community String: public Enable v1/v2 Traps Destination IP Address(es): [Port: 162 SIMP v3 Enable v3 Agent User Name: [Password: [Authentication: MD5 Encryption: None Enable v3 Traps Destination IP Address(es): [Port: 162 Destination IP Address(es): [Port: 162 Destination IP Address(es): [Port: 162 Destination IP Address(es): [Password: [Password: [Password: [Password: [Port: 162 Destination IP Address(es): [Port: 162 Destination IP Address(es): [Port: 162 Destination IP Address(es): [Port: 162 Destination IP Address(es): [Port: 162 Destination IP Address(es): [Port: [Password:	Citrix Virtual WAN Appliance
support@citrix.com System Location: Citrix SNMP v1/v2 Enable v1/v2 Agent Community String: public Destination IP Address(es): IC SNMP v3 Enable v1/v2 Traps Destination IP Address(es): IC SNMP v3 Enable v3 Agent User Name: IC None IC None Enable v3 Traps Destination IP Address(es): IC None IC IC None IC	stem Contact:
System Location: Citrix Citrix SNMP v1/v2 Enable v1/v2 Agent Community String: public public Enable v1/v2 Traps Destination IP Address(es): Enable v3 Agent User Name: Password: Community String Password: Community String SNMP v3 Community String SNMP v3 Community String SNMP v3 SNMP v3 Community String SNMP v3 SNMP v3 Community String SNMP v3 Community String SNMP v3 SNMP v3 Community String SNMP v3 SNMP v3 Community String SNMP v3 SNMP v3	support@citrix.com
Citrix SNMP v1/v2 Enable v1/v2 Agent community String: public Enable v1/v2 Traps Destination IP Address(es): 162 SNMP v3 Enable v3 Agent User Name: 0 Verify Password: 162 Authentication: MD5 Encryption: None Enable v3 Traps Destination IP Address(es): 162 Verify Password: 162 Varies User Name: Verify Password: Verify Password: 162 Verify Password: 163 Verify Password: 164 Verify Password: 165 Verify Password:	stem Location:
SNMP v1/v2 Enable v1/v2 Agent Community String: public public Enable v1/v2 Traps Destination IP Address(es): 162 SNMP v3 Enable v3 Agent User Name: 162 SNMP v3 Carl of the string	Citrix
Enable v1/v2 Agent Community String: public public Enable v1/v2 Traps Destination IP Address(es): Enable v3 Agent User Name: Password: Finable v3 Agent User Name: Enable v3 Traps Destination IP Address(es): Enable v3 Traps Destination IP Add	I NMP v1/v2
Community String: public public Enable v1/v2 Traps Destination IP Address(es): 162 SNMP v3 Enable v3 Agent User Name: Password: MD5 Encryption: None Encryption: None Encryption: None Encryption: None Encryption: None Encryption: None Encryption: None Encryption: None Encryption: None Encryption: None Encryption: Password: Passwo	Enable v1/v2 Agent
public Enable v1/v2 Traps Destination IP Address(es): 162 SNMP v3 Enable v3 Agent User Name: 102 Verify Password: Enable v3 Traps Destination IP Address(es): Image: Password: Encryption: None Enable v3 Traps Destination IP Address(es): Image: Image: Image: Verify Password: Image: Verify Password: Image: Password: Image:	mmunity String:
	public
Destination IP Address(es): Port: 162 SNMP v3 Enable v3 Agent User Name: Password: Authentication: MD5 Encryption: None Encryption: None Encryption: None Encryption: None Encryption: None Encryption: None Encryption: None Encryption: None Encryption: None Encryption: None Encryption: None Encryption: Password: Passwor	Enable v1/v2 Traps
Port: 162 SNMP v3 Enable v3 Agent User Name: Image: Verify Password: Image: Authentication: MD5 Encryption: None Enable v3 Traps Destination IP Address(es): Image: Image: Image: User Name: Image: Image: Verify Password: Image:	stination IP Address(es):
Port: 162 SNMP v3 Carl Agent User Name: Password:	
162 SNMP v3 Enable v3 Agent User Name: Password: Image: Verify Password: Image: Authentication: MD5 Encryption: None Enable v3 Traps Destination IP Address(es): Image: Image: Verify Password: Image: Verify Password: Image: None	ert:
SNMP v3	162
Enable v3 Agent User Name: Password: Authentication: MD5 Encryption: ncryption: Encr	NMP v3
User Name: Password: Password: Verlfy Password: MD5 Encryption: None Encle v3 Traps Destination IP Address(es): 162 User Name: Port: 162 User Name: Verlfy Password: Password: Authentication:	Enable v3 Agent
Password: Image: Constraint of the system of the	er Name:
Password: Verify Password: Authentication: MD5 Encryption: Encryption: Enable v3 Traps Destination IP Address(es): Enable v3 Traps Destination IP Address(es): Port: Enable v3 Traps Destination IP Address(es): Enable v3 Traps Address(es): Enable v3 Traps Destination IP Address(es): Enable v3 Traps Enable v3 Traps Destination IP Address(es): Enable v3 Traps Destination	
Varify Password: Authentication: MD5 Encryption: None Enable v3 Traps Destination IP Address(es): Info Varify Password: Verify Password: Authentication:	issword:
Verify Password: Verify Password: Authentication: MD5 Encryption: None Encryption: Encable v3 Traps Destination IP Address(es): Ioure Port: Ioure Ioure Ioure Verify Password: Ioure Authentication: Ioure I	
Authentication: MD5 Encryption: None Encryption: Port: 162 User Name: Encryption: Encryption: Password: Encryption:	rify Password:
Authentication: MD5 Encryption: None Enclose v3 Traps Destination IP Address(es): 162 User Name: Password: Password: Verify Password: Authentication:	
MD5 Encryption: None Enable v3 Traps Destination IP Address(es): 162 User Name: 94 Port: 162 User Name: 94 Verfy Password: 94 94 94 94 94 94 94 94 94 94 94 94 94	uthentication:
Encryption: None Encryption: None Encryption: Encrypti	MD5 \sim
None Enable v3 Traps Destination IP Address(es): Port: 162 User Name: Password: Verify Password: Authentication:	cryption:
Enable v3 Traps Destination IP Address(es): Fort: 162 User Name: Password: Verify Password: Authentication:	None ~
Destination IP Address(es): Port: 162 User Name: Password: Verify Password: Authentication:	Enable v3 Traps
Port: 162 User Name: Password: Verify Password: Authentication:	estination IP Address(es):
Port: 162 User Name: Password: Output Verify Password: Authentication:	
162 User Name: Password: Uerify Password: Authentication:	rt:
User Name: Password: Verify Password: Authentication:	162
Password: Verify Password: Authentication:	er Name:
Password: Verify Password: Authentication:	
Verify Password:	issword:
Verify Password:	
Authentication:	erify Password:
Authentication:	
	uthentication:
MD5	MD5 ~
Encryption:	cryption:
None	None ~
Save	Save

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.



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.



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.

Citrix SD-WAN Orchestrator

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.

Purge All Current Flows
Note: Purging flows may disconnect network connections, thereby requiring those connections to be reestablished.
Purge All Flows

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

INTE 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		

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

NTF 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		
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

Syslog server settings

You can configure Syslog server settings of SD-WAN appliances using Citrix SD-WAN Orchestrator service. By enabling Syslog settings, you can send system alerts and event details of SD-WAN appliances to an external Syslog server. However, you must select the event type on the SD-WAN appliance UI by navigating to **Configuration > Appliance Settings > Logging/Monitoring > Alarm Options**. For more information, see Configure Alarms.

	Admin Interface	NetFlow	Network Adapters	AppFlow	SNMP	Fallback	DateTime	Syslog	Overlay Soft-Reset Actions	Mobile Broadband Status
Syslog	Server Setting	;s								
🗸 Ena	ble Syslog Messages									
Server IF	P Address									
34.	14.53.44									
Server P	ort									
564	6									
🗸 Aut	hentications to Syslog	g								
🗸 Fire	ewall Logs to Syslog									
Sa	ave									

The following Syslog server settings are configurable through Citrix SD-WAN Orchestrator service:

- Enable Syslog Messages: Enable or disable sending logs or event messages to Syslog server.
- Server IP Address: IP address of the Syslog server.
- Server Port: Port number of the Syslog server.
- Authentication to Syslog: Enable or disable sending authentication logs or event messages to the Syslog server.
- Firewall Logs to Syslog: Enable or disable sending firewall logs to the Syslog server.

Certificate authentication

Citrix SD-WAN Orchestrator service ensures that secure paths are established between appliances in the SD-WAN network by using security techniques such as network encryption and virtual path IPsec tunnels. In addition to the existing security measures, certificate based authentication is introduced in Citrix SD-WAN Orchestrator service.

Certificate authentication allows organizations to use certificates issued by their private Certificate Authority (CA) to authenticate appliances. The appliances are authenticated before establishing the virtual paths. For example, if a branch appliance tries to connect to the data center and the certificate from the branch does not match with the certificate that the data center expects, the virtual path is not established.

The certificate issued by the CA binds a public key to the name of the appliance. The public key works with the corresponding private key possessed by the appliance identified by the certificate.

To enable appliance authentication, at network level, navigate to **Configuration** > **Security** > **Network Security** and select **Enable Appliance Authentication**. Click **Save**.

Network Security (1)							
Network Security Settings							
Encryption							
AES-128 ~							
Enable Encryption Key Rotation							
Enable Extended Packet Encryption Header							
Enable Extended Packet Authentication Trailer							
Extended Packet Authentication Trailer Type							
✓							
Enable FIPS Mode							
C Enable Appliance Authentication							
Save							
Network Secure Key							
Regenerate							

During deployment, if the appliance authentication is enabled but a PKI certificate is not installed in the appliance, then the staging shows failed status.

urrent Deploy	Deployment History	Change Management S	ettings Site Details					
Software Ve	rsion : V							
Cancel	Stage	×	Activate	Ignore Incomp	ete		(Settings
0/2								
				Staged Appliances				
0/2								
				Activated Appliances				
Total Applian	ces	Ready For Activation	Activated		Failed		OffLine	
2		0	0		1		0	
				5	Search			Q
							Export at	CSV Export as PD
Online	Site	Status				HA State	Software Version	Actions
Yes	S1	Staging in Progress				Not Configured	100 million (100 million)	50
Yes	S2	Staging Failed(ER613	3-PKI Cert Not Installed)	h		Not Configured	10.000	5
				.	P	age Size: 50 V Showin	g 1-2 of 2 items Page	1 ofī - →

View certificate

You can go to the device detail page to verify if the PKI Certificate is installed or not. To do that, navigate to **Configuration** > **Network Home** > click the **Action** symbol for the site you want to verify the certificate > click **View Details**.

Network Sites										All 🗸 🗸	d Sites 🗸 🗸	More
2 TOTAL SITES	0 CRITICAL	0 WARNING	2 NORMAL	0 INACTIVE	0 UNKNOWN				Search			Q
											Export	t as CSV Export as PDF
Site Name						Role	Overlay Status	Model	Bandwidth Tier	Orchestrator Connectivity	Serial No	Actions
S1						MCN	NORMAL	VPX-SE	500 Mbps	PRIMARY ACTIVE ONLINE	826EBE8	View Details
S2						Branch	NORMAL	VPX-SE	500 Mbps	PRIMARY ACTIVE ONLINE	92295A28	Clone
												Delete
									Dage Si	50 V Showing 1.2 of	2 items Da	Reboot
									Page 50	ter ov - anowing 1-2 of	e noons Pa	Reset
												Update Password

The following screen populates with the site and device details:

Site Name	S2
Site Role	Branch
Device Model	VPX-SE
Sub-Model	BASE
Bandwidth Tier	500
Device Details	
Device Name	Primary
Orchestrator Connectivity	Yes
	REPORT OF ALL ALL ALL ALL ALL ALL ALL ALL ALL AL
Serial No.	
Serial No. Management IP	11-12-10-10

Under the **Device Details** section, you can view the PKI certificate installation status.

Upload identity bundle

The Identity bundle includes a private key and the certificate associated with the private key. You can upload the appliance certificate issued by the CA into the appliance. The certificate bundle is a PKCS12 file, with .p12 extension. You can choose to protect it with a password. Drag and drop the PKCS12 file, enter a password and click **Upload**. If you leave the password field blank, it is treated as no password protection.

Upload Certificate Authority Bundle (PKCS12)
Click here or drag and drop a Certificate Authority Bundle to upload. Allowed file types are .p12
Upload

Upload certificate authority bundle

Upload the PKCS12 bundle that corresponds to the certificate signing authority. The certificate authority bundle includes the complete chain of signatures, the root, and all the intermediate signatory authority. Drag the PKCS12 bundle and click **Upload**.



Create certification signing request

The appliance can generate an unsigned certificate and create a Certificate Signing Request (CSR). To create a CSR for an appliance, provide the organization name, unit, town/city, province/region/-county/city, country, and email address. The appliance common name is the site name that is auto populated and non-editable. Click **Create CSR**.

Common Name:	Business name / Organization: *							
S2								
Department Name / Organizational Unit:*	Town / City: *							
Province, Region, County or State: *	Country: "							
Email address:*								
Create CSR								

Manage certificate signing request

Once the CSR is generated successfully from the back end, you need to download the CSR from the appliance and get it signed by its CA, upload it back to the appliance in PEM or DER formats. This is used as an Identity certificate for the appliance. First upload the CA to sign the certificate.

Upload Certificate Authority Bundle (PKCS12)	
Click here or drag and drop a Certificate Authority Bundle to upload. Allowed file types are .p12	
cert.p12	
Upload Syccessful	

Once the CA is uploaded, upload the signed CSR.

Manage Certificate Signing Request (CSR)	Manage Certificate Signing Request (CSR)										
Certificate Signing Request: Download CSR											
Click here or drag and drop a Signed CSR to upload. Allowed file types are .pem, .der											
servercert.pem Upload Successful	Ą										

Certificate revocation list manager

A Certificate Revocation List (CRL) is a published list of certificate serial numbers that are no longer valid in the network. The CRL file is periodically downloaded and stored locally on all the appliance. When a certificate is being authenticated the responder examines the CRL to see if the initiators certificate was revoked already. Citrix SD-WAN currently supports version 1 CRLs in PEM and DER format.

To enable CRL, select the CRL enabled check box. Provide the location where the CRL file is maintained. HTTP, HTTPS, and FTP locations are supported. Specify the time interval to check and download the CRL file, the range is 1–1440 minutes. Click **Upload Settings**.

Certificate Revocation List Management (CRL)	
CRL Enabled:	
CRL URI:	
http://example.com	
CRL Update Interval (Minutes): *	
300	
Update Settings	

Note

The reauthentication period for a virtual path can be between 10–15 minutes, if the CRL update interval is set to a shorter duration, the updated CRL list might include a currently active serial number. Make an actively revoked certificate available in your network for a short duration.

Mobile broadband settings

Citrix SD-WAN Orchestrator service allows you to connect a Citrix SD-WAN appliance from your branch site to a network using a mobile broadband connection.

To configure the mobile broadband settings, at the site level, navigate to **Configuration > Appliance** Settings > Mobile Broadband Settings.

Currently, the mobile broadband settings can be configured on Citrix SD-WAN 110 and Citrix SD-WAN-210 appliances.

You can configure the following mobile broadband settings on Citrix SD-WAN Orchestrator service.

SIM PIN status

If you have inserted a SIM card that is locked with a PIN, the SIM state is **Enabled**. You cannot use the SIM card until it is verified using the SIM PIN. You can obtain the SIM PIN from the carrier. Click **Verify**.

Enter the SIM PIN provided by the carrier and click **Verify**.

Disable SIM PIN You can disable SIM PIN functionality for a SIM for which SIM PIN is enabled and verified. Click **Disable**. Enter the SIM PIN and click **Disable**.

Enable SIM PIN To enable the SIM PIN, click **Enable**. Enter the SIM PIN provided by the carrier and click **Enable**.

If the SIM PIN state changes to **Enabled and Not Verified**, it means that the PIN is not verified, and you cannot perform any operations until the PIN is verified.

Click **Verify PIN**. Enter the SIM PIN provided by the carrier and click **Verify PIN**.

Modify SIM PIN Once the PIN is in **Enabled and Verified** state you can choose to change the PIN.

Click **Modify**. Enter the SIM PIN provided by the carrier. Enter the new SIM PIN and confirm it. Click **Modify**.

Unblock SIM If you forget the SIM PIN, you can reset the SIM PIN using the SIM PUK obtained from the carrier.

To unblock a SIM, click **Unblock**. Enter the SIM PIN and SIM PUK obtained from the carrier and click **Unblock**.

Note

The SIM card gets permanently blocked with 10 unsuccessful attempts of PUK, while unblocking the SIM. Contact the carrier service provider for a new SIM card.

APN settings

To configure the APN settings, enter the APN, username, password, and authentication provided by the carrier. You can choose from **PAP**, **CHAP**, or **PAPCHAP** authentication protocols. If the carrier has not provided any authentication type, set it to **None**.

Network settings

You can select the mobile network on Citrix SD-WAN appliances that support internal modems.

Roaming

The roaming option is enabled by default on your devices. You can choose to disable it.

Manage Firmware

Every appliance that has LTE enabled will have a set of available firmware. You can select from the existing list of firmware or upload a firmware and apply it. If you are unsure of which firmware to use, select the AUTO-SIM option to allow the LTE modem to choose the most matching firmware based on the SIM card inserted in the appliance.

Note

Currently, the firmware can be applied only on SD-WAN SE 210 LTE appliances.

Enable/Disable modem

Enable or disable the modem depending on your intent to use the broadband functionality. By default, the modem is enabled.

Reboot modem

Reboots the modem. This process can take up to 3-5 minutes for the reboot operation to complete.

Refresh SIM

Use this option when you hot swap the SIM card to detect a new SIM card.

	Admin Interface	NetFlow	Network Adapters	AppFlow	SNMP	Fallback	DateTime	Syslog	Overlay Soft-Reset Actions	Certificate Authentication	Mobile Broadband Status	Mobile Broadband Settings
Mob	le Broadband Oj	perations										
Mode	т Туре											
I	nternal Modem			~								
	SIM PIN Status (S	IM One)										
	PIN State	N/A										
	PIN Retries Remaining	- 1 										
	Enable	Verify	Modify	Unblock								
	LINDIO	, and a second sec	moonly	Chibitook								
	APN Settings											
	4.04			Authenticett								
	arn			None			\sim					
	Username			Password								
	Apply											
Ne	work Settings											
Net	rork Mode											
	4G		~									
	Apply											
Ro	aming											
Roa	ning Status											
	Disabled		\sim									
	Apply											
Ма	nage Firmware											
	Click here to selec	t the file or dr	ag and drop the selec	ted file.								
Aval	able Firmwares											
	02.33.03.00_TELSTRA			~								
	Apply Delete											
Enab	Enable/Disable Modem											
	Disable											
Daha	at Madam											
Rebo	or wodem											
	COOL											
SIM	Card (SIM One)											
, I	lefresh SIM											

Mobile broadband status

The Mobile broadband status section displays the status of your broadband configuration settings. To view the mobile broadband status, at the site level, navigate to **Configuration** > **Appliance Settings** > **Mobile Broadband Status**. You can view the status of your device and the active SIM.

Admin Interface NetFlow Network Adapter Mobile Broadband Settings	s AppFlow SNMP	Fallback	DateTime S	yslog	Overlay Soft-Reset Actions	Certificate Authentication	Mobile Broadband Status
lobile Broadband Status							
Modem Type	Status Of						
Internal Modem	✓ Device				\sim		
Status							
Active SIM			SIM Two				
Data Service Capability			non-simultan	eous-cs-	ps		
ESN			0				
Expected Data Format			802-3				
Hardware Revision			10000				
IMEI			0157240000	10437			
MEID			8676980403	8963			
MSISDN							
Manufacturer			QUALCOMM	INCORPO	DRATED		
Max RX Channel Rate (bps)			10000000				
Max TX Channel Rate (bps)			5000000				
Model			QUECTEL Mo	bile Broa	dband Module		
Modem Mode			QMI				
Networks			gsm umts Ite				
Operating Mode			online				
Operating Mode HW Restricted			0				
PRL Only Preference			0				
PRL Version			0				
Revision			EG25GGBR0	7A07M20	3		
SIM Capability			supported				
Software Version			EG25GGBR0	7A07M20	à		
Туре			110-WIFI-LTE				

Ethernet Interface Settings

The Ethernet Interface status section displays the connectivity status of the ethernet ports, Interface type, MAC address, auto negotiate, and the duplex setting information. To view the ethernet interface settings, at the site level, navigate to **Configuration** > **Appliance Settings** > **Ethernet Interface Settings**. The ports that are administratively down are indicated in red color.

Note

This setting is currently available in read-only mode on the Citrix SD-WAN Orchestrator service UI. If you want to modify the Ethernet Interface settings, you can do so by using the new user interface for SD-WAN appliances.

Ethernet Interface Settings

Interface	State	MAC Address	Autonegotiate	Speed	Duplex
0/1	•		\checkmark	1000Mb/s	✓ Full ✓
1/1	•			1000Mb/s	✓ Full ✓
1/2	•		\checkmark	1000Mb/s	✓ Full ✓
1/3	•			1000Mb/s	✓ Full ✓
1/4	•		\checkmark	1000Mb/s	✓ Full ✓
1/5	•		\checkmark		V Unknown V
/6	•				V Unknown V
1/7	•		\checkmark	1000Mb/s	✓ Full ✓
/8	•		\checkmark	1000Mb/s	✓ Full ✓
_AG0	•	Device not			

In-band management

February 1, 2022

Citrix SD-WAN Orchestrator service allows you to manage the SD-WAN appliance in two ways, outof-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. Inband 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 Citrix SD-WAN Orchestrator service 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.

Verify C	config 01 Site	Details	2 Device Details 03 Interfaces	04 WAN Links	5 Routes 06 Summary
+ Interface	+ HA I	nterface 🚿	1		
n-band Managemen None	t IP In-band Mar	nagement IPv6	In-band Management DNS In-band V6	and Management DNS None 🗸	
Interface Name	Port(s)	VLAN ID	IP Address	Actions	
1.0001			172 H. M. 1074, MR14, 1044	Ē	
			172-18-31-10-DA, MPROM-10-BA	Ē	
MARKING C					
MARCE 2			172-18-32 10-24, MRIN: 10-84	Ē	
400.1 400.2	1		172 8.32 1034, MRM, 1044 172 8.32 1034, MRM, 1044	till the second	

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 proxy, see DNS proxy.

For use cases where the appliance connectivity to Citrix SD-WAN Orchestrator service toggles between management and in-band ports, configure **InBand Management DNS** or **InBand Management DNS V6** to ensure uninterrupted Citrix SD-WAN Orchestrator service 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 Citrix SD-WAN Orchestrator service, 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.

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.

The fallback configuration retains the connectivity to appliance through the appliance in-band management IP and Citrix SD-WAN Orchestrator service in the following scenarios:

- Where the t2_app crashes
- you attempt to perform the configuration reset

In a scenario, where an appliance has in-band management configured and you perform manual configuration reset or the t2_app crashes more than four times in 120 seconds due to user configuration. In such framework, the service gets disabled and hence you lose connectivity to Citrix SD-WAN Orchestrator service and the appliance.

But if you had fallback configuration enabled, then you get below features:

- Basic in-band access to management features (Web UI/SSH/SNMP)
- Ability for appliance connects to outside services over an in-band port (Citrix SD-WAN Orchestrator service/ZTD)

For such scenarios, instead of disabling the service appliance comes back with fallback configuration with service enabled. The connectivity to Citrix SD-WAN Orchestrator service and the appliance through the in-band management IP remains intact as long as the link has internet connectivity.

Note

After the initial appliance provisioning, ensure that the fallback configuration is enabled for zerotouch 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.

C DASHBOARD	Administrator Interface NetFlow Host Settings Network Adapters	AppFlow Host Settings SNMP Fallback DateTime Syslog Flows Mobile Broadband Status	
REPORTS >			
	'Day 0' Default / 'Day N' Fallback Config		
CONFIGURATION ~	The fallback configuration provides basic network functionality when a critical failure occur	rs and the system can no longer function.	
Site Configuration Advanced Settings	Enable Fallback Configuration	Reset	
Appliance Settings	LAN Settings		
WAN-OP Settings	VLAN ID IP Address		
	0 192.168.101.1/24		
S TROUBLESHOOTING >	Enable DHCP Server		
	DHCP Start DHCP End		
	192.168.101.50 192.168.101.250		
	Jynamic DNS Servers		
	DNS Server Alt DNS Server		
	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.

ay O' Default / 'Day N' Fallback Cor	nfig	
ne fallback configuration provides basic network	functionality when a critical failure occurs and the system can	n no longer function.
Enable Fallback Configuration		Re
LAN Settings		
VLAN ID	IP Address	
0	192.168.101.1/24	
Enable DHCP Server		
DHCP Start	DHCP End	
192.168.101.50	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	⊖ WAN	• LAN	O Disabled				
2	• WAN	\bigcirc LAN	O Disabled				
3	\bigcirc wan	\bigcirc LAN	• Disabled				
4	\bigcirc wan	\bigcirc LAN	• Disabled				
5	⊖ WAN	\bigcirc LAN	• Disabled				
6	⊖ WAN	\bigcirc LAN	• Disabled				
7	⊖ WAN	\bigcirc LAN	• Disabled				
8	⊖ WAN	\bigcirc LAN	• Disabled				
MGT	⊖ WAN	\bigcirc LAN	 Disabled 				
Unassigned Port Bypass Mode							
Fail to Block	\sim						

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**, 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	DHCP		0	9,9.9.9

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

Citrix SD-WAN Orchestrator service 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 Citrix SD-WAN Orchestrator service immediately.

Once the connection is established, a service agent running on the appliance sends the heartbeat information to the Citrix SD-WAN Orchestrator service every 10 seconds. If the Citrix SD-WAN Orchestrator service does not receive the heartbeat for 5 minutes, the In-band port failover is activated. Citrix SD-WAN Orchestrator service 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 Citrix SD-WAN Orchestrator service is maintained even if the virtual path is down.

Verify Config	Service & Bandwidth			
Internet Service				
Service Name	Cost 5			
Advance Settings				
✓ Preserve route to In	ternet from link even if all ass	sociated paths are down	1	
Cancel	Save			

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.

Verify Config	of Site Details	02 Device Details	03 Interfaces	04 WAN Links	05 Routes	06 Summary
Interface Attributes						
Deployment Mode*	Interface Type *	Security*	Inte	rface Name LAN-1		
Physical Interface						
Select Interface * LAG1 1/1 LTE-E1	MGMT		Lin	< Aggregation Group	2	
Virtual Interfaces						
VLAN ID*	Virtual I	nterface Name *				

To reconfigure the management port to perform management functionality, remove the configuration. Create a configuration without using the management port and activate it.

View configuration (Preview)

June 14, 2022

The **View configuration** page provides a consolidated summary of a site's configuration settings. To view the configurations, at the site level, navigate to **Configuration** > **View Configuration**. For more information about site configuration, see Site configuration.

Sites

The **Sites** page displays a summary of the site details. The site summary includes network properties, site properties, and WAN link status. To view the site configuration details, navigate to **Configuration** > **View Configuration** > **Site**.

View Configuration (Preview) (i)

Site Interfaces WAN Links Routes Application Routes Dynamic Routing

Network Properties

Encryption Mode is: aes128 Encryption Rekey is: Enabled

Site Properties

WAN to WAN forwarding is: Enabled Device Model: cbvpx Sub-Modal: BASE Device Edition: SE Site Role: client Bandwidth Tier (Mbps): 20 Gateway ARP Timer (ms): 1000 Primary Device Serial Number: Max dynamic virtual paths configured is: 4

WAN Links

Broadband-ACT-1

Interfaces

The **Interfaces** page displays a summary of the configured interfaces. To view the configuration details of the virtual interfaces, navigate to **Configuration** > **View Configuration** > **Interfaces**.

In-band Management Settings LAN-1		
Interface Attributes Deployment Mode: fail.to.block Security: touted Ethernet Interfaces: 1 Bridge Pairs: NIA	Virtual Interfaces VIF-2-LAN-1 Routing Domain: Default, RoutingDomain Firewall Zone: Default, LAN, Zone IP Addresses:	
WAN-1		
Interface Attributes Deployment Mode: fail_to_block Security: untersted Ethernet Interfaces: 3 Bridge Pairs: NUK	Virtual Interfaces VIF-WAN-3-VLAN-0 Routing Domain: Default_RoutingDomain Firewall Zone: Default_LAN_Zone IP Addresses:	
WAN-2		
nterface Attributes Deployment Mode: Fall_to_block Security: trusted Ethernet Interfaces: 2 Bridge Pairs: N/A	Virtual Interfaces VIF-1-WAN-2 Routing Domain: Default_RoutingDomain Freewall Zone: Default_LAN_Zone IP Addresses:	

WAN links

To view the configuration details of the configured WAN links, navigate to **Configuration** > **View Con-figuration** > **WAN Links**.



Routes

To view the route information of the IP routes created, navigate to **Configuration > View Configura**tion > Routes.

Site Interfaces	Site Interfaces WilN Links Routes Application Routes								
Routes for routing	domain Default_RoutingDomain :								
Network Addr	D Getreny P Addr D	Service Type 0	Service Name 0	Cest 1	Expert Route 0	Summary Roote 0	Eligibility Based or Generary	Eligibility Besed on Turnel	
		Internet		4					
	10112	Local		5	Disabled	Disabled	Enabled		
		IPHost		5					
				5					
		(PHost		5					
				5					
		IPHost		5					
				5					
		Passthrough		65535					
		Discard		65535					
		Passthrough		65535					
		Discard		65535	-				

Application routes

To view a summary about the specific application routes, navigate to Configuration > View Configuration > Application Routes.

View Configuration (
Site	Interfaces	WAN Links	Routes	Application Rout	bes Dynamic Rot	uting						
Rou	Routes for routing domain RD1 :											
Ap	plication Object		Service Type		Service Name		Cost		Eligibility Based on Gateway		Eligibility Based on Tunnel	
cu	tom_app_test		Internet Break	out	-		8		-		-	
De	fault_SIA_Conn	ector_App	Internet Break	out	-		20		-		-	
Inc	omplete virtual	protocol	Internet Break	out	-		21		-		-	
Dis	stributed Compu	ting Envir	Zscaler		zscalerService		21		-		Enabled	
Ad	vance Message	Queuing P	IPSec Tunnel		ipsec2		21		-		Enabled	
Ne	tware Core Prot	ocol	Cloud Direct Service		-		45		-		-	
Ma	lformed virtual (protocol	Secure Intern	et Access Servi	citrixSIAService		45		-		Enabled	
cu	stom1_IP		Secure Intern	et Access Servi	citrixSIAService		45		-		Enabled	
03	650ptimize_Inte	ernetBrea	Internet Break	out	-		50		-		-	
Cit	rix_Cloud_and_	Gateway	Internet Break	out	-		50		-		-	
Rou	Routes for routing domain RD2 :											
Ap	plication Object		Service Type		Service Name		Cost		Eligibility Based on Gateway		Eligibility Based on Tunnel	
ар	p23		IPSec Tunnel		ipsec1		3		-		Enabled	

Dynamic routing

To view a summary of the OSPF, BGP, import filter, and export filter configurations, navigate to Configuration > View Configuration > Dynamic Routing.

Site	Interface	s WAN Link	s Routes	Application Rou	ites Dynami	c Routing					
OSP	F Enabled										
Expo	Export OSPF Route Type: type 5 as external										
Adve	Advertise Citrix SD-WAN Routes: Enabled										
SDW	AN Routes	Tag Value: 22									
Adve	ertise BGP I	Routes: Enable	d								
BGP	Routes Tag	g Value: 34									
Prote	ocol Prefer	ence: 150									
Rout	er ID Settir	ngs:									
Rou	ting Do 🌻	Area ID 🌲	Is Stub Area 🇘	Virtual Inte 🗘	Source IP 🌲	Authentica 🗘	Cost 🌲	Network Ty	Hello Interv‡	Dead Interv\$	Dead Interval 🗘
Def	fault_Ro	23	Disabled	VIF-1-Bridg		None	10	Auto	10	40	40
BGD	Enabled										
Loca	I Autonomi	ous System: 1									
Advertise Citrix SD-WAN Routes: Fnabled											
Advertise OSPF Routes: Enabled											
Prote	Protocol Preference: 100										
Rout	er ID Settir	ngs:									

Office 365 optimization

April 14, 2023

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 Office 365 traffic directly to the Internet from branch environments. Avoid practices such as backhauling to a central proxy. 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.

The Office 365 traffic is directed to the nearest Office 365 service endpoint, which exists at the edges of Microsoft Office 365 infrastructure worldwide. Once traffic reaches a front door, it goes over Microsoft network and reaches the actual destination. It minimizes latency as the round trip time from the customer network to the Office 365 endpoint reduces.

How Office 365 optimization works

The Microsoft endpoint signatures are updated at most once a day. Agent on the appliance polls the Citrix service (sdwan-app-routing.citrixnetworkapi.net), every day to obtain the latest set of end-point

signatures. The SD-WAN appliance polls the Citrix service (sdwan-app-routing.citrixnetworkapi.net), once every day, when the appliance is turned on.

If there are new signatures available, the appliance downloads it and stores it in the database. The signatures are essentially a list of URLs and IPs used to detect Office 365 traffic based on which traffic steering policies can be configured.

Note

Except for the Office 365 Default category, first packet detection and classification of Office 365 traffic is performed by default, irrespective of whether the Office 365 breakout feature is enabled or not.

When a request for the Office 365 application arrives, the application classifier, does a first packet classifier database lookup, identifies, and marks Office 365 traffic. Once the Office 365 traffic is classified, the auto created application route and firewall policies take effect and breaks out the traffic directly to the Internet. The Office 365 DNS requests are forwarded to specific DNS services like Quad9.



The signatures are downloaded from Cloud Service (sdwan-app-routing.citrixnetworkapi.net).

Configure Office 365 breakout

The Office 365 breakout policy allows you to specify which category of Office 365 traffic you can directly break out from the branch. On enabling Office 365 breakout and compiling the configuration, a DNS object, application object, application route, and a firewall policy template is auto-created and applied to branch sites with the Internet service.

Prerequisites

Ensure that you have the following:

- 1. To perform Office 365 breakout, an internet service has to be configured on the appliance.
- 2. Ensure that the Management interface has internet connectivity.
- 3. Ensure that the management DNS is configured.

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

DASHBOARD	C DASHBOARD									
REPORTS	>	Cost Rar	vst Ranges: Custom Application (1-20) Application (21-40) Application Group (41-60) IP (1-65535)							
© CONFIGURATION	~	+ A	+ Application Route			Search for Route Q				
		No	Match Type	Name	Delivery Service	Routing Domain	Sites		Cost	Actions
Network Config Ho	ne	1	Application Group	Default Cloud Dir	Cloud Direct Service	Any	Global		45	Ē
Delivery Services	>	2	Application Group	03650ptimize_In	Internet Breakout	Any	Global		50	Ē
Routing	~	3	Application Group	Citrix_Cloud_and	Internet Breakout	Any	Global		50	
Routing Policies										
Routing Domain	s									
Import Route Pr	ofiles									
Export Route Pr	ofiles									
Transit Nodes										
Link Settings	>									
QoS	>									
Security	>									
Site & IP Groups	>									
App & DNS Setting	3 >									
Profiles & Template	s									
ECMP Groups										
WAN Optimization	>									

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

	Verify Coarling Application Routes IP Routes						
	Cost Ranges: Outrom Application (1-20) Application (21-40) Application Group (41-60) IP (1-65535)						
 ⊘ CONFIGURATION ∨ 	Application Group Match Criteria						
Network Config Home	Match Type Application Group *						
Delivery Services >	Application Group V 03650ptimize_InternetReakout V						
Routing 🗸							
Routing Policies	Scope						
Routing Domains	Global Route Stet / Group Specific Route						
Import Route Profiles							
Export Route Profiles	naur aneant						
Transit Nodes	Delivery Service						
Link Settings >	Internet Breakout						
QoS >	0385 Network Optimization Settings						
Security >							
Site & IP Groups >	Review Office 385 Network Connectivity Principles						
App & DNS Settings >	Task transfer Admittaskan in data ministrati under ander an						
Profiles & Templates	🧭 Teams Realtime 🖉 Exchange Online 🧭 SharePoint Optimize						
WAN Ontimization	Allow (Enable optimization for less latency sensitive 0365 services eg: https://protection.outloak.com; https://protection.com; https:						
	✓ Teams TCP Failback. ☑ Exchance Mail. ☑ SharePoint Allow ☑ 0365 Common						
() ALERTS >	2 Out-th. At antimizing sequence for (2015) and set is the extension as there (include difference (include difference)).						
-							
😢 TRUIBLESHOTING > Wannie Celevania en see V 🗠 Elabara Uodo Installighter Fall Steekkunt							
-							
<	Cancel Save						

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 networksensitive 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:

- Microsoft 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
- 0365 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.
- 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.

Transparent forwarder for Office 365

The branch breaks out for Office 365 begins with a DNS request. The DNS request going through Office 365 domains have to be steered locally. If Office 365 Internet break out is enabled, the internal DNS routes are determined and the transparent forwarders list is auto populated. Office 365 DNS requests are forwarded to open source DNS service Quad 9 by default. Quad 9 DNS service is secure, scalable, and has multi pop presence. You can change the DNS service if necessary.

Transparent forwarders for Office 365 applications are created at every branch that has Internet service and office 365 breakout enabled.

If you are using another DNS proxy or if SD-WAN is configured as the DNS proxy, the forwarder list is auto populated with forwarders for Office 365 applications.

Important considerations for upgrade

Optimize and Allow categories

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, the upgrade becomes unsuccessful. 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:

Verification Results	×
Status: Validation Failed	
Parsing Region:Default_Region * -> ERROR: EC14000: Application QoE references either an unknown or disabled Application (O3650ptimize_InternetBreakout)	
This Configuration is invalid. Please fix the above errors and recompile the configuration.	
Files created: versions.lst basic_2_site_config_package1.xml	
Ok	

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 becomes successful too. However, the DNS proxy rules and transparent forwarding rules do not take effect in Citrix SD-WAN 11.4.0.

Note

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

Limitations

- If the Office 365 breakout policy is configured, deep packet inspection is not performed on connections destined to the configured category of IP addresses.
- The auto created firewall policy and application routes are uneditable.
- The auto created firewall policy has the lowest priority and is uneditable.
- The route cost for the auto created application route is five. You can override it with a lower cost route.

Office 365 beacon service

Microsoft provides the Office 365 beacon service to measure the Office 365 reachability through the WAN links. The beacon service is basically a URL - sdwan.measure.office.com/apc/trans.png, which is probed at regular intervals. Probing is done on each appliance for every internet enabled WAN link. With each probe, an HTTP request is sent to the beacon service and an HTTP response is expected. The HTTP response confirms the availability and reachability of the Office 365 service.

Citrix SD-WAN allows you to not only perform beacon probing, but also determines the latency to reach Office 365 endpoints through each WAN link. The latency is the round trip time taken to send a request and get a response from the Office 365 beacon service over a WAN link. This enables network administrators to view the beacon service latency report and manually choose the best internet link for direct Office 365 breakout. Beacon probing is enabled only through Citrix SD-WAN Orchestrator. By default, beacon probing is enabled on all Internet enabled WAN links when Office 365 break-out is enabled through Citrix SD-WAN Orchestrator.

Note

Office 365 beacon probing is not enabled on metered links.

To disable Office 365 beacon service, in SD-WAN Orchestrator, at network level navigate to **Configura**tion > Routing > Routing Policies > O365 Network Optimization Settings and clear Enable Beacon Service.

Dashboard	Vuriy Centre Application Routes IP Routes								
REPORTS >	Cost Ranges: Custom Application (2-40) Application Group (41-60) IP (1-8533)								
\odot configuration \sim	Application Group Match Criteria								
Network Config Home Delivery Services >	Match Type Application Group* Application Group 03850ptinize_InternetBreakout								
Routing ~	Sсеря								
Routing Policies Routing Domains	Global Route Site / Group-Specific Route								
Import Route Profiles	Traffic Steering								
Export Route Profiles	Deline Senie								
Transit Nodes	Internet Breakout								
QoS >	0385 Network Optimization Settings								
Security > Site & IP Groups > App & DNS Settings > Profiles & Templates WAN Optimization >	Review Office 365 Network Connectivity Principles Network Connectivity in the Microsoft 365 Admin Center Optimize Enable estimization for highly intercy seculity 0355 services og Exchange Sharepoint, Skype for Business, Teams etcl I Teams Realitime 🖉 Exchange Online 🖉 SharePoint Optimize								
① ALERTS >	Allow (Enable antihization for free latency senalitie Q355 services eg: https://protection.autiods.com/. https://ecountlaccess.com/inidews.ser/) Teams TCP Fallback 😥 Exchange Mail 🖉 SharePoint Allow 💟 0385 Common								
\sim troubleshooting >	Conception Concepting Concepting Concepting Concepting Concepting Concepting Concep								
$\underline{\Omega}$ administration >	Cancel Save								
<									

To view the beacon probing availability and latency reports, in Citrix SD-WAN Orchestrator, at network level navigate to **Reports** > **O365 Metrics**.

								Change Role	\$ 0
DASHBOARD	Î	Network Reports: 0365	Metrics C			Relative T	me 🗸 Interval: Last 30 Mins 🛇	/ Site Group: All	~
REPORTS	~	Site Name	WAN Link Name	Availability	Latency (ms)	Lowest Latency (ms)	WAN Link Selected	Total Decisions Taken	
	- 1	BR1100_HF	BR1100_HF-Broadband-Airtel-1	No	21.14	16.17	0	0	
Alerts		MCN_HF	MCN_HF-Broadband-Airtel-1	Yes	423.77	416.23	0	0	
Usage		MCN_HF	MCN_HF-Broadband-Airtel-2	No	421.21	416.60	1	1	
Wi-Fi									
Inventory									
Security	>								
Secure Internet Ser	vice								
HDX	>								
Quality									
OoS									
Historical Statistics									
Real Time									
Claud Direct									
Application Quality									
Application Quality	-								
U305 Metrics									
CAS Analytics									
Top Talkers									

To view a detailed site level report of beacon service, in SD-WAN Orchestrator, at site level navigate to **Reports > 0365 Metrics**.

C DASHBOARD	Site Reports: 0365	5 Metrics 📿						Relati	re Time 🧹 Interval: 🗌 La	st 30 Mins 🗸
REPORTS V	Select WAN Link : M	CN_HF-Broadband-Airtel-1 🗸								
Alerts	12:12pm	12:15pm	12:19pm	12:22pm	12:25pm	12:29pm	12:32pm	12:35pm	12:39pm	12:42pm
Usage										
Quality										
QoS										
Historical Statistics										
Real Time >	Latency (ms) :									
Cloud Direct	515									
0365 Metrics	300				Time : 12	2:26pm				
Appliance Reports	150				Value : 4	H9 ms				
WAN Link Metering	0									
	Lowest Latency (ms)									
O CONFIGURATION >	461									
	300									
	150									
S INCODEESHOUTING >	0_									

Metering and Standby WAN Links

November 10, 2021

Citrix SD-WAN Orchestrator service supports enabling metered links, which can be configured such that user traffic is only transmitted on a specific Internet WAN Link when all other available WAN Links are disabled.

Metered links conserve bandwidth on links that are billed based on usage. With the metered links you can configure the links as the Last Resort link, which disallows the usage of the link until all other nonmetered links are down or degraded. Last Resort is typically enabled when there are three WAN Links to a site (that is, MPLS, Broadband Internet, 4G/LTE) and one of the WAN links is 4G/LTE and might be too costly for a business to allow usage unless it is necessary. Metering is not enabled by default and can be enabled on a WAN link of any access type (Public Internet / Private MPLS / Private Intranet). If metering is enabled, you can optionally configure the following:

- Data Cap
- Billing Cycle (weekly/monthly)
- Start Date
- Standby Mode
- Priority
- Active heartbeat interval Interval at which a heartbeat message is sent by an appliance to its peer on the other end of the virtual path when there has been no traffic (user/control) on the path for at least a heartbeat interval

A metered path can be formed with 1 or 2 metered links. If a path is formed between two metered links, the active heartbeat interval used on the metered path is the larger of the two configured active heartbeat intervals on the links.

A metered path is a non-standby path and is always eligible for user traffic. When there is at least one non-metered path that is in GOOD state, a metered path carries the reduced amount of control traffic

and is avoided when the forwarding plane searches for a path for a duplicate packet.

When a metered link is enabled, you can view the WAN link metering information under **Reports > WAN Link Metering**.

Prerequisites to configure metering and standby WAN links

- A metered link might be of any access type.
- All links at a site can be configured with metering enabled.
- A standby link might be of Public Internet or Private Intranet access type. A WAN link of Private MPLS access type cannot be configured as a standby link.
- At least one non-standby link must be configured per site. A maximum of 3 standby links per site is supported.
- Internet/Intranet services might not be configured on on-demand standby links. On-demand standby links support Virtual Path service only.
- Internet service might be configured on a last-resort standby link, but only load balance mode is supported.
- Intranet service might be configured on a last-resort standby link, but only secondary mode is supported and primary reclaim must be enabled.

Configure metering

To configure a metered link, at the site level configuration, navigate to **Configuration > Site Configuration > WAN Links** tab. In the **Advanced WAN Options** section, select the **Enable Metering** check box and enter the details in the following fields:

- 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.

If the **Disable Link if Data Cap Reached** check box is selected, then the metered link and all its related paths will be disabled until the next billing cycle, if the data usage reaches the data cap.

By default, the **Disable Link if Data Cap Reached** check box will be cleared, where it retains the current mode or state set for the metered link to be continued after the data cap is reached until the next billing cycle.

If the metered link is configured, you can provide the approximate data already used in MB for the metered link.

To track the proper metered link usage, you must enter the approximate usage on the metered link if the link has already been used for some days in the current billing cycle. This approximate usage is only for the first cycle. Total usage since the start date to the current date is calculated and shown in the dashboard.

If the metered link is configured, you can provide the approximate data already used in MB for the metered link.

To track the proper metered link usage, you must enter the approximate usage on the metered link if the link has already been used for some days in the current billing cycle. This approximate usage is only for the first cycle. Total usage since the start date to the current date is calculated and shown in the dashboard.

Advanced WAN Options		•
✓ Enable Metering Adap	otive Bandwidth Detection	
Congestion Threshold (µs)	Provider ID	Frame Cost (Bytes)
20000		1
Standby Mode	MTU (Bytes)	
Disabled \lor	1350	
Data Cap(MB)	Billing Cycle	Starting From
	monthly ~	MM/DD/YYYY
	Approximate Data Already Used (MB)	
Disable Link if Data Cap Reached	0	

Standby mode

A standby WAN link is not used to carry user traffic unless it becomes active. The standby mode of a WAN link is disabled by default. To enable standby mode, you must specify in which one of the following two modes the standby link operates • **On-demand**: The standby link that becomes active when one of the conditions is met.

When the available bandwidth in the virtual path is less than the configured on-demand bandwidth limit AND there is sufficient usage. Sufficient usage is defined as more than 95% (ON_DEMAND_USAGE_THRESHOLD_PCT) of the current available bandwidth, or the difference between current available bandwidth and current usage is less than 250 kbps (ON_DEMAND_THRESHOLD_GAP_KBPS) both parameters can be changed using t2_variables when all the non-standby paths are dead or disabled.

• **Last-resort**: A standby link that becomes active only when all non-standby links and ondemand standby links are dead or disabled.

Standby priority indicates the order in which a standby link becomes active, if there are multiple standby links:

- A priority 1 standby link becomes active first whereas a priority 3 standby link becomes active last.
- Multiple standby links can be assigned the same priority.

When configuring a standby link, you can specify standby priority and two heartbeat intervals:

- Active heartbeat interval the heartbeat interval used when the standby path is active (default 50ms/1s/2s/3s/4s/5s/6s/7s/8s/9s/10s)
- **Standby heartbeat interval** the heartbeat interval used when the standby path is inactive (default 1s/2s/3s/4s/5s/6s/7s/8s/9s/10s/disabled)

A standby path is formed with 1 or 2 standby links.

- **On-Demand** An on-demand standby path is formed between:
 - a non-standby link and an on-demand standby link
 - 2 on-demand standby links
- Last-Resort A last-resort standby path is formed between:
 - a non-standby link and a last-resort standby link
 - an on-demand standby link and a last-resort standby link
 - 2 last-resort standby links

The heartbeat intervals used on a standby path are determined as follows:

- If standby heartbeat is disabled on at least 1 of the 2 links, heartbeat is disabled on the standby path while inactive.
- If standby heartbeat is not disabled on either link, then the larger of the two values are used when the standby path is standby.

• If active heartbeat interval is configured on both links, then the larger of the two values are used when the standby path is active.

Heartbeat (keep alive) messages:

- On a non-standby path, heartbeat messages are sent only when there has been no traffic (control or user) for at least a heartbeat interval. The heartbeat interval varies depending on the path state. For non-standby, non-metered paths:
 - 50 ms when the path state is GOOD
 - 25 ms when the path state is BAD

On a standby path, the heartbeat interval used depends on the activity state and the path state:

- While inactive, if the heartbeat is not disabled, heartbeat messages are sent regularly at the configured standby heartbeat interval since no other traffic is allowed on it.
- The configured active heartbeat interval is used when the path state is GOOD.
- 1/2 the configured active heartbeat interval is used when the path state is BAD.
- While active, like non-standby paths, heartbeat messages are sent only when there has been no traffic (control or user) for at least the configured active heartbeat interval.
- The configured standby heartbeat interval is used when the path state is GOOD.
- 1/2 the configured standby heartbeat interval is used when the path state is BAD.

While inactive, standby paths are not eligible for user traffic. The only control protocol messages sent on inactive standby paths are heartbeat messages, which are for connectivity failure detection and quality metrics gathering. When standby paths are active, they are eligible for user traffic with added time cost. This is done so that the non-standby paths, if available, are favored during forwarding path selection.

The path state of a standby path with disabled heartbeat, while inactive, is assumed to be GOOD and it is displayed as GOOD in the Path Statistics table under **Reports > WAN Link Metering**. When it becomes active, unlike a non-standby path that starts in DEAD state until it hears from its Virtual Path peer, it starts in GOOD state. If connectivity with the Virtual Path peer is not detected, the path goes BAD and then DEAD. If connectivity with the Virtual Path peer is re-established, the path goes BAD and then GOOD again.

If such standby path goes DEAD and then becomes inactive, the path state does not immediately change to (assumed) GOOD. Instead, it is kept in DEAD state for time so that it cannot be used immediately. This is to prevent activity from oscillating between a lower priority path group with assumed good DEAD paths and a higher priority path group with actually GOOD paths. This on-hold period (NO_HB_PATH_ON_HOLD_PERIOD_MS) is set to 5 min and can be changed via t2_variables.

If path MTU discovery is enabled on a Virtual Path, the standby path's MTU is not used to calculate the Virtual Path's MTU while the path is standby. When the standby path becomes active, the Virtual Path'
s MTU is recalculated considering the standby path's MTU. (The Virtual Path's MTU is the smallest path MTU among all active paths within the Virtual Path).

Events and log messages are generated when a standby path transitions between standby and active.

Configure standby WAN links

To configure a standby WAN link, at the site level configuration, navigate to **Configuration > Site Configuration > WAN Links** tab. In the **Advanced WAN Options** section, choose a standby mode from the **Standby Mode** drop-down list.

Advanced WAN Options					
Enable Metering	Ad	aptive Bandwidth Detection			
Congestion Threshold (µs)		Provider ID		Frame Cost (Bytes)	
20000				1	
Standby Mode		MTU (Bytes)			
On-Demand	\sim	1350			
Priority		Active Heartbeat Interval (s)		Standby Heartbeat Interval (s)	
1	\sim	Default	\checkmark	1	\checkmark

If an on-demand standby link is configured, the global default on-demand bandwidth limit (120%) is applied to the Virtual Path. This specifies the maximum WAN-to-LAN bandwidth allowed for the Virtual Path. It is expressed as a percentage of the total bandwidth provided by all non-standby links in the Virtual Path. As long as the available bandwidth in the Virtual Path is below the limit and if there is sufficient usage, the appliance attempts to activate on-demand paths to supplement bandwidth.

If you want to apply an on-demand bandwidth limit specific to a Virtual Path and keep the global default setting unchanged, a Virtual Path Default Set must be created and the on-demand bandwidth limit can be changed.

To apply settings for a specific Virtual Path, navigate to **Configuration > Basic Settings > Interfaces** tab.

Zero touch deployment

December 16, 2020

Zero touch deployment allows SD-WAN appliances to be provisioned and configured automatically, eliminating the manual labor involved in setting up your SD-WAN network.

Appliances/devices need access to the following domain names for Zero touch deployment to work:

- sdwanzt.citrixnetworkapi.net
- download.citrixnetworkapi.net
- trust.citrixnetworkapi.net

Zero touch deployment workflow

- Create and define sites using the guided workflow. For more information, see Site configuration.
- Verify and compile the configuration using the deployment tracker. For more information, see the Deployment Tracker section in Network configuration topic.
- Power on and cable up the SD-WAN appliances at the Data Center and branch sites.
- Appliances contact the Citrix SD-WAN Orchestrator service with their serial number.
- Citrix SD-WAN Orchestrator service receives requests for configuration and pushes the relevant files to the appliances.
- The virtual paths are established and the SD-WAN network is now up and running.



IP rules

March 3, 2022

IP Rules help you to create rules for your network and take certain Quality of Service (QoS) decisions based on the rules. You can create custom rules for your network. For example, you can create a rule as –If source IP address is 172.186.30.74 and destination IP address is 172.186.10.89, set **Traffic Policy** as **Persistent Path** and **Traffic Type** as **Realtime**.

You can create rules for traffic flow and associate the rules with applications and classes. You can specify criteria to filter traffic for a flow, and can apply general behavior, LAN to WAN behavior, WAN to LAN behavior, and packet inspection rules.

You can create global and site-specific IP rules at the network level. If a site is associated with the globally created rule, you can create site specific rules. In such cases, site specific rules take precedence and override the globally created rule.

The default IP protocol rules HTTP, HTTPS, and ALTHTTPS always appear at the top of the list on the Rules table. However, site-specific IP rules (once created) appear above HTTP, HTTPS, ALTHTTPS, and global IP rules on the Rules table.

Create IP rules

To create IP rules, navigate to **Configuration > QoS > QoS Policies > IP Rules**. Select the **Global Rules** tab for creating IP rules at the global level or **Site/Group Specific Rules** for creating rules at a site level.

Click New IP Rule under the IP Rules section.

🕤 Edit IP Protocol (Gla	obal Rules)			
IP Protocol Match Criteria				
Louise Network	C De P Drug	Destination Nationals	Cor P Strap	
Aty		Any		Sec + Deal
Source Port		Destination Part		
Any		kış		Sire = Deut
Protocol		010*		
Any	v	Any	v	Retird Flow On DBCR Ownge
Ruting Suman		where all		
Any	v			
Virtual Path Traffic Policy				
virtual Part Mercure She			tuto tuto	
yeld there used all unreally		Ŷ	Last beance rates	
QoS Settings				
hander fase*		Provide 1		
Interactive	~	Medium	¥	
Note: Bandwidth share available par QoS ch Intelligent default values are auto-picked, w	less per overlay virtual path is data ith ability to override the defaults	rmined by <u>Ood Profiles</u> vie oustom Ood profiles		
Internet Traffic Policy				
Enable Internet Policy				
O. Advanced Settings				
Cancel Save				

• 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.
- **Protocol**: The protocol with which the rule matches. You can select one of the predefined protocols, or select **Any**, or **Number**.
- Protocol Number: This field appears only when you select Number from the Protocol drop-down list. When you select a protocol number, the integer associated with the protocol is used for the back-end configurations.
- **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 DSCP Change**: When selected, flows that are otherwise identical in terms of match criteria are treated as separate if their DSCP fields differ.
- Virtual Path Traffic Policy

Select the Enable Virtual Path Traffic Policy check box.

- 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 Path**: Application traffic remains on the same path until the path is no longer available. Select one of the following **Persistence Policies**:
 - **Persist on the originating link**: The application traffic remains on the originating link until the path is no longer available.
 - **Persist on MPLS link if available, else on the originating link**: The application traffic remains on the MPLS link. If the MPLS link is unavailable, then the traffic remains on the originating link.
 - **Persist on Internet link if available, else on the originating link**: The application traffic remains on the internet link. If the internet link is unavailable, then the

traffic remains on the originating link.

• **Persist on Private Intranet link if available, else on the originating link**: The application traffic remains on the private intranet link. If the private intranet link is unavailable, then the traffic remains on the originating link.

Persistence Impedance is the time (in ms) until which the application traffic remains on the link.

- * **Duplicate Paths**: Application traffic is duplicated across multiple paths, increasing reliability.
- **Override Service**: Traffic for the flow overrides to a different service. Select the service type as Intranet, Internet, pass-through, or Discard to which the virtual path service overrides.

Virtual Path Traffic Policy				
Enable Virtual Path Traffic Policy Virtual Path Remote Site		Traffic Policy	Override Service	
Any (determined by routing)	~	Override Service	<n a=""></n>	~
QoS Settings			<n a=""></n>	
Qeff Class Travite Taxe*	Party"		Passthrough Discard	

- QoS Settings (QoS Class)
 - 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.

Note

A virtual path service cannot override another virtual path service.

QoS Policies (i)

Global Rules : IP Protocol	
IP Protocol Match Criteria	
Gource Network Use IP Grou	Destination Network Use IP Group
Any	Any Src = Dest
Source Port	Destination Port
Any	Any Src = Dest
rotocol	DSCP
Any	Any
louting Domain	Vlan Id
Any	· .
QoS Settings QoS Class	
Interactive	Priority"
Note: Bandwidth share available p Intelligent default values are auto-	rr QoS class per overlay virtual path is determined by <u>QoS Profiles</u> . picked, with ability to override the defaults via custom QoS profiles
Internet Traffic Policy	
Enable Internet Policy	
> Advanced Settings	
Cancel Save	
lvanced Settings	

Citrix SD-WAN Orchestrator

Advanced Settings					
WAN General					
Retransmit Lost Packets	Enable Packet Aggrega	ition			
TCP Termination	Header Comp	ression			
Enable TCP Termination	Enable GP	RE 🗌	Enable IP, TCP, UDP		
LAN To WAN					
General :					
Drop Depth (bytes)	Drop Limit (ms)		Large Packet Size Byted		
128000	50		0		Enable Red
Duplicate Packets Disable Depth Bytes)	Duplicate Packets Disable Limit Imsl		Large Packets Drop Depth Byte	d	Large Packets Drop Limit (ms)
128000	0		0		0
Reassign :					
Priority	Transfer Type		Large Packet Size (bytes)		Resulgt Size Byted
~		~	0		2000
Duplicate Packets Disable Depth Bytes)	Duplicate Packets Disable Limit Imsl		Large Packets Drop Depth Bytes		Large Packets Drop Limit (ms)
129000	0		0		0
Normal Packets Drop Depth Bytesl	Normal Packets Drop Limit Incl				
129000	50		Enable Red		
WAN to LAN					
Doop Tag	Hold	d Time (ms)			
Any Classic Proble Pr	cket Resequencing			Discard Late Resequence	e Packets
Done Cancel					

- WAN General
 - **Retransmit Lost Packets**: Sends traffic that matches this rule to the remote appliance over a reliable service and retransmits lost packets.
 - Enable Packet Aggregation: Aggregates small packets into larger packets.
 - **Enable TCP Termination**: Enables TCP termination of traffic for this flow. The round-trip time for acknowledgment of packets is reduced, and therefore improves throughput.
 - Enable GRE: Compresses headers in GRE packets.
 - Enable IP, TCP, and UDP: Compresses headers in IP, TCP, and UDP packets.

Note

IPv6 packets do not support header compression.

• LAN to WAN

General

- **Drop Depth(bytes)**: Queue depth threshold after which packets are dropped.
- **Drop Limit**: Time after which packets waiting in the class scheduler are dropped. Not applicable for a bulk class.
- Large Packet Size: Packets smaller than or equal to this size are assigned the Drop Limit and Drop Depth values specified in the Large Packets Drop Depth(bytes) and Large Packets Drop Limit(ms) fields. Packets larger than this size are assigned the values specified in the default Drop Limit and Drop Depth fields.
- **Enable RED**: Random Early Detection (RED) ensures fair sharing of class resources by discarding packets when congestion occurs.
- **Duplicate Packet Disable Depth(bytes)**: The queue depth of the class scheduler at which point the duplicate packets are not generated.
- **Duplicate Packet Disable Limit**: Time for which duplication can be disabled to prevent duplicate packets from consuming bandwidth.
- Large Packets Drop Depth(bytes): If the queue depth exceeds this threshold, the packets are discarded and statistics are counted.
- Large Packets Drop Limit(ms): The maximum amount of estimated time that packets larger than or equal to the Large Packet Size must wait in the class scheduler. If the estimated time exceeds this threshold, the packets are discarded and statistics are counted. Not valid for Bulk classes.

Reassign

- **Priority**: You can set the priority of the standby WAN link as needed. The standby WAN link priority indicates the order in which a standby WAN link becomes active. A high priority standby WAN link becomes active first. A low-priority WAN link becomes active last.
- **Transfer Type**: Select a transfer type with which to associate this rule.
- **Duplicate Packet Disable Depth(bytes)**: The queue depth of the class scheduler at which point duplicate packets are not generated.
- **Duplicate Packet Disable Limit**: Designates the amount of time a packet waits in the queue before duplication is not performed, which prevents duplicate packets from consuming bandwidth when bandwidth is limited.
- Large Packets Drop Depth(bytes): If the queue depth exceeds this threshold, the packets are discarded and statistics are counted.
- Large Packets Drop Limit(ms): If the estimated time exceeds this threshold, the packets are discarded and statistics are counted. Not valid for Bulk classes.
- Normal Packets Drop Depth (bytes): If the queue depth exceeds this threshold, the packets are discarded and statistics are counted.
- Normal Packets Drop Limit (ms): If the estimated time exceeds this threshold, the packets are discarded and statistics are counted. Not valid for Bulk classes.
- WAN to LAN

- **DSCP Tag**: DSCP tag applied to the packets that match this rule on WAN to LAN, before sending them to the LAN.
- **Enable Packets Resequencing**: The traffic flows that match the rule gets tagged for sequence order, and the packets gets reordered (if necessary) at the WAN to LAN appliance.
- **Hold Time**: Time interval for which the packets are held for resequencing, after which the packets are sent to the LAN. When the timer expires, the packets are sent to the LAN without waiting any further for the prerequisite sequence numbers.

If the rule has a traffic policy as duplicate path, the default hold time is 80 ms. Otherwise, the default is 900 ms for TCP rules and 250 ms for non-TCP rules.

- **Discard Late Resequencing Packets**: Discards out-of-order packets that arrived after the packets needed for resequencing have been sent to the LAN.

Click **Save** to save the configuration settings. Click **Verify Configuration** on the **Configuration** > **QoS Policies** page to validate any audit error.

		VerbyConfiguration Software Version: 11.3.2.25-GA
	©	
Global Rules	Site / Group Specific Rules	

Verify IP rules

To verify IP rules, navigate to **Reports > Real Time > Flows**. Select the site for which you want to view the flow information and the number of flows to display. Click **Customize Columns** and select the check boxes corresponding to the flow information you want to view. Verify if the flow information is according to the configured rules.

Navigate to **Reports > Real Time > Statistics** and select **Rules**. Choose the site and click **Retrieve latest data**. Verify the configured rules. For more information, see <u>Site reports</u>.

Application rules

January 26, 2022

Application rules allow the Citrix SD-WAN appliance to parse incoming traffic and classify them as belonging to a particular application or application group. This classification enhances the Quality of Service (QoS) of individual application or application families by creating and applying application rules.

You can filter traffic flows based on application, application group, or application object match-types and apply application rules to them. The application rules are similar to the Internet Protocol (IP) rules. For information on IP rules see, IP Rules.

For every application rule, you can specify the traffic policy. The following are the available traffic policies:

- Load Balance Path: 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 Path**: Application traffic remains on the same path until the path is no longer available.
- **Duplicate Path**: Application traffic is duplicated across multiple paths, increasing reliability. The application rules are associated to classes.

How application rules are applied?

In the SD-WAN network, when the incoming packets reach the SD-WAN appliance, the initial few packets do not undergo DPI classification. At this point, the IP rule attributes such as Class, TCP termination are applied to the packets. After DPI classification, the application rule attributes such as Class, traffic policy override the IP rule attributes.

The IP rules have more number of attributes as compared to the application rules. The application rule overrides only a few IP rule attributes. The rest of the IP rule attributes remain processed on the packets.

For example, consider you have specified an application rule for a webmail application such as Google Mail that uses the SMTP protocol. The IP rule set for the SMTP protocol is applied initially before DPI classification. After parsing the packets and classifying it as belonging to the Google Mail application, the application rule specified for the Google Mail application is applied.

Create application rules

To create application rules, navigate to **Configuration > QoS > QoS Policies > Application Rules**. Select **Global Rules** tab for creating application rules at the global level or **Site/Group Specific Rules** for creating rules at a site level.

Click New Application Rule under the Application Rules section.

- Apps and Domains Match Criteria
 - Apps & Domains: Choose an application or domain from the drop-down list. You can also create a domain app by clicking + New Domain App. Enter a name and add domains.

- **Routing Domain**: Select a routing domain. You can select the default routing domain or select **Any**.
- Source Network: Source IP address and the subnet mask to match against the traffic.
- Destination Network: Destination IP address and the subnet mask to match against the traffic.
- Source Port: Source port number or port range to match against the traffic.
- **Destination Port**: Destination port number or port range to match against the traffic.
- **Src = Dest**: If selected, the source port is also used for the destination port.
- Virtual Path Traffic Policy

Select the Enable Virtual Path Traffic Policy check box.

- 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 Path**: Application traffic remains on the same path until the path is no longer available. Select one of the following **Persistence Policies**:
 - **Persist on the originating link**: The application traffic remains on the originating link until the path is no longer available.
 - **Persist on MPLS link if available, else on the originating link**: The application traffic remains on the MPLS link. If the MPLS link is unavailable, then the traffic remains on the originating link.
 - **Persist on Internet link if available, else on the originating link**: The application traffic remains on the internet link. If the internet link is unavailable, then the traffic remains on the originating link.
 - **Persist on Private Intranet link if available, else on the originating link**: The application traffic remains on the private intranet link. If the private intranet link is unavailable, then the traffic remains on the originating link.

Persistence Impedance is the time (in ms) until which the application traffic remains on the link.

- * **Duplicate Paths**: Application traffic is duplicated across multiple paths, increasing reliability.
- QoS Settings (QoS Class)
 - 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.

Advanced Settings

- WAN General
 - **Retransmit Lost Packets**: Sends traffic that matches this rule to the remote appliance over a reliable service and retransmits lost packets.
 - Enable Packet Aggregation: Aggregates small packets into larger packets.
- LAN to WAN
 - **Drop Depth(bytes)**: Queue depth threshold after which packets are dropped.
 - **Drop Limit**: Time after which packets waiting in the class scheduler are dropped. Not applicable for a bulk class.
 - **Enable RED**: Random Early Detection (RED) ensures fair sharing of class resources by discarding packets when congestion occurs.
 - **Duplicate Packet Disable Depth(bytes)**: The queue depth of the class scheduler at which point the duplicate packets are not generated.
 - **Duplicate Packet Disable Limit**: Time for which duplication can be disabled to prevent duplicate packets from consuming bandwidth.
- WAN to LAN
 - **DSCP Tag**: DSCP tag applied to the packets that match this rule on WAN to LAN, before sending them to the LAN.
 - **Enable Packets Resequencing**: The traffic flows that match the rule gets tagged for sequence order, and the packets gets reordered (if necessary) at the WAN to LAN appliance.
 - Hold Time: Time interval for which the packets are held for resequencing, after which the packets are sent to the LAN. When the timer expires, the packets are sent to the LAN without waiting any further for the prerequisite sequence numbers.

If the rule has a traffic policy as duplicate path, the default hold time is 80 ms. Otherwise, the default is 900 ms for TCP rules and 250 ms for non-TCP rules.

 Discard Late Resequencing Packets: Discards out-of-order packets that arrived after the packets needed for resequencing have been sent to the LAN.

Click **Save** to save the configuration settings.

 Edit Apps & Domains (Global Rules) 			
Apps & Domains Match Criteria			
Augus & Damana "	tere Dortert App	Routing Domain	
	v	Any	
Source Mesonik	Depth alton Network		
Any	Any		Sing = Dealt
Saura Pert	Destructure Part		
Arg	Any		Brs + Dest
Evaluar Variaus Data Traditic Datasy Variaus And Asserve Star Any Softwarmined by routing QoS Settings	v	Yuth; Micz Load Balanca Paths	
Transfer Type*	Produ [*]		
Interactive v	Medium	v	
Note: Bandwidth share available per QoS class per avarlay virtual path is de Intelligent default values are auto-picked, with ability to overvide the default	termined by QoS Profiles to vie oustom QoS profiles		
© Advanced Settings			
Cancel Save			

Click **Verify Configuration** on the **Configuration** > **QoS** > **QoS Policies** page to validate any audit error.

		Verify Configuration Software Version: 113225-04
	0	
Global Rules	Site / Group Specific Rules	

Create custom application rules

You can also create custom application rules. To create a custom application rule, navigate to **Configuration > QoS > QoS Policies > Custom Application Rules**. Select **Global Rules** tab for creating custom application rules at the global level or **Site/Group Specific Rules** for creating rules at a site level.

Click **New Custom Application Rule** under the **Custom Application Rules** section. Click **New Custom App** next to the **Custom Application** field name. Enter a name for the custom application. In the **Match Criteria** section, select the application, protocol, DSCP tag and enter the network IP and port number. Click **Save**.

Enter details in the other fields as needed. For information on field descriptions, refer Create application rules.

Citrix SD-WAN Orchestrator

← Edit Custom Application (Global Rules)						
Custom Application Match Criteria						
Evolution Application *	Time Doctory Aug	Realing Sumain	P Address			
	Ŷ	Any v				
Virtual Path Traffic Policy						
C Enable Virtual Path Traffic Policy						
Unual Felh Remote Site		Traffic Policy				
Any (determined by routing)	Ŷ	Loed Balance Partis 🗢 🗸				
QoS Settings						
Transfer Type*	Proping *					
Interactive v	Medium	v				
Note: Bandwidth share available per QoS class per overlay virtual peth is det Intelligent default values are auto-picked, with ability to overvide the defaults	rmined by <u>QuS Profiles</u> , via custom QuS profiles					
O Advanced Settings						
Cancel Save						

Create application group rules

You can create rules for a group of applications. To create application group rules, navigate to **Configuration > QoS > QoS Policies > Application Group Rules**. Select **Global Rules** tab for creating application group rules at the global level or **Site/Group Specific Rules** for creating rules at a site level.

Click **New Application Group Rule** under the **Application Group Rules** section. Click **New App Group** next to **Application Group** field name. Enter a name for the application group. Search and add applications as needed. Click **Save**.

Enter details in the other fields as needed. For information on field descriptions, refer Create application rules.

 Edit Application Group (Global Rules) 				
Application Group Match Criteria				
Application forward	THE ARE DONE	Roung Summ	P Address	
	v	Any	v	
Virtual Path Traffic Policy				
Distability Visual: Path: Traffic Paticy				
Virtual Path Remote time		Traffic Palica		
Any idelemined by routing)	v	Losd Balance Paths	u l	
QoS Settings				
Transfer Type"	houring ⁴			
hirsche v	Medum	~		
Note: Bandwidth share available per GoS class per averlay virtual path is dete- intelligent default values are auto-picked, with ability to overvide the defaults	mined by <u>Oct Profiles</u> via custom Oct profiles			
O Advanced Settings				
Carcel Save				

Verify application rules

To verify application rules, navigate to **Reports > Real Time > Flows**. Select the site for which you want to view the flow information and the number of flows to display. Click **Customize Columns**

and select the check boxes corresponding to the flow information you want to view. Verify if the flow information is according to the configured rules.

Navigate to **Reports > Real Time > Statistics** and select **Rules**. Choose the site and click **Retrieve latest data**. Verify the configured rules.

For more information about reporting, see Flows.

Classes

November 25, 2021

Citrix SD-WAN Orchestrator service provides a default set of application and IP/Port based QoS policies that are applied to all traffic going over Virtual Paths. These settings can be customized to fit the deployment needs.

Classes are useful to prioritize the traffic. Application and IP/Port based QoS policies classify traffic and put it into appropriate classes specified in the configuration.

For more information on application based QoS policies and IP address based QoS policies, see QoS policies.

Citrix SD-WAN Orchestrator service supports 13 classes. The following are the default 13 classes:

Bandwidth allocation per QoS Class							
Traffic Type	ic Type Bandwidth Share						
		Realtime Classes: Bandwidth Breakup					
		HDX High	96				
Realtime	5	High					
		Medium	.56				
		Low	56				
		Interactive Classes: Bandwidth B	Breakup				
		HDX High	%				
		HDX Medium	56				
Interactive	5	HDX Low	.56				
		High	.56				
		Medium	96				
		Low	56				
		Bulk Classes: Bandwidth Breakup (Relative Share)					
	56	High	96				
Bulk	(Best Effort, Not Guaranteed)	Medium	56				
		Low	96				
Cancel Save							

The following are the different types of classes:

- **Real-time**: Used for low latency, low bandwidth, time-sensitive traffic. Real-time applications are time sensitive but do not require 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 bulk class. These applications involve little human interference and are mostly handled by the systems themselves.

Bandwidth sharing among classes

Bandwidth is shared among classes as follows:

- **Real-time**: Traffic hitting real-time classes are guaranteed to have low latency and bandwidth is capped to the class share when there is competing traffic.
- **Interactive**: Traffic hitting the interactive classes get remaining bandwidth after serving realtime traffic and the available bandwidth is fair shared among the interactive classes.
- **Bulk**: Bulk is best effort. Bandwidth left over after serving real-time and interactive traffic is given to bulk classes on a fair share basis. Bulk traffic can starve if real-time and interactive traffic uses all the available bandwidth.

Note

Any class can use all available bandwidth when there is no contention.

The following example explains the bandwidth distribution based on the class configuration:

Consider there is an aggregated bandwidth of 10 Mbps over Virtual Path. If the class configuration is:

- Real-time: 30%
- Interactive High: 40%
- Interactive Medium: 20%
- Interactive Low: 10%
- Bulk: 100%

The bandwidth distribution outcome is:

• Real-time traffic gets 30% of 10Mbs (3 Mbps) based on the need. If it needs less than 10%, then the rest of the bandwidth is made available to the other classes.

- Interactive classes share the remaining bandwidth on fair share basis (4 Mbps: 2 Mbps: 1 Mbps).
- Anything leftover when real-time, interactive traffic is not fully using their shares is given to the Bulk class.

For information about customizing QoS classes, see QoS profiles.

Application classification

October 20, 2022

The Citrix SD-WAN appliances perform deep packet inspection (DPI) to identify and classify applications using the following techniques:

- DPI library classification
- Citrix-proprietary Independent Computing Architecture (ICA) classification
- Application vendor APIs (for example Microsoft REST APIs for Office 365)
- Domain name based application classification

DPI library classification

The Deep Packet Inspection (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 Settings & Groups > DPI Settings** and clear the **Enable Global DPI** check box option.

To enable DPI library classification, in the **Configuration Editor**, navigate to **Global > Applications > DPI Settings** and select the **Enable Deep Packet Inspection** check box.

Citrix SD-WAN Orchestrator

Verify Config Application Settings	
Global Application Settings	
Site Overrides Application Settings will be applied to the sites listed below	
Sites (1) Boston	Select Sites
Save	

ICA classification

Citrix SD-WAN appliances can also identify and classify Citrix HDX traffic for virtual apps and desktops. Citrix SD-WAN recognizes the following variations of the ICA protocol:

- ICA
- ICA-CGP
- Single Stream ICA (SSI)
- Multi-Stream ICA (MSI)
- ICA over TCP
- ICA over UDP/EDT
- ICA over non-standard ports (including Multi-Port ICA)
- HDX Adaptive Transport
- ICA over WebSocket (used by HTML5 Receiver)

Note

Classification of ICA traffic delivered over SSL/TLS or DTLS is not supported in SD-WAN Standard Edition but is supported in SD-WAN Premium Edition and SD-WAN WANOP Edition.

Classification of network traffic is done during initial connections or flow establishment. Therefore, pre-existing connections are not classified as ICA. Classification of connections is also lost when the connection table is cleared manually.

Framehawk traffic and Audio-over-UDP/RTP are not classified as HDX applications. They are reported as either "UDP" or "Unknown Protocol."

Since release 10 version 1, the SD-WAN appliance can differentiate each ICA data stream in multistream ICA even in a single-port configuration. Each ICA stream is classified as a separate application with its own default QoS class for prioritization.

- For Multi-Stream ICA functionality to work properly, use SD-WAN Standard Edition 10.1 or above, or SD-WAN Premium Edition.
- For HDX user based reports to be shown on SDWAN-Center, use SD-WAN Standard Edition or Premium Edition 11.0 or above.

Minimum software requirements for HDX information virtual channel:

- A Current Release of Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop), since the prerequisite functionality was introduced in XenApp and XenDesktop 7.17 and is not included in the 7.15 Long-Term Service Release.
- A version of the Citrix Workspace app (or its predecessor, Citrix Receiver) that supports multi-stream ICA and the HDX Insights information virtual channel, CTXNSAP. Look for HDX Insight with NSAP VC and Multiport/Multi-stream ICA in the Citrix Workspace app Feature Matrix. See the currently supported release versions at HDX Insights.
- From 11.2 release onwards, packet duplication is now enabled by default for HDX real-time traffic when multi-stream ICA is in use.

Once classified, the ICA application can be used in application rules and to view application statistics similar to other classified applications.

There are five default application rules for ICA applications one each for the following priority tags:

- Independent Computing Architecture (Citrix)(ICA)
- ICA Real-time (ica_priority_0)
- ICA Interactive (ica_priority_1)
- ICA Bulk-Transfer (ica_prority_2)
- ICA Background(ica_priority_3)

For more information, see Rules by Application Name

If you are running a combination of software that does not support Multi-Stream ICA over a single port, then to perform QoS you must configure multiple ports, one for each ICA stream.

To classify HDX on non-standard ports as configured in XA/XD server policy, you must add those ports in ICA port configurations. Also, to match traffic on those ports to valid IP rules, you must update the ICA IP rules.

In ICA IP and port list you can specify non-standard ports used in XA/XD policy to process for HDX classification. IP address is used to further restrict the ports to a specific destination. Use '*'for port destined to any IP address. IP address with combination of SSL port is also used to indicate that the traffic is likely ICA even though traffic is not finally classified as ICA. This indication is used to send L4 AppFlow records to support multi-hop reports in Citrix Application Delivery Management.

For information on enabling ICA classification, see HDX QoE configuration

	MCN	Orchestartor service
ICA	On	On
MSI	On	Off
HDX reporting	On	Off
Application QoE	Not configured	Not configurd

ICA behaviour matrix

Application vendor API based classification

Citrix SD-WAN supports the following application vendor API based classification:

- Office 365. For more information, see Office 365 optimization.
- Citrix Cloud and Citrix Gateway service. For more information, see Gateway Service Optimization.

Domain name based application classification

The DPI classification engine is enhanced to classify applications based on the domain name and patterns. After the DNS forwarder intercepts and parses the DNS requests, the DPI engine uses IP classifier to perform first packet classification. Further DPI library and ICA classification are done and the domain name based application ID is appended.

The Domain name based application feature allows you to group several domain names and treat it as a single application. Making it easier to apply firewall, application steering, QoS, and other rules. A maximum of 64 domain name based applications can be configured.

To define domain name based applications, at the network level, navigate to **App Settings & Groups** > **Domains & Apps** > **Domain Name Based Apps**. Enter an application name and add the required domain names or patterns. You can either enter the full domain name or use wild cards at the beginning. The following domain name formats are allowed:

- example.com
- *.example.com

omain Name Based Apps	Pre-classified Apps	
Somain based App Name		
Ecommerce		
Configure Ports		
Add Domains		
Domain Name/Pattern		Delete
www.amazon.com		Ē

The classified domain name based applications are used in configuring the following:

- DNS Proxy
- DNS Transparent forwarder
- Application objects
- Application Routes
- Firewall policy
- Application QoS Rules
- Application QoE

Note

From Citrix SD-WAN 11.5 onwards, IPv6 and AAAA records are supported.

Limitations

- If there are no DNS request/response corresponding to a domain name based application, the DPI engine does not classify the domain name based application and hence does not apply the application rules corresponding to the domain name based application.
- If an Application Object is created such that the port range includes port 80 and/or port 443, with a specific IP address match type that corresponds to a domain name based application, the DPI engine does not classify the domain name based application.
- If explicit web proxies are configured, you have to add all the domain name patterns to the PAC file, to ensure that the DNS response does not always return the same IP address.
- The domain name based application classifications are reset on configuration upgrade. Reclassification happens based on pre 11.0.2 release classification techniques such as DPI library classification, ICA classification and Vendor application APIs based classification.
- The application signatures learned (destination IP addresses) by domain name based application classification are reset on configuration update.
- Only the standard DNS queries and their responses are processed.
- DNS response records split over multiple packets are not processed. Only DNS responses in a single packet are processed.
- DNS over TCP is not supported.
- Only top-level domains are supported as domain name patterns.

Classifying encrypted traffic

Citrix SD-WAN appliance detects and reports encrypted traffic, as part of application reporting, in the following two methods:

- For HTTPS traffic, the DPI engine inspects the SSL certificate to read the common name, which carries the name of the service (for example - Facebook, Twitter). Depending on the application architecture only one certificate might be used for several service types (for example - email, news, and so on). If different services use different certificates, the DPI engine would be able to differentiate between services.
- For applications that use their own encryption protocol, the DPI engine looks for binary patterns in the flows, for instance in case of Skype the DPI engine looks for a binary pattern inside the certificate and determines the application.

For detailed procedure on configuring encrypted traffic and viewing reports, see HDX QoE.

To configure application classification settings:

Application Groups

Application groups enable you to group different types of match criteria into a single object that can be used in firewall policies and application steering. IP Protocol, Application, and Application Family are the available match types.

The following features use application groups as a match type:

- Application Routes
- Firewall policy
- Application QoS Rules
- Application QoE

For more information on creating application groups, see Application Groups

MPLS queues

June 28, 2022

MPLS queues simplify creating SD-WAN configurations when adding a Multiprotocol Layer Switching (MPLS) WAN Link.

Citrix SD-WAN Orchestrator service allows you to add an MPLS specific WAN Link (that is, Access Type). When a new Private MPLS Access Type is selected, you can define the MPLS queues associated with the WAN Link. This allows a single VIP with multiple DSCP tags that correspond to the provider's queuing implementation for the MPLS WAN Link. This maps the Intranet Service to multiple MPLS Queues on a single MPLS WAN Link.

It also allows MPLS providers to identify traffic based on DSCP markings so that the class of service can be applied by the provider.

Note

If you have existing MPLS configurations and would like to implement the Private MPLS Access Type, contact Citrix Support for assistance.

Configure MPLS queues

- To configure MPLS queues, at the site level, navigate to Configuration > Site Configuration > WAN Links.
- 2. Click + WAN Link and select the Create New radio button.

- 3. Select **MPLS** from the **Access Type** drop-down list. Choose your ISP from the **ISP Name** dropdown list.
- 4. Provide a name for the MPLS link. Enter egress and ingress speeds and their corresponding physical or permitted rates.
- 5. Click + Queue under the MPLS Queues section. Provide the following details and click Save.
 - 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, DCSP 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.

MPLS Queues						
Queue Name:MPLS-Captive_Audience-QUEUE-1						
DSCP Tag *		LAN to WAN (%) *	WAN to LAN (%) *			
default	\sim	50	50			
Tracking IP Address	C	Congestion Threshold (µs)	_			
a.b.c.d		20000	✓ Unmatched No Retag			
Eligibility :						
		LAN to WAN	WAN to LAN			
	Real Time	\checkmark	\checkmark			
	Interactive	\checkmark	\checkmark			
	Bulk	\checkmark	\checkmark			
			Osmaal	0		

- 6. Enter access interface details and other required details under **WAN Links**. Save the WAN link configuration.
- 7. Navigate to **Configuration > Link Settings > Interlink Communication**. On the **MPLS Groups** tab, click + **MPLS Inter-link Communication Group**.
- 8. If there is no one-to-one mapping based on the DSCP tag between queues at the local site and the remote site, you must map MPLS Queues to specific Autopath Groups. Inheriting an Autopath Group from the MPLS WAN Link automatically generates paths between queues with matching DSCP tags. All the MPLS links belonging to the ISPs listed under one group can talk to each other by default, through auto-creation of paths.

Provide a name for the MPLS group, choose a DSCP tag. Click + MPLS Provider and select the ISP from the drop-down list. Click **Save**.

Note

You cannot create multiple MPLS queues using a WAN link template with the same Internet service provider name. However, you can use a different WAN link template with a different Internet service provider name, and use that template to create the site WAN link.

Interlink Communication (i)

	Group Name	Description				
	Internet-All	All Internet links can talk to each other by default. If a sub-set of internet links need to talk only ar	All Internet links can talk to each other by default. If a sub-set of internet links need to talk only among th			
2	MPLS-Same-ISP	All MPLS links belonging to the same ISP can talk to each other by default, through auto-creation	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	-creatio			
usto	m Inter-link Communication Groups					
_S Gro	up Name *	DSCP Tag				
+ N	IPLS Provider					
	LNET	Custom				
BE		Custom				

QoS fairness (RED)

November 12, 2021

The QoS fairness feature improves the fairness of multiple virtual path flows by using QoS classes and Random Early Detection (RED). A virtual path can be assigned to one of 16 different classes. A class can be one of three basic types:

- Real-time classes serve traffic flows that demand prompt service up to a certain bandwidth limit. Low latency is preferred over aggregate throughput.
- Interactive classes have lower priority than real-time but have absolute priority over bulk traffic.
- Bulk classes get what is left over from real-time and interactive classes, because latency is less important for bulk traffic.

Users specify different bandwidth requirements for different classes, which enable the virtual path scheduler to arbitrate competing bandwidth requests from multiple classes of the same type. The scheduler uses the Hierarchical Fair Service Curve (HFSC) algorithm to achieve fairness among the classes.

HFSC services classes in first-in, first-out (FIFO) order. Before scheduling packets, Citrix SD-WAN examines the amount of traffic pending for the packets class. When excessive traffic is pending, the packets are dropped instead of being put into the queue (tail dropping).

Why does TCP cause queuing?

TCP cannot control how quickly the network can transmit data. To control bandwidth, TCP implements the concept of a bandwidth window, which is the amount of unacknowledged traffic that it allows in the network. It initially starts with a small window and doubles the size of that window whenever acknowledgments are received. This is called the slow start or exponential growth phase.

TCP identifies network congestion by detecting dropped packets. If the TCP stack sends a burst of packets that introduce a 250 ms delay, TCP does not detect congestion if none of the packets are discarded, so it continues to increase the size of the window. It might continue to do so until the wait time reaches 600–800 ms.

When TCP is not in the slow start mode, it reduces the bandwidth by half when packet loss is detected, and increases the allowed bandwidth by one packet for each acknowledgment received. TCP therefore alternates between putting upward pressure on the bandwidth and backing off. Unfortunately, if the wait time reaches 800 ms by the time packet loss is detected, the bandwidth reduction causes a transmission delay.

Impact on QoS fairness

When TCP transmission delay occurs, providing any kind of fairness guarantee within a virtual-path class is difficult. The virtual path scheduler must apply tail-drop behavior to avoid holding enormous amounts of traffic. The nature of TCP connections is such that a small number of traffic flows to fill the virtual path, making it difficult for a new TCP connection to achieve a fair share of the bandwidth. Sharing bandwidth fairly requires making sure that bandwidth is available for new packets to be transmitted.

Random Early Detection

Random Early Detection (RED) prevents traffic queues from filling up and causing tail-drop actions. It prevents needless queuing by the virtual path scheduler, without affecting the throughput that a TCP connection can achieve.

How to use RED

- 1. Start a TCP session to create the virtual path. Verify that with RED enabled, the wait time on that class stays at around 50 ms in the steady state.
- 2. Start a second TCP session and verify that both the TCP sessions share the virtual path bandwidth evenly. Verify that the wait time on the class stays at the steady state.
- 3. Verify that RED is enabled for a rule in SD-WAN Orchestrator Service.

How to enable RED

At the network level, navigate to **Configuration** > **QoS** > **QoS Policies**. Add a rule and navigate to **Advanced Settings** > **LAN to WAN** and select **Enable RED**.

WAN General Retransmit Lost Packets Enable Packet Aggregation LAN To WAN General: Drop Depth (bytes) Drop Limit (ms) 128000 50 Duplicate Packets Disable Depth (bytes) Duplicate Packets Disable Depth (bytes) Duplicate Packets Disable Depth (bytes) Outplicate Packets Disable Depth (bytes) Duplicate Packets Disable Limit (ms) 128000 0 MAN to LAN Dscp Tag Any Enable Packet Resequencing Discard Late Resequence Packets	Advanced Settings				×
Retransmit Lost Packets Enable Packet Aggregation LAN To WAN General: Drop Depth (bytes) Drop Limit (ms) 128000 50 Duplicate Packets Disable Depth (bytes) Duplicate Packets Disable Depth (bytes) 128000 Ouplicate Packets Disable Depth (bytes) 0 VAN to LAN Dscp Tag Hold Time (ms) Any Enable Packet Resequencing Discard Late Resequence Packets	WAN General				
LAN To WAN General: Drop Depth (bytes) 128000 50 Duplicate Packets Disable Depth (bytes) Duplicate Packets Disable Depth (bytes) 128000 MAN to LAN Dscp Tag Hold Time (ms) Any Image: Comparison of the time (ms) Discard Late Resequence Packets	Retransmit Lost Packets	Enable Pac	ket Aggregation		
General: Drop Depth (bytes) 128000 50 Duplicate Packets Disable Depth (bytes) Duplicate Packets Disable Limit (ms) 128000 0 WAN to LAN Dscp Tag Hold Time (ms) Any Enable Packet Resequencing Discard Late Resequence Packets	LAN To WAN				
Drop Depth (bytes) Drop Limit (ms) 128000 50 Duplicate Packets Disable Depth (bytes) Duplicate Packets Disable Limit (ms) 128000 0 WAN to LAN Dscp Tag Any Enable Packet Resequencing Discard Late Resequence Packets	<u>General :</u>				
128000 50 Duplicate Packets Disable Depth (bytes) Duplicate Packets Disable Limit (ms) 128000 0 WAN to LAN Dscp Tag Hold Time (ms) Any Enable Packet Resequencing Discard Late Resequence Packets	Drop Depth (bytes)	Drop Limit (ms)			
Duplicate Packets Disable Depth (bytes) Duplicate Packets Disable Limit (ms) 128000 0 WAN to LAN Dscp Tag Any Hold Time (ms) Discard Late Resequence Packets	128000	50		✓ Enable Red	
128000 0 WAN to LAN Image: Constraint of the second constraint of the secon	Duplicate Packets Disable Depth (bytes)		Duplicate Packets Disab	ıle Limit (ms)	
WAN to LAN Dscp Tag Hold Time (ms) Any Enable Packet Resequencing Discard Late Resequence Packets	128000		0		
Dscp Tag Hold Time (ms) Any Enable Packet Resequencing Discard Late Resequence Packets	WAN to LAN				
Any 🗸 Enable Packet Resequencing Discard Late Resequence Packets	Dscp Tag	ŀ	lold Time (ms)		
	Any 🗸 Enable Pack	ket Resequencing		Discard Late Resequence Packets	

QoS policies

January 27, 2022

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.

Citrix SD-WAN Orchestrator

Global Rules	Site / Group Specific Rules				
Sisted Qut Bandy	with Setault Profile				
Standard-H	DX-Multistream V				
Dandard HDX-M	distreen profile recommended for multi-streen VDK soms-ded	an Profiles			
Custom Applic	ation Rules Application Rules HDX Rules	Application Group Rules IP Rules Default	P-Protocol Rules		
Search	Q				
749	Protocol	DECF	Device	Transmit Mode	Quil Letting
1	5.0	af	Virtual Path	Duplicate Paths	High: Realtime
2	ICA.	Any	Wrtval Path	Load Balance Paths	High: Interactive
э	ICACSP	Any	Virtual Path	Losd Balance Paths	High: Interactive
4	ICAUDP	Any	Virtual Path	Losd Balance Paths	High: Interactive
5	ICACSPUDP	Any	Virtual Path	Load Balance Paths	High: Interactive
6	ICMP	Any	Virtual Path	Persistent Path	Medium: Interactive
7	55H	Any	Virtual Path	Load Balance Paths	Medium : Interactive
8	TELNET	Any	Virtual Path	Load Balance Paths	Medium: Interactive
9	ROP	Any	Virtual Path	Load Balance Paths	Medium: Interactive
10	RPC	Any	Virtual Path	Load Balance Paths	Medium: Interactive

Create new rule

An administrator must place the defined rule based on the priority. The priorities are categorized based on parameters such as top of the list, bottom of the list, or a specific row.

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 selected. 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

Navigate to **Configuration** > **QoS** > **Custom Application Rules**. Specify how the traffic needs to be steered.

 Edit Custom Application (Global Rules) 			
Custom Application Match Criteria			
Contrart Application*	The Control Age Reading Domain	# Address	
	√ Any	v	
Virtual Path Traffic Policy			
C Drabbe Virsual Path Traffic Policy			
Virtual Path Remote Site	Traffic Policy		
Any literamined by routing	Used Balance Paths	v	
QoS Settings			
handertige* to	ang*		
Interactive v	Melun v		
Note: Bandwidth share available per QoS class per overlay virtual path is determ intelligent default values are auto-picket, with ability to override the defaults via	ined by <u>Out Profiles</u> - custom God profiles		
O Advanced Settings			
And a			

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

- Custom application
- Protocol (TCP, UDP, ICMP)
- Network IP/Prefix
- Port
- DSCP tag

You can also create a domain name based custom application.

Custom Applications	5				
Custom App Name*					
Enter Name					
Enable Reporting					
Reporting Priority					
Match Criteria					
Add Match Criteria					
Application	Protocol	Network IP	Port	DSCP	Actions
Cancel Sav	re				

Click **Verify Configuration** on the **Configuration** > **QoS Policies** page to validate any audit error.

Citrix SD-WAN Orchestrator

	VerifyConfiguration Software Version: II.3.2.25-GA
Global Rules Site / Group Specific Rules	

IP Rules IP Rules help you to create rules for your network and take certain Quality of Service (QoS) decisions based on the rules. For more information on IP rules, see IP rules.

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

Default Global QoS P	Profile (Applicable	to all Virtual Paths)		
Default QoS Profile				Sites Count
Standard	\sim			0/0
Create New Default Pro	ofile			
Site Specific Overrid	es (Applicable to `"	`Site-Control Node`"` Virtual	Paths)	

Click **Verify Configuration** on the **Configuration** > **QoS Policies** page to validate any audit error.

		VerifyConfiguration Software Version: 8.3.2.25-GA
	©	
Global Rules	Site / Group Specific Rules	

Customizing QoS profiles

If the virtual path default sets are in use, classes can be modified under **Configuration** > **QoS** > **QoS Profiles**. Click **Create New Default Profile**, enter a name for the default set, select the sites, and update the bandwidth allocation for the QoS class. Click **Save**. For more information about Classes, see Classes.

Bandwidth allocation per QoS Class						
Traffic Type	Bandwidth Share					
Realtime		Realtime Classes: Bandwidth Br	eakup			
	%	HDX High	96			
		High	5			
		Medium	56			
		Low	s.			
	76	Interactive Classes: Bandwidth I	Breakup			
		HDX High	s			
		HDX Medium	56			
Interactive		HDX Low	5			
		High	5			
		Medium	56			
		Low	5			
		Bulk Classes: Bandwidth Break	up (Relative Share)			
	56	High	56			
Bulk	(Best Effort, Not Guaranteed)	Medium	96			
		Low	%			
Cancel Save						

HDX QoE

January 26, 2022

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 dashboard 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:

- At the network level, navigate to Configuration > App Settings & Groups > 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 Configurati	ion		
Туре	Application	QoE Profile	Actions
Application	ICA Realtime	DefaultQOEProfile	a
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.

 Navigate to Configuration > QoS > QoS Profiles and provide a name for the QoS profile. Standard-HDX-Multistream is the default QoS Profile selected and the HDX Reporting option is selected by default. Clear HDX Reporting if HDX reporting is not required.

Verif	y Config QoS Profiles			
QOS Profile Name * HDX-multi-st	e Name ream-profile			
Profile Mode HDX Multi St Custom Defir HDX	ream	IPI for HDX	Multi-stream QoS for HDX	HDX Reporting
No.	HDX IP / Prefix	HDX Port		

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 Classes: Bandw	vidth Breaku	p	
		HDX High	30	%	
Realtime	55 %	High	10	%	
		Medium	8	%	
		Low	7	%	
		Interactive Classes: Band	width Break	cup	
		HDX High	8	%	
		HDX Medium	4	%	
Interactive	30 %	HDX Low	2	%	
		High	8	%	
		Medium	5	%	
		Low	3	%	
		Bulk Classes: Bandwidth Breakup (Relative Share)			
	15 %	High	9	%	
Bulk (Be	(Best Effort, Not Guaranteed)	Medium	4	%	
		Low	2	%	

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

Configuration / QoS / QoS Profiles	
QoS Profiles @	
Default Global QoS Profile (Applicable to all Virtual Paths)	
Default QoS Profile	Sites Count
Test 💛 Create New Default Profile	0/5

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



5. Add HDX rules. These configurations assign proper QoS settings to HDX connections. To check the rule details or edit the rules, navigate to the **Actions** column, click the horizontal ellipsis (...), and select the **Edit** option. To change the setting of any default rule, click **Clone** and make the required modification.

Global Rules	Site / Group Specific Rules				
Custom Applic	ation Rules Application Rules HOX Rules App	ication Group Rules IP Rules Default IP-Protocol Rul	ing.		
Global Qui Bar	dwalth behault Profile				
Standard	HOX-Mutistream				
Danded Hits	Multistreen profile recommended for multi-stream ADX users-DeS BW	Posties			
Search	Q				New HOX Rule
Top of Li	at 🕐 Bottom of List. 🔿 Specify Row Number 👘 Row r	unber			
14	Application	Virtual Peth	Traffic Policy	Qui betting	Actions
1	ICA Realtime(cs, priority, 0)	Any	Duplicate Paths	High: HDK Realtime	
2	ICA Interactive(ca_priority_1)	Any	Load Balance Paths	High: HDX Interactive	
3	ICA Bulk-Transfer(ica, priority, 2)	Any	Load Balance Paths	Medium : HDX Interactive	
4	ICA Background(ca,priority,3)	Any	Load Balance Paths	Low:HDK Interactive	
5	Independent Computing Architecture (Citrici)cal	Any	Load Balance Paths	Medium : Interactive	

These configurations can be modified:

- QoS class: Real-time, Interactive, Bulk
- Traffic policy:
 - Duplicate Paths: The traffic is duplicated across multiple paths to increase reliability.
 - Persistent Path: The traffic of a flow remains 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.

Citrix SD-WAN Orchestrator

🕤 Edit Citrix HDX (Global Rules)

Citrix HDX Match Criteria					
Application *		Realing Damas			
	~	Any	~		
bourde hereienk	Destruction Network				
Any	Any		Sirc + Deat		
Ann	bectranae nan		Site + Deat		
~7	14				
Virtual Path Traffic Policy					
🛃 Enable Wesail Path Traffic Policy					
Velual Path Remote Site		Traffic Policy			
Any (determined by routing)	v	Load Balance Paths	¥		
QoS Settings					
hander type"	Priority*				
Hereive v	Medium				
Note: Bandwidth share available per QuS class per overlay virtual path is deto	armined by Oct. Profiles				
intelligent default values are auto-picked, with ability to overvide the defaults	a via custom QoS profiles				
O Advanced Settings					
Cancel Seve					
Advanced Settings					
Advanced Settings					
Advanced Settings					
Advanced Settings					
Advanced Settings WAN General					
Advanced Settings VAN General	C Enable	Pecket Aggregation			i
Advanced Settings WAN General	_ Enable	Packet Aggregation			
Advanced Settings WAN General Petransmit Lost Packets	Enable I	Packet Aggregation			
Advanced Settings WAN General Retransmit Lost Packets .AN To WAN	Enable I	Packet Aggregation			
Advanced Settings WAN General Retransmit Lost Packets .AN To WAN General :	Enable I	Packet Aggregation			
Advanced Settings WAN General Retransmit Lost Packets AN To WAN General : rrat Graph Runnel	Conplication	Packet Aggregation			
Advanced Settings WAN General Retransmit Lost Packets AN To WAN Reneral : reg Graph Retrail 120000	Enable I Drug Limit im 50	Packet Aggregation		Enable Red	
Advanced Settings WAN General Petransmit Lost Packets AN To WAN General : reg Greph Ryted 128000	Enable I Dreg Lent int 50	Packet Aggregation		Enable Red	
Advanced Settings WAN General WAN General Retransmit Lost Packets LAN To WAN General : Instruction bytend I 20000 Nutlicere Packets Depth Bytend	Drep Lieft for 50	Packet Aggregation	uplicate Precient Stable Limit Imi	Enable Red	
Advanced Settings VAN General Or Petransmit Lost Packets AN To WAN General: res Draph flyted 120000 upticate Packets Death Eyen) 120000	Enable I Drag Liett im S0	Packet Aggregation	uplicate Packats Double Limit Ind	Enable Red	
Advanced Settings WAN General WAN General Retransmit Lost Packets AN To WAN General: rationation for the set of the set o	Drep Linit im	Packet Aggregation	uplicane Precises Staable Limit limit	_ Enable Red	
Advanced Settings WAN General WAN General Retransmit Lost Packets AN To WAN General: rational Settings rational Settings rational Settings Retransmit Lost Packets Retransmit	Dree Linit im	Packet Aggregation	aplicane Packets Double Limit limit	_ Enable Red	
Advanced Settings VAN General VAN General Retransmit Lost Packets AN To WAN General: rat Depth Systel 128000 rations Fracients Double Depth Systel 128000 RAN to LAN	Drep Linit im	Packet Aggregation	uplicate Packets Double Limit limit	_ Enable Red	
Advanced Settings WAN General Petransmit Lost Packets AN To WAN General : 120000 120000 WAN to LAN 12000	Enabled Drug Linst lins 50	Packet Aggregation	aplicate Packets Disable Limit limit	_ Enable Red	
Advanced Settings WAN General WAN General Retransmit Lost Packets AN To WAN Receral: Retransmit Lost Packets Retransmit Lost P	Enable I Drug Limit for 50	Packet Aggregation	epicere Packets Deable Limit (ind) 0	Enable Red	
Advanced Settings WAN General Retransmit Lost Packets AN To WAN General : res Depth flyred S2000 Walkcer Fackets Depth flyred S2000 WAN to LAN We fac Any	c Enable I Crep Linit in Crep Linit in So rt Resequencing	Packet Aggregation	uplicate Prochets Double Limit limit 0	Enable Red	
Advanced Settings WAN General Retransmit Lost Packets LAN To WAN General Retransmit Lost Packets LAN To WAN General Retransmit Lost Packets LAN General Retransmit Lost Packets LAN General Retransmit Lost Packet Retr	Drap Liet in 50	Packet Aggregation	uplicate Packets Double Limit limit 0	Enable Red	
Advanced Settings WAN General WAN General Retransmit Lost Packets AN To WAN General : Tablered T28000 Tablecer Packets Death Byted T28000 WAN to LAN We Trac Any C Enable Packet	Dree Linit les	Packet Aggregation	asloose Packets Double Limit Ind 0	Card Late Resequence Packets	
Advanced Settings WAN General Retransmit Lost Packets LAN To WAN General: 128000 Vations Packets Deable Deable based 128000 WAN to LAN Nee Tra: Any Enable Packet	Enable Drug Limit de 50	Packet Aggregation	alicene Packets Deable Limit limit 0	Card Late Resequence Packets	
Advanced Settings WAN General Retransmit Lost Packets AN To WAN General : reso Graph Reyred 128000 Valourer Packets Double Depth Ryred 128000 VAN to LAN Nos Tre Any Concel Cancel	Creatient Creatient Creatient Creation So	Packet Aggregation	splicere Peckets Double Limit limit	Enable Red	
Advanced Settings VAN General Retransmit Lost Packets AN To WAN Reneral : res Depth flyred S20000 VAN to LAN Vest Tre Any Cancel Cancel Cancel	c Enabled Drep Livel im 50	Packet Aggregation	uplicate Peckets Studie Linit Ind 0	Enable Red	

Note

For more information about Classes, see Classes.

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 introduce 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 roundtrip 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**.

Reports /	HDX /	Sites								
HDX Performance Last 1 Hour Y										
Sites 6 Total Sites	2 Good QoE (71-100)	0 Fair QoE (51-70)	4 Poor QoE (0-50)		100 - 80 - Number of Sites (% 40 - 20 - 0 -	Site Distribution I	3ased Upon Qc	DE (Over Last 1	L Hour) Later Destination of the second sec	15:20
							Good QoE	(71-100)	Fair QoE (51-70)	Poor QoE (0-50)
Top Affected S	Sites						Good QoE	(71-100)	Fair QoE (51-70)	Poor QoE (0-50)
Top Affected Site Name	Sites QoE Score((0-100) 🔺	Total Users	Total Sessions	Poor HDX QoE Users	Avg WAN Latency	Good QoE Avg Jitter	(71-100) Avg Loss	Avg Throughput	Poor QoE (0-50) Volume
Top Affected Site Name BRANCH1	Sites QoE Score(14	(0-100) 🔺	Total Users	Total Sessions	Poor HDX QoE Users	Avg WAN Latency 126.7 ms	Good QoE Avg Jitter 119.72 ms	(71-100) • Avg Loss 1.38 %	Avg Throughput 0.3 Kbps	Volume 135.52 KB
Top Affected Site Name BRANCH1 branch_1100	Sites QoE Score(14 14	(0-100) 🔺	Total Users 1 2	Total Sessions 1 2	Poor HDX QoE Users	Avg WAN Latency 126.7 ms 125.83 ms	Good QoE Avg Jitter 119.72 ms 119.07 ms	(71-100) • Avg Loss 1.38 % 1.19 %	Fair QoE (51-70) Avg Throughput 0.3 Kbps 0.3 Kbps	Volume 135.52 KB 271.29 KB
Top Affected Site Name BRANCH1 branch_1100 BRANCH4	Sites QoE Score 14 14 14	(0-100) 🔺	Total Users 1 2 1	Total Sessions 1 2 1	Poor HDX QoE Users 1 1 1 1	Avg WAN Latency 126.7 ms 125.83 ms 126.79 ms	Good QoE Avg Jitter 119.72 ms 119.07 ms 120.85 ms	(71-100) • • • • • • • • • • • • • • • • • •	Fair QoE (\$1-70) Avg Throughput 0.3 Kbps 0.3 Kbps 0.3 Kbps	Volume 135.52 KB 271.29 KB 135.58 KB
Top Affected Site Name BRANCH1 branch_1100 BRANCH4 BRANCH2	Sites QoE Score(14 14 14 15	(0-100) 🔺	Total Users 1 2 1 1	Total Sessions 1 2 1 1	Poor HDX QoE Users 1 1 1 1 1 1	Avg WAN Latency 126.7 ms 126.79 ms 126.75 ms	Good QoE Avg Jitter 119.72 ms 119.07 ms 120.85 ms 121.03 ms	(71-100) • • • • • • • • • • • • • • • • • •	Fair QoE (\$1-70) Avg Throughput 0.3 Kbps 0.3 Kbps 0.3 Kbps 0.3 Kbps 0.3 Kbps	Volume 135.52 KB 271.29 KB 135.54 KB 135.54 KB
Top Affected Site Name BRANCH1 branch_1100 BRANCH4 BRANCH2 BRANCH3	Sites QoE Score(14 14 14 15 98	(0-100)	Total Users 1 2 1 1 1 1 1 1	Total Sessions 1 2 1 1 1 1	Poor HDX QoE Users 1 1 1 1 1 0	Avg WAN Latency 126.7 ms 126.79 ms 126.75 ms 126.84 ms	Good QoE Avg Jitter 119.72 ms 119.07 ms 120.85 ms 121.03 ms 121.36 ms	(71-100) Avg Loss 1.38 % 1.19 % 1.43 % 1.43 % 0.1 %	Fair QoE (\$1-70) Avg Throughput 0.3 Kbps 0.3 Kbps 0.3 Kbps 0.3 Kbps 0.3 Kbps 0.3 Kbps	Volume 135.52 KB 271.29 KB 135.54 KB 377.43 KB

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 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 time period, 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 Citrix SD-WAN Orchestrator service 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 /	Reports / HDX / Sites / Details									
HDX Perfo	HDX Performance Last 1 Hour Y									
Search		Q								
Site Name		Total Users	Total Servions	Poor HDX OoF Upper	Ave WAN Latency	Avo littor	Avalors	Ave Throughout	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**.

HDX Per	HDX Performance Last 1 Hour 🗸							
Users 6 Total Users	1 0 Good QoE Fair QoE (71-300) (53-70)	5 Peor QoE (0-50)	Number of Users (N)	User Di 100 80 60 	stribution Based 4 weday, See 29, 14 5 Poor Qof (0–50): 14/50 15	Upon QoE (Over 5 83 %	Last 1 Hour)	15:30 15:40 • Peer QuE (0-50)
Top Affected	Users							
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	117.02 ms	1.17%	0.3 Kbps	135.69 KB
user1	14	BRANCH1	1	126.76 ms	119.69 ms	1.39 %	0.3 Kbps	137.75 KB
user4	14	BRANCH4	1	126.79 ms	120.97 ms	1.44 %	0.3 Kbps	135.52 KB
user5	14	branch_1100	1	125.75 ms	119.62 ms	1.19 %	0.3 Kbps	135.6 KB
user2	15	BRANCH2	1	126.84 ms	121.1 ms	1.43 %	0.3 Kbps	135.6 KB
							View mo	ore affected users
				~				1

The user report shows the performance experienced by each user during the selected period (for ex-

ample, 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 time period. 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 descending, 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 time period, 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 singlestream 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 Citrix SD-WAN Orchestrator service 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 Y									
Search		Q							
Licor Namo	005 Scoro(0.100)	Site Name	Total Sersions	Ave WAN Latency	Aug litter	Avalors	Ava 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.



HDX Performance Last 1 Hour ~

Sessions

The Session report provides details at the session level. To view the session report, navigate to **Re-ports > 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 time period, 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 Citrix SD-WAN Orchestrator service GUI might adjust and change the unit based on the number value.

Clicking any column title, shows the report sorted on that column. Clicking **View more affected sessions** shows 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.

HDX Performance | Last 1 Hour Y

Search	Q							
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
4F568893E203448AA241189936CBE70B	14	administrator	125.8 ms	116.41 ms	1.18%	0.3 Kbps	135.69 KB	ACTIVE
790EE85C53A2419584C488E775D8E173	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
428EFFA8CE39402C8A318C78AA3E36DE	15	user2	126.85 ms	120.87 ms	1.46 %	0.3 Kbps	135.54 KB	ACTIVE
941C878392D247E682980F486A705840	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.



- 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 disconnected and reconnects 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.

Routing

April 4, 2022

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.

	Verify Config Ap	plication Routes IP	P Routes				
Cost Rang	es: Custom Application	n (1-20) Application (2	21-40) Application Group (41	-60) IP (1-65535)			
+ Ap	plication Route		Search for Route		Q		
No	Match Type	Name	Delivery Service	Routing Domain	Sites	Cost	Actions
1	Custom Applicati	customapp23	Internet Breakout	Any	Global	19	Ē
2	Application Group	Default Cloud Dir	Cloud Direct Service	Any	Global	45	Î
3	Application Group	03650ptimize_In	Internet Breakout	Any	Global	50	Ē
4	Application Group	Citrix_Cloud_and	Internet Breakout	Any	Global	50	Ē

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.

Verify Config Application	n Routes IP Rout	tes	
Cost Ranges: Custom Application (1-20)	Application (21-40)	Application Group (41-60)	IP (1-65535)
Apps & Domains Match Criteria			
Match Type	Apps & Domains *	+New Domain App	Routing Domain
Apps & Domains \lor	Ecommerce	~	Default_RoutingDomain ~
Scope			
Global Route Site / Group Speci	fic Route		
Traffic Steering			
Delivery Service	Cost*		
Internet Breakout	21		
Cancel Save			

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

Q	DASHBOARD		Ĝ	Verify Config Ar	pplication Routes	P Routes					
	REPORTS	>	Cost Ra	anges: Custom Applicatio	on (1-20) Application ((21-40) Application Group (4	I1-60) IP (1-65535)				
Ô	CONFIGURATION	~	•	Application Route			Search for Route		Q		
		_	No	Match Type	Name	Delivery Service	Routing Domain	Sites		Cost	Actions
	Network Config Home		1	Application Group	Default Cloud Dir	Cloud Direct Service	Any	Global		45	Ē
	Delivery Services	>	2	Application Group	03650ptimize_In	Internet Breakout	Any	Global		50	Ē
	Routing	~	3	Application Group	Citrix_Cloud_and	Internet Breakout	Any	Global		50	
	Routing Policies										
	Routing Domains										
	Import Route Profi	les									
	Export Route Profi	les									
	Transit Nodes										
	Link Settings	>									
	QoS	>									
	Security	>									
	Site & IP Groups	>									
	App & DNS Settings	>									
	Profiles & Templates										
	ECMP Groups										
	WAN Optimization	>									

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

	Verifu Confer							
REPORTS >								
	Cost Ranges: Costom Application (12-0) Application (21-40) Application Group (41-40) IP (1-65535)							
CONFIGURATION V	Application Group Match Criteria							
Network Config Home	Match Type Application Group *							
Delivery Services >	Application Group							
Routing 🗸								
Routing Policies	Scope							
Routing Domains	Global Route Site / Group Specific Route							
Import Route Profiles	Traffe Staning							
Export Route Profiles	Traffic Steering							
Transit Nodes	Detirery Service							
Link Settings >	Internet Breakout							
QoS >	0385 Network Optimization Settings							
Security >								
Site & IP Groups >	Revew Office 365 Network Connectative Principles							
App & DNS Settings >	Instruction LADITERATING CARL INTER INVESTIGATION CONTINUES AND ADDRESS AND ADDRES							
Profiles & Templates	🧭 Teams Realtime 📝 Exchange Online 🖉 SharePoint Optimize							
ECMP Groups	Allow: (Faski orthination for less labours sensitive ORR sensitive or "https:// in resterior autional cont" https://orthination.com							
WAN Optimization >	Z Teams TCP Failback Z Exchange Mail Z SharePoint Allow Z 0365 Common							
() ALERTS >								
	У цетаци: (но организато неринетато съоз венисен и пас сектору чуг, парагладо стансевра и е сото, парагладо сектори на съоз парагладо сектори на съоз парагладо сектори на съоз парагладо на Съоз парагладо на съоз br>Парагладо на съоз парагладо на съоз п съоз парагладо на съоз па съоз парагладо на съоз пара съоз па							
C TROUBLESHOOTING >	V Linked Understrike Text (V) Linked Good installigent is an understanding							
<	Cancel Save							

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. 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.
- **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.
- **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, the Optimize, Allow, and Default options 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.

IP Routes

	erify Config Applica	tion Routes	IP Routes		.,		
Cost Ranges:	Custom Application (1-20) Applica	ation (21-40)	Application Group (41-60)	IP (1-65535)		
IP Protocol	Match Criteria						
Destination Netwo	work *	Use IP Group	Routing Doma	in ~			
Scope							
 Global Rot 	ute 🔵 Site / Group	Specific Route					
Traffic Stee	ring						
Delivery Service	reakout	Cost *					
Eligibility C	riteria						
Z Export Rou	ute						
Cancel	Save						

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**: The cost field 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.

Route Summarization

Route summarization reduces the number of routes that a router must maintain. A summary route is a single route that is used to represent multiple routes. Route summarization saves bandwidth by sending a single route advertisement, reducing the number of links between routers. Route summarization saves memory because only one route address is maintained. The CPU resources are used more efficiently by avoiding recursive lookups. You have an option to add summary routes without specifying the gateway IP address.

Routing domains

Routing domain helps to improve network security/functionality and work with the IP network routers that enables multiple routing table instances to exist in a virtual router and work simultaneously. With this functionality, the connectivity increases by enabling the network paths to be segmented without using multiple devices as the traffic is automatically segregated. VRF also increases network security and can eliminate the need for encryption and authentication.

Routing domain focuses on Layer 3 traffic through MPLS. The multiprotocol label switching or MPLS cloud in the service provider cloud environment uses multiprotocol border gateway protocol or multiprotocol BGP. Routing domain isolates traffic from source to destination through that MPLS cloud. To

separate overlapping routes and make use of common services, Routing domain incorporates Route Distinguishers (RDs) and Route Targets (RTs).

The following topology describes how the routing domains work:



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.

Verify Config Ro	outing Domains	
Routing Domain		
+ Routing Domain		
Name	Default	Actions
Default_RoutingDomain	۲	
		-

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 Configu	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

Citrix SD-WAN Orchestrator service 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 Citrix SD-WAN Orchestrator service:

- 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.

Routing Domains i

Default	Actions
۲	
ce	
Routing Domain1	Routing Domain2
	Ce Routing Domain1

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.

Routing Policies (i)
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
172.16.18.0/24 Domain1 V
Scope
Global Route O Site / Group Specific Route
Traffic Steering
Delivery Service Name* Cost*
Inter Routing Domain V interroutedomain1 V 5
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.

Firewall Policies (i)

Delieu Information			
Policy Information			
Policy Name *			
poliicy1	Active Policy		
Firewall Type			
Built-in Firewall	~		
Match Criteria			
Match Type	Routing Domain		
Apps & Domains	✓ Default_RoutingDor	nain V	
Apps & Domains * + Ne	w Domain App		
Base virtual protocol	\checkmark		
Filtering Criteria			
Source Zone		Destination Zone	
Any ×	×	Any X	\sim
Source Service Type	Source Service Name *	Source IP	Source Port
Inter Routing Domain	v interroutedomain1	Any	Any
Dest Service Type	Dest Service Name *	Dest IP	Dest Port
Inter Routing Domain	v interroutedomain1	Any	Any
IP Protocol	DSCP		
Any	Any	Allow Fragments Reverse Also	Match Established
Actions			
Action			
Allow	~		
Connection State Tracking			
✓ Log Connection Start & End E	vents		
✓ Log Packet Statistics Ev	very 5 mins \sim		

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 meet before importing dynamic routes into the SD-WAN route database. By default, no routes are imported.

Verify Config	Import Route Profiles	
+ Import Filter P	rofile	
Profile Name		Actions
Default		圃
one		<u></u>

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 Profile	Name *							
Sample-i	mport-filter-profile							
Import Filte	rs							
Protocol	Routing Domain	Source Router	Destination IP	Use IP Group	Prefix	Next Hop	Route Tag	
Any 🗸	Default_RoutingDomain	*	*		eq 🗸 *	*	*	
🗸 Include	Export F	Route to Citrix SD-WAN Ap	pliances					
Citrix SD-WAN	Cost * Service Type							
6	Local	\sim						
Cance	Done							_
Profile Avai	lability							
Import Filte	r Profile Settings will be a	applied to the sites listed	below				Select Sites	
Sites (2)								
Sites (2) Boston								
Sites (2) Boston Dallas								
Sites (2) Boston Dallas								

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 *					
sample-export-filter-profile					
Export Filters					
Routing Domain	Network Address/Mask 🗹 Use IP Group	Prefix	Cost	Service Type	Gateway IP Address
Default_RoutingDomain ~	ipg1 ~	eq ~ *	eq 🗸 *	Local	*
Export OSPF Route Type	Export OSPF Route Weight	🗸 Include			
Type 5 AS External 🗸 🗸	Weight				
Cancel Done					
Profile Availability					
Export Filter Profile Settings will be a	applied to the sites listed below			Select	Sites
Sites (1)					
Boston					

Click Verify Config to validate any audit error.

Transit nodes

Virtual overlay Transit Node

You can reduce the cost of routing by configuring a site to route data via a virtual overlay transit node. 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 via 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 The control nodes (MCN/RCN) and the geo-control nodes (Geo-MCN/RCN) are 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 control nodes as transit nodes, by default, for site-to-site communication. If you disable hub-and-spoke communication, ensure that there are site-specific rules that enable the non-control node to act as transit nodes.

Global Transit Node Settings			
Enable Spoke-to-Spoke communicatior	n via Hub by default across the network (Re	ecommended)	${\mathbb C}$ Restore Default
Control Transit Node Settings			
D This section hosts the configuration related Geo control nodes)	to override the global transit node settings	s on a specific or a set of control transit nodes in	the network. (MCN/RCN and
+ Add Node		+ Add Geo-Node	
Transit on Control Node	Default Virtual Path Cost (Site to Control Node)	Transit on Geo-Control Node	Default Virtual Path Cost (Site to Geo-Control Node)
Site1 Override Global Transit Settings Spoke to Spoke Forwarding Route Export	 ✓ 6 ⋒ 	S3 Cverride Global Transit Settings Spoke to Spoke Forwarding Route Export	6
SiteRCN Override Global Transit Settings Spoke to Spoke Forwarding Route Export	 ✓ 6 	SiteRegion2 Override Global Transit Settings	 ✓ 6

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.

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 Virtu	ual Ove	erlay Transit Nodes					
Primary Transit Node * Cos	t		Secondary Transit Node	Cost		Tertiary Transit Node	Cost
Germany_Masternode 🗸	6		London_Site 🗸	7		Greece_Site_Clone 🗸	8
Sites to be Routed via Intermediate Node							
Select Region/Groups		Select Sites					
✓ Select All		✓ Select All					
✓ default		✓ London_Site					
Cancel Review					Showing 1 - 2 of 2 it	ems Page 1 of 1	\mathbf{A}

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.

Verify Config Virtu	al Overlay Transit Nodes Internet Transit Nodes Intranet Transit Nodes
Primary Default Internet Trans	it Node 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 T	ransit Nodes for the Network
Service Name internet	v
Transit Node Settings will be app	Nied to the sites listed below Select Sites
	No Sites have been Selected
Save	

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.

Verify Config Virtu	al Overlay Transit Nodes Internet Transit Nodes Intranet Transit Nodes
Primary Default Intranet Trans	t Node 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 No	ides to reach the subnets selected
Service Name Non_SDWAN_Sites	~
Transit Node Settings will be app	lied to the sites listed below Select Sites
	No Sites have been Selected
Save	

Dynamic routing

August 10, 2022

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 first 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 all the configured routing domains (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.

Router ID Settings			
Routing Domain*		Router ID*	
Default_RoutingDomain	~		
Save Router ID Settings	Cancel		

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**: The IPv4 address used for OSPF advertisements. This field is optional. If it is not specified, the lowest virtual IPv4 address of the virtual interfaces participating in routing is chosen. For the IPv6 interface, it is mandatory to specify the router ID in IPv4 format. For example, 1.1.1.1.

Note

- The router ID configuration is optional for an IPv4 network. But for an IPv6 network, the router ID configuration is mandatory. The router ID for an IPv6 network must be configured in the same IPv4 format (32-bit notation).
- You must create separate IPv4 and IPv6 peering to the same router (if applicable) for learning and advertising.
- **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 ③					
OSPF BGP Import Filters Export	Filters				
OSPF Basic Settings Areas					
Enable					
Export OSPF Route Type					
Type 5 AS External \sim					
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*	Router ID *				
Default_RoutingDomain	✓				
Save Router ID Settings	ancel				

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	(i)

Area ID* Enter Area ID	Stub Area		
Virtual Interfaces	Routing Domain *	Authentication Type	Password
Virtual Interfaces Name * Select Interface	Routing Domain*	Authentication Type	Password
Virtual Interfaces Name* Select Interface Interface Cost*	Routing Domain *	Authentication Type None Hello Interval *	Password Center Password Dead Interval*

BGP

To configure BGP, navigate to **Configuration > Advanced Settings > Dynamic Routing > BGP**.

Configuration	/ Advanced Settings / Dynamic Routing
Dynamic	Routing (i)
OSPF BGP	Import Filters Export Filters
BGP Basic Set	tings Communities Policies Neighbors

BGP basic settings

The following 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**: The IPv4 address used for BGP advertisements. If the router ID is not specified the lowest virtual IPv4 address of the virtual interfaces participating in routing is chosen.

Note

- The router ID configuration is optional for an IPv4 network. But for an IPv6 network, the router ID configuration is mandatory. The router ID for an IPv6 network must be configured in the same IPv4 format (32-bit notation).
- You must create separate IPv4 and IPv6 peering to the same router (if applicable) for learning and advertising.
- 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.

Configuration / Advanced Setting	/ Dynamic Routing
Dynamic Routing ①	
OSPF BGP Import Filters I	xport Filters
BGP Basic Settings Communities	Policies Neighbors
Enable	
Local Autonomous System	
1	
Advertise Citrix SD-WAN Routes	
Advertise OSPF Routes	
Protocol Preference*	
100	
Router ID Settings	
Routing Domain*	Router ID *
Select a Routing Domain	✓
Save Router ID Settings	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.

OSPF	BGP In	nport Filters	Export Filters		
Com	nmunity Info	rmation			
Com	munity Name* Enter Commu	nity Name			
Com	nmunity Strir	ngs			
Manu	ual/Well Known	\checkmark	New Format(AA:NN)	ASN*	Value *
Ν	Vanual	\checkmark			
	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.

SPF	BGP	Import Filters	Export Filters
Pol	icy Inform	ation	
BGP	Policy Nam	e*	
	Enter Polio	cy Name	
_			
Rou	ıte 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.

	Export Filters			
Neighbor Information				
Routing Domain *	Virtual Interface*	Nei	ghbor IP *	
Default_RoutingDomain	~	~		
Neighbor AS *	Hold Time*	Local Preference*	Password	
1	180	100		۲
🖌 IGP Metric 🗹 Multi Hop				
IGP Metric Multi Hop Neighbor Policies	Network Address	up Community String list	BGP Community(AA-NN)	
✓ IGP Metric ✓ Multi Hop Neighbor Policies	Network Address Use IP Grou	up Community String list	BGP Community(AA:NN)	
IGP Metric Image: Multi Hop Neighbor Policies Order 100	Network Address Use IP Grou	up Community String list Manual	BGP Community(AA:NN)	
IGP Metric Image: Multi Hop Neighbor Policies Order 100 AS Path	Network Address Use IP Grou * BGP Policy *	up Community String list Manual Dir	BGP Community(AA:NN)	
IGP Metric Multi Hop Neighbor Policies Order 100 AS Path *	Network Address Use IP Grou * BGP Policy *	up Community String list Manual Dir	BGP Community(AA:NN)	~

Route filtering

For networks with Route Learning enabled, Citrix SD-WAN Orchestrator provides more control over which SD-WAN routes are advertised to routing neighbors rather and which routes are received from routing neighbors, rather than advertising and accepting all or no routes.

Import filters

Import Filters are used to accept or not accept routes which are received using OSPF and BGP neighbors based on specific match criteria. Import filter rules are the rules that must be met before importing dynamic routes into the SD-WAN route database. No routes are imported by default.

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

Click + Import Rule.

mport Filte	r Rule Attributes								
Protocol	Routing Domain	Source Router		Destination IP	Use IP Group	Pre	fix	Next Hop	Route Ta
Any 🗸	Default_RoutingDomain	*		*		eq 🗸	*	*	*
AS Path	Length Citrix SD-WAN	Cost	🗸 Export R	oute to Citrix Applian	ces	✓ Include			
Eligibility	/ Based on Gateway		Eligibilit	y Based On Path					
Service Type			Service Name			Path			
Local		\sim	Select Nam	le	\sim	Select Path			\sim
Local Internet Intranet GRE Tunne	l								

Use the following criteria to construct each Export Filter that you want to create.

Field Criteria	Description	Value
Protocol	The routing protocol using which a route is learned. Select the protocol from the drop-down list.	Any, OSPF, BGP
Routing Domain	Enter the routing domain from the drop-down list.	 Routing Domain name
Source Router	The IP address of the source router, it is applicable for iBGP only	IP address
Destination IP	The IP address and subnet mask of a route's destination	IP address
Use IP Group	Select the Use IP Group check box as needed.	• IP Group
Prefix	To match routes by prefix, choose a match predicate from the menu and enter a Route prefix in the adjacent field	 eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to

Field Criteria	Description	Value
Next Hop	The IP address of the next hop	IP address
Route Tag	The OSPF Route tag that the filter matches. OSPF route tags prevent routing loops during mutual redistributing between OSPF and other protocols	Numeric value
Cost	The route cost used to match OSPF routes for importing	Numeric value
AS Path Length	The AS path length used to match BGP routes for importing	Numeric value
Export Route to Citrix Appliances	Select the check box to enable this filter. Otherwise the filter is ignored	None
Include	Select the check box to Include routes that match this filter. Otherwise matching routes are ignored	None
Eligibility Based on Gateway	Select this check box and provide the Service Type , Service Name and Path from the drop-down list.	Service Type (Local, Internet, Intranet, GRE Tunnel, Passthrough), Service Name, and Path
Eligibility Based on Path	Select this check box and provide the Service Type , Service Name and Path from the drop-down list.	Service Type (Local, Internet, Intranet, GRE Tunnel, Passthrough), Service Name, and Path

Click **Done** to save the settings.

Export filters

Export Filters are used to include or exclude routes for advertisement using OSPF and BGP protocols based on specific match criteria. Export filter rules are the rules that must be met when advertising SD-WAN routes over dynamic routing protocols. All the routes are advertised to peers by default.

Click + Export Rule.
Citrix SD-WAN Orchestrator

Dynamic Routing (i) OSPF BGP Import Filters Export Filters Export Filter Rule Attributes Routing Domain Network Address/Mask Use IP Group Prefix Cost Service Type Service Name Gateway IP Address eq Select Name V Default_RoutingDomain eq Any Export OSPF Route Type Export OSPF Route Weight Type 5 AS External ∨ Weight Include Cancel Done

Use the following criteria to construct each Export Filter that you want to create.

Field Criteria	Description	Value
Routing Domain	Select the routing domain from the drop-down list.	Routing domain
Network Address/Mask	Enter the IP address and subnet mask of configured Network Object that describes the route's network	IP address
Use IP Group	Select the check box if needed and enter the IP group from the drop-down list.	• IP group
Prefix	To match routes by prefix, choose a match predicate from the menu and enter a Route prefix in the adjacent field	 eq: Equal to, - lt: Less than, - le: Less than or equal to, - gt: Greater than, - ge: Greater than or equal to
Cost	The method (predicate) and the SD-WAN Route Cost that are used to narrow the selection of routes exported	Numeric value
Service Type	Select the Service types that are assigned to matching routes from a list of Citrix SD-WAN Services	Any, Local, Virtual Path, Internet, Intranet, LAN GRE Tunnel, LAN IPsec Tunnel

Field Criteria	Description	Value
Site/Service Name	For Intranet, LAN GRE Tunnel, and LAN IPsec Tunnel, specify the name of the configured Service Type to use	Text string
Gateway IP Address	If you choose LAN GRE Tunnel as the Service Type, enter the gateway IP for the tunnel	IP address
Export OSPF Route Type	Advertise the Citrix SD-WAN route to OSPF neighbors as type 1 Intra-area route or type 5 External route. Default route is always advertised as type - 5 external route to normal areas and type-3 summary route to stub areas.	Route type
Export OSPF Route Weight	When export Citrix SD-WAN routes to OSPF, and the weight to each route's Citrix SD-WAN cost as total cost.	Weight
Include	Select the check box to Include routes that match this filter. Otherwise matching routes are ignored	None

Route filtering is implemented on LAN routes and Virtual Path routes in an SD-WAN network (Data Center/Branch) and is advertised to a non-SD-WAN network through using BGP and OSPF.

You can configure up to 512 Export Filters and 512 Import Filters. This is the overall limit, not per routing domain limit.

SD-WAN Overlay Routing

December 7, 2021

Citrix SD-WAN provides resilient and robust connectivity between remote sites, data centers, and cloud networks. The SD-WAN solution can accomplish this connectivity by establishing tunnels between SD-WAN appliances in the network. Establishing tunnels enables connectivity between sites

by applying route tables that overlay the existing underlay network. SD-WAN route tables can fully replace or coexist with the existing routing infrastructure.

Citrix SD-WAN appliances measure the available paths unidirectionally in terms of availability, loss, latency, jitter, and congestion characteristics. The appliances then select the best path on a per-packet basis. It means that the path chosen from Site A to Site B, need not necessarily be the path chosen from Site B to Site A. The best path at a given time is selected independently in each direction. Citrix SD-WAN offers packet-based path selection for rapid adaptation to any network changes. SD-WAN appliances can detect path outages after just two or three missing packets, allowing seamless subsecond failover of application traffic to the next-best WAN path. SD-WAN appliances recalculate every WAN link status in about 50 ms. The following article provides detailed routing configuration within the Citrix SD-WAN network.

Citrix SD-WAN Route Table

The SD-WAN configuration allows static route entries for specific sites, and route entries learned from the underlay network through supported routing protocols; such as OSPF, eBGP, and iBGP. Routes are defined by their next hop and by their service type. It determines how the route is forwarded. The following are the main service types in use:

• Local Service: Denotes any route or subnet local to the SD-WAN appliance. It includes the Virtual Interface subnets (automatically creates local routes), and any local route defined in the route table (with a local next hop). The route is advertised to other SD-WAN appliances that have a Virtual Path to this local site where this route is configured when trusted as a partner.

Note

Be cautious when adding default routes, and summary routes as local routes as it can result in virtual path routes at other sites. Always check the route tables to make sure that the correct routing is in effect.

- **Virtual Path** –Denotes any local route learned from a remote SD-WAN site that is reachable down the virtual paths. These routes are normally automatic, however a virtual path route can be added manually at a site. Any traffic for this route is forwarded to the defined Virtual Path for this destination route (subnet).
- Intranet –Denotes routes that are reachable through a private WAN link (MPLS, P2P, VPN, and so on). For example, a remote branch that is on the MPLS network but does not have an SD-WAN appliance. It is assumed that these routes must be forwarded to a certain WAN router. Intranet Service is not enabled by default. Any traffic matching this route (subnet) is classified as intranet traffic.

Note

Notice that when adding an Intranet route there is no next hop, but rather a forward to an Intranet Service. The Service is associated with a given WAN link.

• **Internet** –Similar to Intranet but is used to define traffic flowing to public Internet WAN links rather than private WAN links. One unique difference is that the Internet service can be associated with multiple WAN links and set to load balance (per flow) or be active/backup. A default Internet route gets created when internet service is enabled (it is off by default). Any traffic matching this route (subnet) is classified as Internet for this appliance for delivery to public internet resources.

Note

Internet Service routes can be advertised to the other SD-WAN appliances or prevented from being exported depending on whether you are backhauling Internet access over the Virtual Paths.

• **Passthrough** –Acts as a last resort or override service when an appliance is in-line mode. If a destination IP address fails to match with any other route, then the SD-WAN appliance simply forwards it onto the WAN link next hop. A default route: 0.0.0.0/0 cost of 16 pass-through route is created automatically. Passthrough does not work when the SD-WAN appliance is deployed out of path or in Edge/Gateway mode. Any traffic matching this route (subnet) is classified as passthrough for this appliance. It is recommended that passthrough traffic is limited as much as possible.

Note

Passthrough can be useful when conducting a POC to avoid having to configure numerous routings. Be careful in production because SD-WAN does not account for WAN link utilization for traffic sent to passthrough. It is also helpful when troubleshooting issues and you want to take a certain IP flow out of delivery over the Virtual Path.

- **Discard** Not a service but a last resort route that drops the packets if it matches. Normally, is does not occur expect when the SD-WAN appliance is deployed out of the path. You must have an Intranet service or local route as a catch all route. Otherwise, the traffic is discarded as there is no passthrough service (even though a passthrough default route is present).
 - <!--The SD-WAN Configuration Editor enables route table customization for each available site

Route table entries are populated from different inputs:

- Configured Virtual IP Address (VIP) auto-populate as Service Type Local route. The Configuration Editor prevents the same VIP assignment to different site nodes.
- Internet Services enabled at a local site auto-populate a default route (0.0.0.0/0) locally for direct internet breakout.

- Admin defined static routes on a per site basis, which are defined as a Service Type Local route.
- A default (0.0.0/0) catches all route with cost 16 defined as Passthrough

Administrators can configure one of the preceding routes. In addition to the route cost, include a service type, next hop, or gateway depending on the service type. A default route cost is automatically added to each route type (refer the following table for default route costs). Also, only trusted routes are advertised to other SD-WAN appliances. Untrusted routes are only used by the local appliance.

With WAN-to-WAN Forwarding (Routes Export Template) enabled under Global settings, the MCN site shares the advertised routes to all clients participating in the SD-WAN overlay. This feature enables IP connectivity between hosts at different client node sites, with the communication traveling through the MCN.

Each route for remote branch office subnets is advertised as a Service through the Virtual Path connecting through the MCN. The **Site** column is populated with the client node where the destination resides as a local subnet.

In the following example, **WAN-to-WAN Forwarding** (Routes Export) are enabled. Branch A has a route table entry for the Branch B subnet (10.2.2.0/24) through the MCN as a next hop.



How Citrix SD-WAN Traffic Matches on Defined Routes

The match process for defined routes on Citrix SD-WAN is based on the longest prefix match for the destination subnet (similar to a router operation). The more specific the route, the higher the change on it being matched. Sorting is done in the following order:

- 1. Longest prefix matches
- 2. Cost
- 3. Service

Therefore a /32 route always precedes a /31 route. For two /32 routes, a cost 4 route always precedes a cost 5 route. For two /32 cost 5 routes, routes are chosen based on ordered IP host. Service order is as follows: Local, Virtual Path, Intranet, Internet, Passthrough, Discard.

As an example, consider the following two routes as follows:

- 192.168.1.0/24 Cost 5
- 192.168.1.64/26 Cost 10

A packet destined for the 192.168.1.65 host would use the latter route even though the cost is higher. It is common for configuration to be in place for the routes intended to be delivered over the Virtual Path overlay with other traffic falling into catch all routes such as a default route to the passthrough service.

Routes can be configured in a site node route table that have the same prefix. The tie break then goes to the route cost, the service type (Virtual Path, Intranet, Internet, and so on), and the next hop IP.

Citrix SD-WAN Routing Packet Flow

- LAN to WAN (Virtual Path) Traffic Route Matching:
 - 1. LAN interface receives and processes the incoming traffic.
 - 2. The received frame is compared to the route table for the longest prefix match.
 - 3. If a match is found, the rule engine processes the frame and creates a flow in the flow database.
- WAN to LAN (Virtual Path) Traffic Route Matching:
 - 1. SD-WAN receives the Virtual Path traffic from the tunnel and processes it.
 - 2. The appliance compares the source IP address to see if the source is local.
 - If yes then WAN eligible and match IP destination to routing table/Virtual Path.
 - If no –then WAN to WAN forwarding enabled check.
 - 3. (WAN to WAN Forwarding disabled) Forward to LAN based on local routes.
 - 4. (WAN to WAN Forwarding enabled) Forward to Virtual Path based on route table.
- Non-Virtual Path Traffic:
 - 1. Incoming traffic is received on the LAN interface and is processed.

- 2. The received frame is compared to the route table for the longest prefix match.
- 3. If a match is found, the rule engine processes the frame and creates a flow in the flow database.

Citrix SD-WAN Routing Protocol Support

Citrix SD-WAN release 9.1 introduced OSPF and BGP routing protocols into the configuration. Introducing routing protocols to SD-WAN enabled easier integration of SD-WAN in more complex underlay networks where routing protocols are actively in use. With the same routing protocols enabled on SD-WAN, configuration of subnets denoted to use the SD-WAN overlay was made easier. In addition, the routing protocols enable communication between SD-WAN and non-SD-WAN sites with direct communication to existing customer edge routers using the common routing protocol. Citrix SD-WAN participating in routing protocols and operating in the underlay network can be done regardless of the deployment mode of SD-WAN (Inline mode, Virtual Inline mode, or Edge/Gateway mode). Also, SD-WAN can be deployed in "learn only"mode where SD-WAN can receive routes but not advertise routes back to the underlay. It is useful when you introduce the SD-WAN solution into a network in which the routing infrastructure is complex or uncertain.

Important

It is easy to leak the unwanted route, if you are not careful.

The SD-WAN Virtual Path route table works as an External Gateway Protocol (EGP), similar to BGP (think site-to-site). For example, when SD-WAN advertises routes from the SD-WAN appliance to OSPF they are typically considered external to site and protocol.

Note

Be aware of environments that have IGPs across the entire infrastructure (across the WAN). It complicates how SD-WAN advertised routes are used. EIGRP is extensively used in the market and SD-WAN does not interoperate with that protocol.

When introducing Routing Protocols to an SD-WAN deployment, the route table is not available until the SD-WAN service is enabled and operation in the network. Therefore, it is not recommended to enable advertise routes from the SD-WAN appliance initially. Use the import and export filters for a gradual introduction of routing protocols on SD-WAN.

Let us take a closer look by reviewing the following example:



In this example, we examine a routing protocol use case. The preceding network has four locations; New York, Dallas, London, and San Francisco. We deploy SD-WAN appliances at three of these locations. Also, we use SD-WAN to create a hybrid WAN network where MPLS and Internet WAN Links are used to provide a Virtualized WAN. Since Dallas does not have an SD-WAN device, we must consider how to best integrate with existing route protocols to that site. It ensures full connectivity between underlay and SD-WAN overlay networks.

In the example network, eBGP is used between all four locations across the MPLS network. Each location has its own Autonomous System Number (ASN).

In the New York Data Center, OSPF is running to advertise the core Data Center subnets to the remote sites and also announce a default route from the New York Firewall (E). In this example, all internet traffic is backhauled to the data center, even though the London and San Francisco Branches have a path to the internet.

The San Francisco site also must be noted not to have a router. SD-WAN is deployed in Edge/Gateway mode. The appliance is the default gateway for the San Francisco subnet and also participates in eBGP to the MPLS.

- With the New York Data Center, take note that the SD-WAN is deployed in Virtual Inline mode. The intent is to participate in the existing OSPF routing protocol to get traffic forwarded to the appliance as the preferred gateway.
- The London site is deployed in traditional inline mode. The upstream WAN Router (C) remains the default gateway for the London subnet.
- The San Francisco site is a newly introduced site to this network. The idea is to deploy SD-WAN in Edge/Gateway mode and have the appliance act as the default gateway for the new San Fran-

CITRIX

cisco subnet.

Review some of the existing underlay route tables before implementing SD-WAN.

New York Core Router B:

vyos@VYOS-ROUTER-B-CORE:~\$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - ISIS, B - BGP, > - selected route, * - FIB route
O>* 0.0.0.0/0 [110/10] via 172.10.10.3, eth1, 00:08:56
O>* 10.90.1.0/24 [110/20] via 172.10.10.1, eth1, 00:21:02
O>* 10.100.1.0/24 [110/20] via 172.10.10.1, eth1, 00:21:02
C>* 127.0.0.0/8 is directly connected, lo
O 172.10.10.0/24 [110/10] is directly connected, eth1, 1d20h00m
C>* 172.10.10.0/24 is directly connected, eth1
C>* 172.20.20.0/24 is directly connected, eth2
C>* 172.30.30.0/24 is directly connected, eth3
C>* 192.168.65.0/24 is directly connected, eth0

The local New York subnets (172.x.x.x) are available on router B as directly connected. From the route table we identify that the default route is 172.10.10.3 (Firewall E). Also, we can see that the Dallas (10.90.1.0/24) and London (10.100.1.0/24) subnets are available through 172.10.10.1 (MPLS Router A). The route costs indicate that they were learned from eBGP.

Note

In the example provided, San Francisco is not listed as a route. It is because we have not yet deployed the site with SD-WAN in Edge/Gateway mode for that network.

vyos@VYATTA-ROUTER-A:~\$ show ip route
Codes: K - kernel route. C - connected. S - static. R - RIP. O - OSPF.
LISIC B BCD > colocted route * EIP route
I - 1515, D - DGP, > - Selected Toule, - FID Toule
O>* 0.0.0.0/0 [110/10] via 172.10.10.3. eth1. 00:09:52
P > 10.00, 1.0/24 [20/4] via 102.169.10.2 oth2.1d22b00m
D 10.90.1.0/24 [20/1] via 192.100.10.2, eu12, 102310911
B>* 10.100.1.0/24 [20/1] via 192.168.10.3, eth2, 1d23h10m
C>* 127.0.0.0/8 is directly connected, lo
O 172.10.10.0/24 [110/10] is directly connected, eth1, 1d20h01m
C>* 172.10.10.0/24 is directly connected, eth1
O>* 172.20.20.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
O>* 172.30.30.0/24 [110/20] via 172.10.10.2, eth1, 00:21:58
C>* 192.168.10.0/24 is directly connected, eth2
O 192.168.65.0/24 [110/20] via 172.10.10.2, 1d19h57m
C>* 192 168 65 0/24 is directly connected eth0

For the New York WAN Router (A), OSPF learned routes and routes learned across the MPLS through eBGP are listed routes. Note the route costs. BGP is lower administrative domain and cost by default

20/1 compared to OSPF 110/10.

Dallas Router D:

For the Dallas WAN Router (D) all routes are learned across the MPLS.

vyos@VYATTA-ROUTER-D:~\$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - ISIS, B - BGP, > - selected route, * - FIB route
B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:10:17
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 1d23h10m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 1d23h10m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:22:17
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0

Note

In this example, you can ignore the 192.168.65.0/24 subnet. This is a management network and not pertinent to the example. All the Routers are connected to the management subnet but is not advertised in any routing protocol.

After the Citrix SD-WAN appliances have been deployed, we can take a refreshed look at the route tables for the BGP router at the Dallas site. We see 10.80.1.0/24 and 10.81.1.0/24 subnets are being seen correctly through eBGP from the San Francisco SD-WAN.

Dallas Router D:

vyos@VYATTA-ROUTER-D:~\$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF,
I - ISIS, B - BGP, > - selected route, * - FIB route
B>* 0.0.0.0/0 [20/10] via 192.168.10.1, eth2, 00:00:01
B>* 10.80.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.81.1.0/24 [20/0] via 192.168.10.4, eth2, 3d19h07m
B>* 10.90.1.0/24 [20/1] via 192.168.10.2, eth2, 4d23h38m
C>* 10.100.1.0/24 is directly connected, eth1
C>* 127.0.0.0/8 is directly connected, lo
B>* 172.10.10.0/24 [20/1] via 192.168.10.1, eth2, 4d23h38m
B>* 172.20.20.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B>* 172.30.30.0/24 [20/20] via 192.168.10.1, eth2, 00:00:01
B 192.168.10.0/24 [20/0] via 192.168.10.4 inactive, 3d19h07m
C>* 192.168.10.0/24 is directly connected, eth2
C>* 192.168.65.0/24 is directly connected, eth0

Citrix SD-WAN shows all the routes learned, including routes available through the Virtual Path overlay. Let us consider 172.10.10.0/24, which is in the New York Data Center. This route is being learned in two ways:

- As a Virtual Path route (Number 3), service = NYC-SFO with a cost of 5 and type static. It is a local subnet advertised by SD-WAN appliance in New York. It is static in that it is either directly connected to the appliance or it is a manual static route entered in the configuration. It is reachable because the Virtual Path between the sites is in a working/up state.
- As an advertised route through BGP (Number 6), with a cost of 6. This is now considered a fallback route.

The prefix is equal and the cost is different. SD-WAN uses the Virtual Path route unless it becomes unavailable in which case the fallback route is learned through BGP.

Now, let us consider the route 172.20.20.0/24.

- This is learned as a Virtual Path route (Number 9) but has a type of dynamic and a cost of 6. This means that the remote SD-WAN appliance learned this route through a routing protocol, in this case OSPF. By default the route cost is higher.
- SD-WAN also learns this route through BGP with the same cost, so this route might be preferred over the Virtual Path route.

We also see a passthrough and discard route with cost 16. These routes are automatic and cannot be removed. If the device is inline, the passthrough route is used as a last resort. So, if a packet cannot be matched to a more specific route, SD-WAN passes it along to the next hop of the interface group. If the SD-WAN is out of path or in edge/gateway mode, there is no passthrough service, in which case SD-WAN drops the packet using the default discard route. The Hit Count indicates the number of packets that are hitting each route, which can be valuable when troubleshooting.

For the New York site, we want traffic destined to remote sites (London and San Francisco) to be directed to the SD-WAN appliance when the Virtual Path is active.

There are multiple subnets available in the New York site:

- 172.10.10.0/24 (directly connected)
- 172.20.20.0/24 (advertised via OSPF from the core router B)
- 172.30.30.0/24 (advertised via OSPF from the core router B)

We also are required to provide traffic flow to Dallas (10.100.1.0/24) through MPLS.

Dynamic Virtual Paths

Dynamic Virtual Paths can be allowed between two client nodes to build on-demand virtual paths for direct communication between the two sites. The advantage of a dynamic virtual path is that

traffic can flow directly from one client node to the second without having to traverse the MCN or two virtual paths, which can add latency to the traffic flow. Dynamic virtual paths are built and removed dynamically based on user-defined traffic thresholds. These thresholds are defined as either packets per second (pps) or bandwidth (kbps). This functionality enables a dynamic full mesh SD-WAN overlay topology.

Once the thresholds for dynamic virtual paths are met, the client nodes dynamically create their virtualized path to one another using all available WAN paths between the sites and make full use of it in the following manner:

- Send Bulk data if any exists and verify no loss, then
- Send Interactive data and verify no loss, then
- Send Real Time data after the Bulk and Interactive data are considered stable (no loss or acceptable levels)
- If there is no Bulk or interactive data send Real Time Data after the Dynamic Virtual Path has been stable for a period
- If the user data falls below the configured thresholds for a user defined period, the dynamic virtual path is torn down

Dynamic Virtual Paths have the concept of an Intermediate site. The intermediate site can be an MCN site or any other site in the network. The site must have Static Virtual Path configured and connected to two or more other client nodes. Another design consideration requirement is to have WAN-to-WAN Forwarding enabled. It would allow all routes from all sites to be advertised to the client nodes where the dynamic virtual path is desired.

Multiple WAN-to-WAN Forwarding Groups can are allowed in the SD-WAN configuration. It enables full control to path establishment between certain client nodes and not others.





WAN to WAN Forwarding Group:

- A network can have multiple WAN to WAN Forwarding Groups
- Direct dynamic path will have a lower cost then through the intermediate node

51 © 2017 Citrix

CITRIX

Each SD-WAN device has its own unique route table with the following details defined for each route:

- Num –Order of route of the appliance based on match process (lowest Num processed first)
- Network address Subnet or host address
- Gateway if necessary
- Service –Service that is applied for the route
- Firewall Zone The firewall zone classification of the route
- Reachable Identifies if the Virtual Path state is active for the site
- Site –The name of the site where the route is expected to exist
- Type –Identification of route type (Static or Dynamic)
- Neighbor Direct
- Cost Cost of the specific route
- Hit Count –Number of times the route has been used per packet. This information would be used to verify that a route is being hit correctly.
- Eligible
- Eligibility Type
- Eligibility Value

Intranet and Internet Routes

For the Intranet and Internet service types, the user must have defined an SD-WAN WAN Link to support those types of services. It is a pre-requisite for any defined routes for either of these services. If the WAN link is not defined to support the Intranet Service, it is considered as a local route. The Intranet, Internet, and Passthrough routes are only relevant to the site/appliance they are configured for.

When defining Intranet, Internet or Passthrough routes the following are design considerations:

- Must have service defined on the WAN link (Intranet/Internet required)
- Intranet/Internet must have gateway defined for the WAN link
- Relevant to local SD-WAN device
- Intranet routes can be learned via the Virtual Path but are done so at a higher cost
- With Internet Service, there is automatically a default route created (0.0.0.0/0) catch all route with a max cost
- Do no assume that Passthrough works, it must be tested/verified, also test with Virtual Path down/disabled to verify desired behavior
- Route tables are static unless the route learning feature is enabled

The maximum supported limit for multiple routing parameters is as follows:

- Maximum Routing Domains: 255
- Maximum Access Interfaces per WAN Link: 64
- Maximum BGP neighbors per site: 255
- Maximum OSPF area per site: 255
- Maximum Virtual Interfaces per OSPF area: 255
- Maximum Route Learning import filters per site: 512
- Maximum Route Learning export filters per site: 512
- Maximum BGP routing policies: 255
- Maximum BGP community string objects: 255

Network address translation

May 3, 2022

Network Address Translation (NAT) on the SD-WAN appliance performs IP address conservation to preserve the limited number of registered IP addresses. It translates the private addresses in the internal network into a legal public address and connects your private SD-WAN network with the public internet. The public IP address is used for communication over the internet. NAT also ensures extra security by advertising only one address for the entire network to the internet, hiding the entire internal network.

You can configure the following types of NAT:

- Dynamic source NAT
- Static NAT
- Destination NAT

Note

The NAT capability can only be configured at the site level. There is no global configuration (templates) for NAT.

To configure NAT for a site using the Citrix SD-WAN Orchestrator service, from site level, navigate to **Configuration > Advanced Settings > NAT**.

NAT (i)					
Dynamic Sou	Irce NAT Static Source N	IAT Destination NAT				
+ Dyna	mic Source NAT					
• Top of L	ist 🔿 Bottom of List 🔿	Specify Row Number	Row number			
No	Туре	Name	Inside Zone	Routing Domain	Inside IP	Actions

Inbound and Outbound NAT

The direction for a connection can either be inside to outside or outside to inside. When a NAT rule is created, you can define the direction using the **On Receive** check box. When the check box is selected, the direction is configured as **Inbound** and when the check box is cleared, the direction is configured as **Outbound**.

- **Inbound**: The source address is translated for packets received on the service. The destination address is translated for packets transmitted on the service. For example, Internet service to LAN service –For packets received (Internet to LAN), the source IP address is translated. For packets transmitted (LAN to Internet), the destination IP address is translated.
- **Outbound**: The destination address is translated for packets received on the service. The source address is translated for packets transmitted on the service. For example, LAN service to

Internet service –for packets transmitted (LAN to Internet) the source IP address is translated. For packets received (Internet to LAN) the destination IP address is translated.

Zone Derivation

The source and destination firewall zones for the inbound or outbound traffic must not be the same. If both the source and destination firewall zones are the same, NAT is not performed on the traffic.

For outbound NAT, the outside zone is automatically derived from the service. Every service on SD-WAN is associated to a zone by default. For example, Internet service on a trusted internet link is associated with the trusted internet zone. Similarly, for an inbound NAT, the inside zone is derived from the service.

For a Virtual path service NAT zone derivation does not happen automatically, you have to manually enter the inside and outside zone. NAT is performed on traffic belonging to these zones only. Zones cannot be derived for virtual paths because there might be multiple zones within the Virtual path subnets.

Dynamic source NAT

Dynamic Source NAT is a many-to-one mapping of a private IP address or subnets inside the SD-WAN network to a public IP address or subnet outside the SD-WAN network. It 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. The traffic from different zones and subnets over trusted (inside) IP addresses in the LAN segment is sent over a single public (outside) IP address.

Note

Dynamic NAT translations allow all reciprocal traffic for a session initiated from the Inside Network. To filter these connections, add filter Policies for the outbound traffic.

Port Address Translation

Dynamic NAT does Port Address Translation (PAT) along with IP address translation. Port numbers are used to distinguish which traffic belongs to which IP address. A single public IP address is used for all internal private IP addresses, but a different port number is assigned to each private IP address. PAT is a cost effective way to allow multiple hosts to connect to the Internet using a single Public IP address.

The **Symmetric** check box defines the PAT configuration. While configuring NAT rules, if the check box is selected, Symmetric NAT is configured and when cleared, Port Restricted NAT gets configured in the back-end.

- **Port Restricted**: Port Restricted NAT uses the same outside port for all translations related to an Inside IP Address and Port pair. This mode is typically used to allow Internet P2P applications.
- **Symmetric**: Symmetric NAT uses the same outside port for all translations related to an Inside IP Address, Inside Port, Outside IP Address, and Outside Port tuple. This mode is typically used to enhance security or expand the maximum number of NAT sessions.

Port Forwarding

Dynamic NAT with port forwarding allows traffic from an Outside network to access specific hosts and ports on the Inside network without the session being initiated from the inside. This is typically used for inside hosts like web servers.

Once the dynamic NAT is configured you can define the port forwarding policies. Configure dynamic NAT for IP address translation and define the port forwarding policy to map an outside port to an inside port. Dynamic NAT port forwarding is typically used to allow remote hosts to connect to a host or server on your private network.

Configure Dynamic Source NAT

To configure dynamic NAT for a site using the Citrix SD-WAN Orchestrator service, from site level, navigate to **Configuration > Advanced Settings > NAT > Dynamic Source NAT** tab. Click **+ Dynamic Source NAT**.

- **Type**: The SD-WAN service types on which the NAT policy is applied. For static NAT, the service types supported are Local, Virtual Paths, Internet, Intranet, and Inter-routing domain services.
- **Routing Domain**: Select the routing domain for which the selected translation applies to.
- IP Address Type: Select the IPv4 or IPv6 address type based on your preference.
- **Destination Service**: Provide a name for the service that corresponds to the Service Type.
- **Inside Zone**: The Inside firewall zone match-type that the packet must be from to allow translation.
- **Inside IP/Prefix**: The inside IP address and prefix that has to be translated to if the match criteria is met.
- **Outside IP**: The outside IP address and prefix that the inside IP address is translated to if the match criteria is met. For outbound traffic using Internet and Intranet services, the configured WAN link IP address is dynamically chosen as the outside IP address.
- **Port Parity**: If enabled, outside ports for NAT connections maintain parity (even if inside port is even, odd if outside port is odd).

- **Bind Responder Route**: Ensures that the response traffic is sent over the same service that it is received on, to avoid asymmetric routing.
- **Allow Related**: Allow traffic related to the flow matching the rule. For example, ICMP redirection related to the specific flow that matched the policy, if there was some type of error related to the flow.
- IPSec Passthrough: Allow an IPsec (AH/ESP) session to be translated.
- **GRE/PPTP Passthrough**: Ensures that the response traffic is sent over the same service that it is received on, to avoid asymmetric routing.
- **On Receive**: When this check box is selected, inbound NAT is configured. When cleared, outbound NAT is configured.
- **Symmetric**: When this check box is selected, Symmetric NAT is configured. When cleared, port restricted NAT is configured.

Port Forwarding Rules:

- Routing Domain: Select the routing domain for which the selected translation applies to.
- **Protocol**: TCP, UDP, or both.
- **Outside Port**: The Outside port that is port forward into the inside port.
- Inside IP: The inside address to forward matching packets.
- Inside Port: The Inside port that the outside port will be port forwarded into.

Every port forwarding rule has a parent NAT rule. The outside IP address is taken from the parent NAT rule.

Note

The Citrix SD-WAN Orchestrator service UI displays auto-created NAT rules when the following conditions are fulfilled:

- Internet service is enabled on the site.
- IPv4 outbound Internet dynamic source NAT rule is not configured at the site.
- At least 1 WAN link is on an untrusted interface or Internet is enabled on all routing domains.

NAT (i)

100	Routing Domain	ІР Туре	
Internet	Default_RoutingDomain	ipv4 ~	
estination Service *	Inside Zone	Inside IP/Prefix	Outside IP
Internet	Default_LAN_Zone	Any	
Port Bind Respo Parity Route	onder Allow IPS Related Pas	ec GRE/PPTP sthrough Passthrough	On Symmetri Recieve
Port Forwarding Rules			
Port Forwarding Rules	Protocol Outside	Port Inside IP*	Inside Port

Static source NAT

Static NAT is a one-to-one mapping of a private IP address or subnet inside the SD-WAN network to a public IP address or subnet outside the SD-WAN network. Configure Static NAT by manually entering the inside IP address and the outside IP address to which it has to translate. You can configure Static NAT for the Local, Virtual Paths, Internet, Intranet, and Inter-routing domain services.

Configure Static source NAT

To configure static NAT for a site using the Citrix SD-WAN Orchestrator service, from site level, navigate to **Configuration > Advanced Settings > NAT > Static Source NAT** tab. Click **+ Static Source NAT**.

- **Type**: The SD-WAN service types on which the NAT policy is applied. For static NAT, the service types supported are Local, Virtual Paths, Internet, Intranet, and Inter-routing domain services
- **Destination Service**: Provide a name for the service that corresponds to the Service Type.
- **Inside Zone**: The Inside firewall zone match-type that the packet must be from to allow translation.
- **Outside Zone**: The outside firewall zone match-type that the packet must be from to allow translation.
- IP Address Type: Select the IPv4 or IPv6 address type based on your preference.

- Routing Domain: Select the routing domain for which the selected translation applies to.
- **Inside IP/Prefix**: The inside IP address and prefix that has to be translated to if the match criteria is met.
- **Outside IP/Prefix**: The outside IP address and prefix that the inside IP address is translated to if the match criteria is met.
- **Bind Responder Route**: Ensures that the response traffic is sent over the same service that it is received on, to avoid asymmetric routing.
- **Proxy ARP**: Ensures that the appliance responds to local ARP requests for the outside IP address.
- **Proxy NDP**: Ensures that the appliance responds to local NDP requests for the outside IP address.
- **On Receive**: When this check box is selected, inbound NAT is configured. When cleared, outbound NAT is configured.
- Auto Learn via PD: This check box gets enabled only when you select IPv6 as the IP Address Type. When selected, Citrix SD-WAN requests a prefix from the upstream delegating router and the delegating router responds with a prefix to Citrix SD-WAN.

NAT (i)

nternet	Default_LAN_Zone 🗸	Default LAN Zone
e IP/Prefix *	Outside IP/Prefix	WAN Link
e	IP/Prefix*	IP/Prefix* Outside IP/Prefix

Static NAT Policies for IPv6 Internet service

Citrix SD-WAN supports static NAT policies for the IPv6 Internet service from release 11.4.0 onwards. A static NAT policy for the IPv6 Internet service specifies the mapping of an inside network prefix to an outside network prefix. The number of static NAT policies required depends on the number of inside networks and the number of outside networks (WAN links). If there are **M** number of inside networks and **N** number of WAN links, then the number of static NAT policies required is **M x N**.

From Citrix SD-WAN release 11.4.0 onwards, while creating a static NAT policy, you can either enter the outside IP address manually or enable **Auto Learn via PD**. When **Auto Learn via PD** is enabled, the SD-WAN appliance receives delegated prefixes from the upstream delegating router through DHCPv6

Prefix Delegation. Before Citrix SD-WAN release 11.4.0, the outside IP address was derived from the service automatically and there was no option to enter the outside IP address manually. If you are upgrading an appliance to 11.4.0 or a later release and have static NAT policies configured for IPv6 Internet service, then you must manually update the policies.

Configuration example

In the following topology, the Citrix SD-WAN appliance is configured with 2 inside networks and 2 WAN links:

- Inside network 1 resides in the CORPORATE routing domain with network prefix FD01:0203:6561::/64
- Inside network 2 resides in the Wi-Fi routing domain with network prefix FD01:0203:1265::/64
- Through WAN Link 1, the SD-WAN appliance receives from the upstream delegating router through DHCPv6 Prefix Delegation, 2 delegated prefixes 2001:0D88:1265::/64. These 2 delegated prefixes are used as the outside network prefixes when the traffic from the inside networks transits WAN link 1.
- Through WAN Link 2, the SD-WAN appliance receives from the upstream delegating router through DHCPv6 Prefix Delegation, 2 delegated prefixes 2001:DB8:8585::/64 and 2001:DB8:8599::/64. These 2 delegated prefixes are used as the outside network prefixes when the traffic from the inside networks transits WAN link 2.



In this scenario, there are M=2 inside networks and N=2 WAN links. Therefore, the number of static NAT policies required for proper deployment of the IPv6 Internet service is 2 x 2 = 4. These 4 static NAT policies specify the address translation for:

- Inside network 1 through WAN link 1
- Inside network 1 through WAN link 2
- Inside network 2 through WAN link 1
- Inside network 2 through WAN link 2

To configure these static NAT policies, from site level, navigate to **Configuration > Advanced Settings > NAT > Static Source NAT**. Click **+Static Source NAT**.

While creating NAT policies, ensure that you select the **Type** as **Internet** and **IP Address Type** as **IPv6**. Select the WAN link and in the **Inside IP/Prefix** field, enter the inside network prefix (only /64 prefixes are allowed). In the **Outside IP/Prefix** field, you can either manually enter the outside network prefix or select the **Auto Learn via PD** check box.

The following is an example where the outside IP address is entered manually in the static NAT policy.

NAT 🛈

Static Source NAT			
Туре	Destination Service *	Inside Zone	Outside Zone
Internet \lor	Internet	Default_LAN_Zone \lor	Default_LAN_Zone
IP Address Type OIPv4 IPv	/6		
Routing Domain	Inside IP/Prefix*	Outside IP/Prefix*	WAN Link
Default_RoutingDomain \lor	FD01:0203:6561::/64	2001:0D88:1265::/64	0365t1-WL-1 🗸
Bind Responder Route	Proxy NDP On Recieve	Auto Learn via PD	•
Cancel Save	I		

If you select the **Auto Learn via PD** check box, ensure that the upstream router supports DHCPv6 Prefix Delegation. Citrix SD-WAN requests a prefix from the upstream delegating router and the delegating router responds with a prefix to Citrix SD-WAN. Citrix SD-WAN uses this delegated prefix to translate the inside IP address to the outside IP address.

The following is an example where **Auto Learn via PD** is enabled, so that the outside network prefix is obtained through DHCPv6 Prefix Delegation.

NAT 🛈

Static Source NAT			
Туре	Destination Service *	Inside Zone	Outside Zone
Internet ~	Internet	Default_LAN_Zone \lor	Default_LAN_Zone
IP Address Type OIPv4 IPv4	/6		
Routing Domain	Inside IP/Prefix *	Outside IP/Prefix	WAN Link
Default_RoutingDomain 🗸	FD01:0203:6561::/64		0365t1-WL-2 🗸
Bind Responder Route	Proxy NDP 🔄 On Recieve 🗸	Auto Learn via PD	
Cancel Save			

Destination NAT

Destination NAT Policies allow for the configuration of Network Address Translation policies between individual hosts or subnets.

Note

- While both Inbound and Outbound translations can be configured simultaneously for a Service, only the first to match will be used. Multiple translations can occur if a rule exists on the Service a packet is received on and the Service a packet is sent on.
- Destination NAT translations are applicable only for traffic originating from Local Service.

To configure these destination NAT policies, from site level, navigate to **Configuration > Advanced Settings > NAT > Destination NAT**. Click **+ Destination NAT**.

- **Type**: The SD-WAN service types on which the NAT policy is applied. For static NAT, the service types supported are Local, Virtual Paths, Internet, Intranet, and Inter-routing domain services
- Service Name: Provide a name for the service that corresponds to the Service Type.
- IP Type: Select the IPv4 or IPv6 address type based on your preference.
- **Inside Port**: The Inside port that the outside port will be port forwarded into.
- **Outside IP**: The outside IP address and prefix that the inside IP address is translated to if the match criteria is met. For outbound traffic using Internet and Intranet services, the configured WAN link IP address is dynamically chosen as the outside IP address.
- **Outside Port**: The Outside port that is port forward into the inside port.
- Routing Domain: Select the routing domain for which the selected translation applies to.
- **On Receive**: When this check box is selected, inbound NAT is configured. When cleared, outbound NAT is configured.

NAT (i)

Destination NA	AT			
Туре	Service Name *	IP Type		
Internet $ \smallsetminus $	Internet	ipv4	\sim	
Inside IP/ Prefix *	Inside Port	Outside IP*	Outside Port	Routing Domain
				Default_RoutingDomain \smallsetminus
Cancel	Save			

Dynamic host configuration protocol

November 22, 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 ⁽ⁱ⁾							
Server Subnets	Relays	DHCP Options Set (Global)					
+ Server Sub	net						
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 🛈

rtual Interface		IP Subnet			Domain Name		
VIF-5-LAN-2 ~		10.146.110.1/23		uk.bgroup.bz			
imary DNS		Secondary DNS					
172.27.0.3		172.27.0.4			Z 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							
xed IP Address *			MAC Address *				
10.146.110.21			58:e6:ba:2b	:30:b1			
HCP Options Set + DHCP Options Set							

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 is 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 (i)						
Server Subnets	Relays	DHCP Options Set (Global)				
+ DHCP Rel	lay					
Virtual Interface				IP Address		
Virtual Interfa	се		\sim	Server IP	Ē	
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 (i)

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.

Bridi				
Server Subnets Relays D	HCP Options Set (Global)			
Set Name *				
IP Address Type V4 V6 + DHCP Options				
DHCP Option Name	Option Number	Data Type	DHCP Option Value	Actions
Cancel Save				

WAN link IP address learning through DHCP client

Citrix SD-WAN appliances support WAN Link IP address learning through DHCP Clients. This functionality reduces the amount of manual configuration required to deploy SD-WAN appliances and reduces ISP costs by eliminating the need to purchase static IP addresses. SD-WAN appliances can obtain dynamic IP addresses for WAN Links on untrusted interfaces. This eliminates the need for an intermediary WAN router to perform this function.

Notes

- DHCP Client can only be configured for untrusted non-bridged interfaces configured as Client Nodes.
- DHCP client and data port can be enabled on MCN/RCN only if Public IP address is configured.
- One-Arm or Policy Based Routing (PBR) deployment is not supported on the site with DHCP Client configuration.
- DHCP events are logged from the client's perspective only and no DHCP server logs are generated.

For information about configuring DHCP for an untrusted virtual interface on fail-to-block mode and fail-to-wire mode, see Site level configuration.

Multicast routing

July 15, 2022

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.

Multicast configuration

To configure multicast, perform the following on the SD-WAN Orchestrator service 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/MLD proxy to carry the IGMP control channel information for multicast routing.
- 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.

Note:

Once the Branch or MCN is configured as upstream, it needs to be configured as upstream for the other groups as well.

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 (IPv4 or IPv6) 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.

Note:

- When a multicast source is configured as an Intranet service, the source IP of the multicast stream must have a route mapped to the Intranet service.
- Ensure to create appropriate firewall policies to allow multicast traffic on the SD-WAN appliance.

Multicast Groups ③

Multicast Groups ③

Multicast Group				
Group Name * Grp2	Group IP* 232.1.1	Routing Domain * Default_RoutingDomain	✓ Enable IGMP Proxy	
Service				
+ Service				
Service Type	Service Instance	Direction	Upstream	Actions
Local	VIF-1-LAN-1	Send	No	<u>ت</u>
Virtual Path	orch_mcn	Receive	Yes	Ē
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.

roup Name * iDC1_Grp	Group IP* 232.1.1.1	Routing Domain* Default_Routi	ngDomain 🗸 🗸 Enab	le IGMP Proxy
Service				
+ Service				
Service Type	Service Instance	Direction	Upstream	Actions
Local	VIF-2-WAN-1	Receive	Yes	Ē
Virtual Path	orch mc	Send	No	Ī

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

Citrix SD-WAN Orchestrator

list of source senders the SD-WAN appliance will not have any reporting data.

Site I	ite Reports:Real Time Flows																
Maximum number of flows to display \vee Retrieve latest data Search Q						Q											
🗸 Upl	V Upload V Download											Columns					
Info	No	Application	Direction	Throughput (Kbps)	Routing Domain	Source IP Addr	Dest IP Addr	Source Port	Dest Port	Proto IP	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
											Showinį	Showir	ng 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.

Maximum number	of Connections to dis	play	~	Retrieve latest data	Search	Q			Customize) Columns
				Source		Destina	ation			Sent
Application	Family	Routing Domain	IP Addr	Service Type	IP Addr	Service Type	State	Is NAT	Bytes	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

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.

🗭 dashboai	RD	Site Report : Real Ti	me Statistics				
REPORTS	~	ARP Routes Virt	ual Path Services Classes	Ethernet Observed Protocols	Wan Path Application QOS	Multicast Group 🗠	
Alerts Usage		Retrieve latest data Multicast Group Destinati	ion Services				
Quality		Multicast Group	Service Type	Service Name	Packets	Kbps	
QoS		ATGDC1_Grp	IPHOST		1071	1068.503	
Historical St	tatistics						
Real Time	\sim						
Statistic	CS	Multicast Group Source S Multicast Group	ervices Service Type	Service Name	Packets	Kbps	
Flows		ATGDC1 Grp	VPath	Ombud1	1071	1068.503	
Firewall	Connections						
Cloud Direc	t						
O365 Metri	cs	Multicast Group Statistics	Packets Received	Kbps Received	Packets Sent	Kbps Sent	
Appliance R	Reports (preview)	ATGDC1_Grp	1071	1068.503	1071	1068.503	
A CONFICUR							

IGMP/MLD

When the multicast receivers initiate a join group request, you can see the receiver details under **Reports** > **Real Time** > **IGMP/MLD** > **IGMP/MLD Stats**. You can see this information at both the source and the destination. Click **Refresh** to get the current data.

The following image shows that the IGMP/MLD packets received and the filter type RECV is used to include IGMP/MLD receive packets.

IGMP/MLD

		IGMP/MLD	Proxy Group	IGMP/MLD Stat	tistics			
[R	efresh	Purge I	GMP/MLD Proxy Gr	oup		Purge IGMP/MLD Statistics]
9	Туре	e:RECV $ imes$ Click here t	o search or you can ente	er Key : Value format				× :
		TYPE		DESCRIPTION	VALUE	-	+	
>		RECV		Receive IGMP packets	613			
>		RECV		Receive V2 Leave	307			
>		RECV		Receive V3 General Query Upstream	306			

To view the details of IGMP proxy groups, navigate to **Reports** > **Real Time** > **IGMP/MLD** > **IGMP/MLD Proxy Groups**. Click **Refresh** to get the current data.

Select **Purge IGMP/MLD Stats** to purge IGMP statistical data from the IGMP stats table.

Select **Purge IGMP/MLD Group** to purge IGMP group data from the IGMP groups table.

Virtual router redundancy protocol

July 27, 2022

Virtual Router Redundancy Protocol (VRRP) is a widely used protocol that provides device redundancy to eliminate the single point of failure inherent in 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.

A back-up router automatically takes over if the primary / main router fails. In a VRRP set-up, the main router sends a VRRP packet known as an advertisement to the back-up routers. When the main router stops sending the advertisement, the back-up router sets the interval timer. If no advertisement is received within this hold period, the back-up router starts the failover routine.

VRRP specifies an election process in which, the router with the highest priority becomes the main router. If the priority is the same among the routers, the router with the highest IP address becomes

the main router. The other routers are in backup state. The election process is initiated again if the main router fails, a new router joins the group, or an existing router leaves the group.

VRRP ensures a high availability default path without configuring dynamic routing or router discovery protocols on every end-host.

Citrix SD-WAN release version 10.1 supports VRRP version 2 and version 3 to inter-operate with any third party routers. Citrix SD-WAN release version 11.5 supports version 6. The SD-WAN appliance acts as the main router and direct the traffic to use the Virtual Path Service between sites. You can configure the SD-WAN appliance as the VRRP main router 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 option.

The below network diagram shows a Citrix SD-WAN appliance and a router configured as a VRRP group. The SD-WAN appliance is configured to be the main router. If the SD-WAN appliance fails, the back-up router takes-over within milliseconds, ensuring that there is no downtime.



Data Center

To configure VRRP, in the Site configuration page, navigate to **Configuration** > **Advanced Settings** > **VRRP** > click + **Add VRRP**.

VRRP (i)

VRRP Settings			
VRRP Group ID *	Version V3 ~	Priority*	Advertisement Interval *
Authentication Type	Authentication Text	Reclaim	Use V2 Checksum
Virtual Router IPs			
Virtual Interface *	Virtual IP Address *		VRRP Router IP *
VIF-1-One-Arm-1	✓ 1.1.1.1/1		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 main router.

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 main router. 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. If IPv6 is used, then the virtual interface will have NDP RA enabled by default. 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. You can specify either the IPv4 or IPv6 address.
- 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. The VRRP Virtual Router IP should be a link-local IPv6 address.

Limitations

- VRRP is supported in Gateway Mode deployment only.
- You can configure up to four VRRP IDs (VRID).
- Up to 16 virtual network interfaces can participate in VRID.

High Availability and VRRP

You can significantly reduce network downtime and traffic disruption by applying both the high availability and VRRP features on your SD-WAN network. Deploy a pair of Citrix SD-WAN appliance in active/standby roles along with a standby router to form the VRRP group. This group appears as a single default gateway with one virtual IP address and one virtual MAC address.



The following are 2 cases with the High Availability and VRRP deployment:

1st case: High availability failover timer on SD-WAN equals the VRRP failover timer.

The expected behavior is high availability switchover to happen before the VRRP switchover, that is the traffic continues to flow through the new Active SD-WAN appliance. In this case SD-WAN continues with the VRRP Master role.
2nd case: High availability failover timer on SD-WAN greater than the VRRP failover timer.

The expected behavior is the VRRP switchover to the router happens, that is the router becomes VRRP Master and traffic might momentarily flow through the router, bypassing the SD-WAN appliance.

But once the high availability switchover happens, SD-WAN again becomes VRRP Master, that is the traffic now flows through the new active SD-WAN appliance.

For more information on high availability deployment modes, see High Availability.

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 Set-tings > DNS Settings**.

DNS (i)			
Site Specific	DNS Services DNS Proxies DNS Transport	rent 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 Service Name *	Ty	vpe	
Eg: dns_service1		Static	\sim
Service Type	S	ervice Instance	
	~		\sim
Primary DNS*	S	econdary DNS	
Eg: a.b.c.d		Eg: a.b.c.d	

DNS (i)

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 requests based on application domain names.

DNS (i)	
DNS Proxy	
DNS Proxy Name*	
DNS-proxy-1	
Interfaces to intercept DNS requests	
Virtual Interface	
VIF-1-LAN-1	
VIF-2-WAN-1	
VIF-3-WAN-2	
VIF-4-LAN-2	
IPv4 Default DNS Service	
IPv6 Default DNS Service	
~	
App Specific DNS Forwarding Rule	
Application * IPv4 DNS Service * IPv6 DNS Service	
	\sim
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 (i)

DNS Transparent Fo	rwarder		
Application *			
	\sim		
IPv4 DNS Service *	IPv6 DNS Service		
	×	\sim	
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.

Virtual Path Route Cost

November 10, 2021

Citrix SD-WAN supports the following routing enhancements related to data center administration.

For example, consider the SD-WAN network with two data centers; one in North America and one in Europe. You want all sites in North America to route traffic through the data center in North America and all sites in Europe to use the Europe data center. Previously, in SD-WAN 9.3 and earlier release versions, this functionality of data center administration was not supported. This is implemented with the introduction of Virtual Path Route cost.

• Virtual Path Route cost: You can configure the Virtual Path route cost for individual virtual paths that are added to the route cost when a route is learned from a remote site.

This feature invalidates or deletes the WAN to WAN forwarding Cost.

- OSPF Route Cost: You can now import OSPF route cost (type1 metric) by enabling Copy OSPF Route Cost in the import filters. OSPF Route cost is considered in route selection instead of SD-WAN cost. Cost up to 65534 instead of 15 is supported, but it is advisable to accommodate for an appropriate virtual path route cost that is added if the route is learned from a remote site.
- BGP VP cost to MED: You can now copy the Virtual Path route cost for SD-WAN routes into BGP MED values when exporting (redistributing) SD-WAN routes to BGP peers. This can be set for individual neighbors by creating a BGP policy and applying it in the "OUT" direction for each neighbor.
- Any site can have multiple virtual paths to other sites. Sometimes, if there is a Branch to which there is connectivity to services through more virtual paths, there can be two virtual paths from the Branch site. One virtual path through DC1 and the other through DC2. DC1 can be an MCN and DC2 can be a Geo-MCN, and can be configured as another site with Static Virtual Path.
- Add a default cost for each VP as 1. Virtual Path Route cost helps associate a cost to each virtual path of a site. This helps to manipulate route exchanges/updates over a specific virtual path instead of default site cost. With this, we can manipulate which data center to be preferred for sending out the traffic.
- Allow cost to be configured within a small range of values (for example; 1–10) for each VP.
- Virtual path cost must be added to any route shared with neighbor sites to indicate routing preference, including routes learned via Dynamic Routing.
- No Static Virtual Path must have a lower cost than a Dynamic Virtual Path.

Note

VP Route cost deprecates the WAN to WAN forwarding cost that existed in release versions earlier than release version 10.0. The routing decisions based on WAN to WAN forwarding costs have to be reinfluenced by using VP route cost as the WAN to WAN forwarding cost has no significance when you migrate to release version 10.0.

How to Configure Virtual Path Route Cost

To configure Virtual Path Route Cost, at the site level navigate to **Advances Settings** > **Delivery Services** > **Virtual Paths** > **Static Virtual Paths** and enter the route cost for the virtual path. All routes are installed with basic Citrix SD-WAN cost + VP route cost to influence route costs across multiple virtual paths.

	Virtual Paths Internet Service	Intranet Services				
CONFIGURATION V	Static Virtual Paths					
Site Configuration	Virtual Path (LCY2_IT_DC-DXB1)					
Advanced Settings V	OOR Bratile LCV2 IT I	20 Tracking ID	DV P1 Revores Tracking ID	ECMD Ozoup		Route Cast
ARP		AC TREAMING IN	DVD1 Keverse tracking in	ECMP Group		Route Cost
NDP	DG-site			<none></none>	~	1005
Delivery Services	Active Member Paths					
DHCP				_		
DNS					Restore Default Me	mber Paths
NAT	Path					Actions
Dynamic Routing	LCY2_IT_DC-LCY2_IT_DC	-CL-DXB1-DXB1-DU				Ø
Multicast Groups	LCY2_IT_DC-LCY2_IT_DC	-TE - DXB1 - DXB1-DU				Ø
LAG						
VRRP	WAN Link Properties					
Fallback Config Settings	Name	UDP Port	Alternate Port	Port Switching Interval (min)	Tunnel Header Size	Action
Prefix Delegation	DXB1-DXB1-DU	4980		1440	0	ø
Groups	LCY2_IT_DC-LCY2_IT_DC-CL	4980		1440	0	ø
WAN Optimization	LCY2_IT_DC-LCY2_IT_DC-TE	4980		1440	0	Ø
Firewall Settings						
Appliance Settings	Cancel Save					
WAN-OP Settings						
View Configuration						

Use Case:

For example, there are subnets 172.16.2.0/24 and 172.16.3.0/24. Assume that there are two data centers DC1 and DC2 that use both these subnets to transmit traffic to SD-WAN. With the default virtual path route cost, you cannot influence routing since it depends on which route got installed first it can be either the DC2 first or the DC1 next.

With virtual path, you can influence specifically DC2 virtual path to have a higher virtual path route cost (for example, 10) while DC1 has the default VP route cost of 5. This manipulation helps install routes with DC1 first and DC2 next for both.

You can have four routes, two routes to 172.16.2.0/24; one via DC1 with lower cost and then via DC2 with higher cost, and 2 more for 172.16.3.0/24.

Security

July 1, 2022

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.

Firewall Zones (i)

+ Firewall Zone	
Name	Actions
Trail-firewall-zone	Ē
Default_LAN_Zone	
Internet_Zone	
Untrusted_Internet_Zone	
Inter_Routing_Domain_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.

Firewall Defaults ③	
Global Default Firewall Actions	
Action When No Firewall Rules Match	
Allow	
Action When Security Profiles Cannot be Inspected	
Ignore ~	
Action When Security Profiles Inspection Traffic is IPv6	
lgnore ~	
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)
60	120
TCP closed Timeout (s)	
30	
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 in-

spected 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.
- Action When Security Profiles Inspection Traffic is IPv6: Select an option (Ignore or Drop) for the traffic that match the inspect firewall policies.
 - If you select the Ignore option, it allows to bypass the traffic through Citrix SD-WAN network and send it to respective service.
 - If you select the Drop option, IPv6 packets matching the Inspect firewall policies are dropped.

Note

If the INSPECT firewall policies are configured and matching criteria explicitly includes IPv6, an audit error is thrown as shown in the following screenshot:

Configu	ration results	>	<
Search			
			2
1 TOTAL MESS	AGES ERRORS	0 WARNINGS	
Туре	Audit Scope	Audit Message	
8	BR1100	(EC910) At Site BR1100, firewall_filter. Inspect Rules can not be configured for IPv6-Only traffic. Invalid <source address="" ip=""/> : 2001::db8/32.	

For example, you can explicitly select the source/destination IP as IPv6 with inspect (for IP Protocol) action while creating a firewall policy and save it. When you click **Verify Configuration**, an audit error appears.

• **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 policies 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**.

F	irew	all Policies					
G	lobal Def	ault Site Specific	Global Override				
	+ G	lobal 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 Pol	icies						
Policy Information							
Policy Name *		Active Policy					
Firewall Rules							
Create New Rul	e						
• Top of List	Bottom of List O Specify Row	Number Row num	ber				
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

Policy Information			
Policy Name*	Active Policy		
Firewall Type			
Built-in Firewall	~		
Match Criteria			
Match Type	Routing Domain		
Apps & Domains	∨ Default_RoutingDomain	n ~	
Apps & Domains * <u>+ New D</u>	omain App		
Ecommerce	\sim		
Filtering Criteria			
Source Zone		Destination Zone	
Any X	~	Any X	\sim
Source Service Type	Source Service Name *	Source IP	Source Port
Any 🗸	Any 🗸	Any	Any
Dest Service Type	Dest Service Name *	Dest IP	Dest Port
Any 🗸	Any 🗸	Any	Any
IP Protocol	DSCP		
Any 🗸	Any ~	Allow Fragments Reverse Also	Match Established
Actions			
Action	Schedule		
Allow ~	Always On (Default)	\checkmark	
	Add Schedule		
Connection State Tracking			
✓ Log Connection Start & End Ever	nts		
✓ Log Packet Statistics Every	∕5 mins ∨		
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, a domain name-based 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 security

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.

FIPS compliance

FIPS mode enforces users to configure FIPS compliant settings for their IPsec Tunnels and IPsec settings for Virtual Paths.

Enabling FIPS mode offers the following capabilities:

- Displays the FIPS compliant IKE Mode.
- Displays a FIPS Compliant IKE DH Group from which users can select the required parameters for configuring the appliance in FIPS compliant mode (2,5,14–21).
- Displays the FIPS compliant IPsec Tunnel Type in IPsec settings for Virtual Paths
- IKE Hash and (IKEv2) Integrity mode, IPsec auth mode.
- Performs audit errors for FIPS based Lifetime Settings.

To enable FIPS compliance on Citrix SD-WAN Orchestrator service:

- 1. Go to **Configuration > Security > Network Security**.
- 2. In the Network Security Settings section, click the Enable FIPS Mode check box.

Enabling FIPS mode enforces checks during configuration to ensure that all IPsec related configuration parameters adhere to the FIPS standards. You are prompted through audit-errors and warnings to configure IPsec.

Network Security (i)

Network Security Settings	
Encryption	
AES-128	~
Enable Encryption Key Rotation	
Enable Extended Packet Encryption Header	er
Enable Extended Packet Authentication Trailer	
Extended Packet Authentication Trailer Type	
	~
Enable FIPS Mode	
Enable Appliance Authentication	
Network Secure Key	
Regenerate	

If the IPsec configuration does not comply with FIPS standards when it is enabled, an audit error might be triggered. Following are the type of audit errors that are displayed when you click **Verify Config** on the Citrix SD-WAN Orchestrator service UI.

- When FIPS mode is enabled and Non-FIPS compliant option is selected.
- When FIPS mode is enabled and incorrect lifetime value is entered.
- When FIPS mode is enabled and IPsec settings for virtual path default set is also enabled, and incorrect Tunnel mode is selected (ESP vs ESP_Auth / AH).
- When FIPS mode is enabled, IPsec settings for virtual path default set are also enabled, and incorrect lifetime value is entered.

Enable Encryption Key Rotation: When enabled, encryption keys are rotated at intervals of 10–15 minutes.

Enable Extended Packet Encryption Header: When enabled, a 16 bytes encrypted counter is prepended to encrypted traffic to serve as an initialization vector, and randomize packet encryption.

Enable Extended Packet Authentication Trailer: When enabled, an authentication code is appended to the contents of the encrypted traffic to verify that the message is delivered unaltered.

Extended Packet Authentication Trailer Type: This is the type of trailer used to validate packet contents. Select one of the following from the drop-down menu: **32-Bit Checksum** or **SHA-256**.

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 Inspec-tion > 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. Enabling this option may result in otherwise legitimate traffic getting blocked, that is, HTTP traffic on port 443 or HTTPS traffic from sites with an expired certificate.
- **Client Connection Protocols**: Select the required client protocols. The protocols available are SSLvHello, SSLv3, TLSv1, TSLv1.1, TLSv1.2, and TLSv1.3.
- Server Connection Protocols: Select the required server protocols. The protocols available are SSLvHello, SSLv3, TLSv1, TSLv1.1, 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 i

Configuration	Root Certificate	rusted Server Certific	ates		
Enable HTTPS	Traffic Processing				
Block Invalid H	ITTPS Traffic				
Client Conne	ection Protocols	;			
SSLvHello	SSLv3	TLSv1	TLSv1.1	TLSv1.2	TLSv1.3
Server Conn	ection Protocol	S			
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) in PKCS#8 format. 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 U	SSL	Inspection	i
------------------	-----	------------	---

Configuration Root Certificate Trusted Server Certificate	es	
Root Certificate and		
Import the files or copy paste the Root Certificate and		
Kev Root Certificate	Root Key	
		4
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 (i)

Configuration Roo	ot Certificate Trusted Server Certi	ficates			
Trusted Server Certificates Trust all server ce	prtificates				
• Trust all server ce	ertificates signed by root authority and o	certificates listed below			
Add Certificate	e				
Certficate 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**.

Verify Config IPS	Profiles IPS Rules						
Intrusion Prevent	tion						
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 <u>Emerging Trends</u>							
Total Rules: 4 (Preset - 4, Custon	-0)					New	Rule
Rule name	Description	Туре	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.

Citrix SD-WAN Orchestrator

Verify Config IPS Prof	les IPS Rules		
∽ Rule			
Rule Name*			
rule-block-chome-dos			
Description			
Block denial of service through	throme browser.	le de	
IF THE FOLLOWING CONDITI	ON IS MET*		
Category	is	∨ browser-chrome ×	~
OR			
Class Type	is	✓ denial-of-service ×	~
THEN DO THE FOLLOWING*			
Enable Block		×	

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 Preven-tion > IPS Profiles** and click **New Profile**.

Verify Config	PS Profiles IPS Rules				
Each IPS Profile contains or Total Profiles: 1	e or many IPS Rules applied to sites			New Profile	
Profile name	Description	Status	Rules	Sites	
Profile-1				4 1 •••	

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

Citrix SD-WAN Orchestrator

New IPS Prof	ile								
file Name *									
Profile-2									
cription									
		<i>i</i>							
Rules Sites		ß							
Rules Sites	Description		Туре	Status	Categories		Class Type		Action
Rules Sites	Description Critical Priority		Type Proset	Status	Categories	0	Class Type	15	Action
i Rules Sites ule name ritical Priority igh Priority	Description Critical Priority High Priority		Type Preset Preset	Status	Categories	0	Class Type	15	Action blocklog blocklog
Rules Sites Ule name ritical Priority igh Priority iedium Priority	Description Critical Priority High Priority Medium Priority		Type Preset Preset Preset	Status	Categories	0	Class Type	15 15 7	Action blocklog log

On the Sites tab, click Select Sites. Select the sites and click Save. Click Create Profile.

	Site Selector	
Verify Config IPS Profiles IPS Rules	Browse or search the list of sites, regions and groups below. You can ado subset of its members to add/remove.	d/remove entire Regions and Groups, or click into them and choose a
← New IPS Profile	Search	
Profile Name * Profile-2	Filter By Region / Custom Groups	مم
Description IPS Rules Sites Profile-2 Description Description IPS Rules Sites Global(All Sites) IPS Rules Sites Intrusion Prevention Settings will be applied to the sites listed below Intrusion Prevention Settings will be applied to the sites listed below	Available (5 sites) Boston Dallas Kansas SantaClara myLTE	Selected (0 sites)
Create Profile Cancel	Save	

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

Virtual Path IPsec 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.

Virtual Path IPsec 🔅	
Static Virtual Paths IPSec Dynamic Virtual F	aths IPSec
Dynamic Virtual Path IPSec Settings	
Encrypt Dynamic Virtual Path with IPSec	
Encapsulation Type *	
ESP ~	
Encryption Mode *	
AES 128-Bit V	
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.

Certificates i	
+ Add Certificate	
Certificate Name	Actions

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.

Certificates (i)

Certificate	
Certificate Name*	Certificate Type
Enter Name	Trusted \checkmark
Base64 Certificate *	Trusted Identity
Base64 Key	
Cancel Save	

Hosted firewalls

Citrix SD-WAN Orchestrator service supports the following hosted firewalls:

- Palo Alto Networks
- Check Point

Palo Alto Networks

Citrix SD-WAN Orchestrator service 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

Citrix SD-WAN Orchestrator service 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 Citrix SD-WAN Orchestrator service 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.

Citrix SD-WAN Orchestrator

Hosted Firewall @					
Hosted Firewall Profiles VM Administrat	ion VM Images				
Provision Start	Shutdown De-Provision				Befresh Status
Orchestrator Connectivity	Site	VM Model	Admin State	Status	Device Access
				Page Size: 50 ✓ Showing 0-	0 of 0 items Paget of1 < >

4. Provide the following details:

Palo Alto Networks	\sim
Model *	
VM50	\sim
Image File Name *	
Select Image	~
Sites*	
Select Sites	\sim
Panorama Primary IP Or Fqdn	
Panorama Primary IP Or Fqdn	
Panorama Secondary IP Or Fqdn	
Panorama Secondary IP Or Fqdn	
Authentication Code	
Authentication Code	
Authentication Key	
Authentication Key	

- 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

 \cap

Verify Config

Hosted Firewall Profiles

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

(Verify Config	Hosted Firewall Profiles	VM Administration	VM Images		
	Add Profile					
N	lame	Vendor		Model	Deployment Mode	Actions

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

VM Administration VM Images

Hosted Firewall				
Hosted Firewall Profile Name *				
PROFILE_PA				
Vendor	Model		Deployment Mode	
Palo Alto Networks	∨ VM50	\sim	Virtual Wire	\sim
Primary Management Server IP/FQDN		Secondary Management Serv	ver IP/FQDN	
www.hostedfirewall.com		10.105.203.122		
Hosted Firewall Redirection Interfaces				
Logical Interface Name *	Input Interface	Output Int	erface	VLAN ID*
INT1	Interface-1	 ✓ Inter 	face-2	~ 0
Cancel Done				

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

agement 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**.

	Verify Config Firewall Profiles	
Global	Override Profiles	
Site S	pecific Profiles	
Global	Profiles	
+ (Global Profile	
No	Name	Actions
1	branch	Ī

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

Ы	Verify Config Fi	ewall Profiles						
Profil	e Information							
Profile Na	ime * ile1		Active Profile					
Firew	all Rules							
Cr	eate New Rule							
• To	p of List 🔵 Bottom o	of List 🔵 Specify Row	Number Row num	ber				
No	Match Type	Application	Src Zone	Dst Zone	Src Network	Dst Network	Action	Actions
Ca	ncel Save							

 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 Firewal	l Profiles		
Profile Information			
Profile Name * Profile1	✓ Active Profile		
Firewall Type			
Hosted Firewall	\sim		
Match Criteria			
Match Type IP Protocol V	Routing Domain Default_RoutingDomain V		
Filtering Criteria			
Source Zone		Destination Zone	
Any X	\sim	Any ×	~
Source Service Type	Source Service Name *	Source IP	Source Port
Any \checkmark	Any 🗸	Any	Any
Dest Service Type	Dest Service Name*	Dest IP	Dest Port
Any \checkmark	Any \checkmark	Any	Any
IP Protocol	DSCP		
Any 🗸	Any 🗸	Allow Fragments Reverse Also	Match Established
Actions			
Action	Hosted Firewall Profile *	Hosted Firewall Redirection Interface*	1
Redirect to Hosted Firewall \vee	~	~	
Connection State Tracking			-
✓ Log Connection Start & End Eve	ints		
✓ Log Packet Statistics Ever	y 5 mins 🗸 🗸		
Cancel Done			

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

Edge security

October 26, 2021

The Citrix SD-WAN Edge security capabilities enable advanced security on Citrix SD-WAN branch appliances. It simplifies information security management for protecting the branch network from internet threats by providing a single management and reporting pane for various security functionalities along with SD-WAN. It eliminates the need for multiple branch solutions, by consolidating routing, SD-WAN, and security capabilities on a single appliance and reduces network complexity and costs.

The Edge Security stack includes the following security functionality:

- Web filtering
- Anti-Malware
- Intrusion Prevention
- SSL Inspection

Edge Security functionality is available on Citrix SD-WAN Advanced Edition appliances. For more information on Editions, see Citrix SD-WAN Platform Editions and Citrix SD-WAN Platform software support. For more information on supported appliances, see the Citrix SD-WAN Data Sheet.

Note

- Citrix SD-WAN 1100 SE, SD-WAN 210 SE, 210 SE LTE, and 410 SE appliances now support Advanced Edge Security capabilities with Advanced Security add-on licenses. The Advanced security add-on license is supported on 210 platforms from Citrix SD-WAN 11.3.1.1000 release onwards. The Advanced security throughput depends upon your advanced security add-on license. Advanced security throughput request beyond the throughput supported by your security add-on license is dropped.
- The Advanced Edge Security capabilities are not supported in Fail-to-wire deployment mode. It is recommended to use Gateway or Fail-to-block deployment modes.

Since the Edge Security feature is compute-sensitive, Citrix advises you to use the Advanced Edition appliance only at branch sites that do not already have a next generation firewall solution.

While configuring a branch site with Edge Security capabilities, ensure that a **Device Model** that supports Advanced Edition is selected and the **Device Edition** is **AE**. For more details on adding and configuring a site, see Site configuration.

Site Configuration : Basic Settings

ite Information							
ite Profile		Site Name *			Site Address*		Lat/I
None	\sim	California_11	DO_UTM		California,	USA	
egion *	Device Model	5	Sub-Model	×	[Device Edition *	
Default-Region	✓ 1100		↓ BASE		~	AE	
te Role *		Bandwidth Tier (Mbp	os) *		Select Tag		<u>Create</u> I
Branch	\sim	300		~			
dvanced Settings							
ateway ARP Timer (ms)		Host ARP Timer (ms)					
1000		1000			Ena	ble Source MAC Learr	ning

Citrix SD-WAN Orchestrator service allows you to define security profiles for Edge Security capabilities and associate these security profiles with firewall policies. The firewall policies are enhanced to accept security profiles parameters that specify the advanced security capabilities.

Note

You can create security profiles and configure Edge Security features through the Citrix SD-WAN Orchestrator service only.

Security profiles

A security profile is a set of specific edge security options that is applied to a specific segment of traffic define by a firewall policy. The intention is to protect the traffic from security threats. For example, you can define security profiles with different levels of security and access rights for different segments of your network. You can enable and configure Web filtering, Anti-Malware, and Intrusion Prevention settings for each security profile.

The security profiles are then associated to firewall policies to set the criteria for the traffic to be inspected. For example, in an organization, you can create different security profiles for employee subnets and guest firewall zones. You can then assign the security profile to an appropriate firewall policy that matches employee and guest traffic respectively. To create a security profile, at the network level navigate to **Configuration > Security > Security Profile** and click **Add Security Profile**.

Security Profiles	(i)					
Add Security Profile						
Profile name	Description	Web filtering	Anti-Malware	SSL Inspector	IPS	Actions

Provide a name and a description for the security profile. Enable and configure Web filtering, Anti-Malware, and Intrusion Prevention settings as required.

Security Profile	
Profile Name	
Web Filtering Intrusion Prevention Anti-Malware SSL Inspection	
Block/Flag Categories	Manage
Block/Flag Sites	Manage
Bypass Sites	Manage
Bypass Client IPs	Manage
✓ Advanced Options	Enabled Manage
Features above can be managed at anytime regardless of whether " Web Filtering" is enabled or disabled. This gives you more control over when you apply your configuration Enable Web Filtering	

Web filtering

Web filtering allows you to filter the websites your network users access through a categorization database which includes about 32 billion URLs and 750 million domains. It can prevent the exposure to inappropriate sites, spyware, phishing, pharming, website redirection, and other Internet threats. It can also enforce internet policies, preventing access to social media, peer to peer communication, gambling, and other sites frequently disallowed by corporate policies. Web Filter monitors internet traffic on your network and filters it by logging web activities and flagging or also blocking inappropriate content.

When you visit a website and web filtering is enabled, the URL is sent to a cloud database for categorization.

Note

Configure a valid DNS server and enable HTTPS internet access through the SD-WAN management interface. This makes the cloud database reachable so that web filtering can work.

The categorization result is then cached on the SD-WAN appliance to increase the processing speed of future requests. The result is then used to flag, block, or allow websites without increasing the load time. You can add rules to block or bypass sites that are either uncategorized or mis-categorized, or to configure exceptions. You can also bypass web filtering for specific user IPs or subnets.

Block/flag category

You can flag or block different categories of websites. Web filtering classifies URLs into six category groups, IT resources, Miscellaneous, Privacy, Productivity, Security, and Sensitive. Each of these groups has different URL categories. When you choose the block option it implicitly flags the website as well. When you try to access a website of a category that is blocked, it is flagged as a violation and the website is blocked. Categories that are flagged allow you to access the websites, but the event is flagged as a violation. You can view the details in the security logs or reports.

 IT Resources (9) 		Blocked: 2 Flagge				
Category	Description	Block	(()	Flag	(i)	
Streaming Media	Sales, delivery, or streaming of audio or video content, including sites that provide downloads for such viewers.	\checkmark		\checkmark		
Shareware and Freeware	Software, screensavers, icons, wallpapers, utilities, ringtones. Includes downloads that request a donation, and open source projects.					
Peer to Peer	Peer to peer clients and access. Includes torrents, music download programs.					
Online Greeting Cards	Online Greeting card sites.					
Personal Storage	Online storage and posting of files, music, pictures, and other data.					
Web Advertisements	Advertisements, media, content, and banners.	\checkmark		\checkmark		
Content Delivery Networks	Delivery of content and data for third parties, including ads, media, files, images, and video.					
Internet Communications	Internet telephony, messaging, VoIP services and related businesses.					
Web Hosting	Free or paid hosting services for web pages and information concerning their development, publication and promotion.					
✓ Misc (2)			Blocked: 1	Flag	ged: 1	
✓ Privacy (5)			Blocked: 0	Flag	ged: 0	
✓ Productivity (33)			Blocked: 0	Flag	ged: 0	
✓ Security (7)			Blocked: 2	Flag	ged: 2	
✓ Sensitive (23)			Blocked: 0	Flag	ged: 0	

Block/flag sites

Cancel

Done

You can add rules to block or flag specific sites that are allowed by the settings in the categories section. You can also block/flag uncategorized or miss-categorized sites. Enter the domain name provide a description and select **Block** or **Flag**. The decisions for URLs in the **Block/Flag Sites** list take precedence over the decisions based on the site category.

Note

- You can only add fully qualified domain names (FQDNs), for example *somedomain.com*. You cannot add URL paths, for example - *somedomain.com/path/to/file*.
- Any domain added to block/flag sites also includes its subdomains. For instance, adding *domain.com* will block/flag *subdomain1.domain.com*, *subdomain2.domain.com*, and *subdo-*

Citrix SD-WAN Orchestrator

mainlevel2.subdomainlev	rel1.domain.com.				
Block/Flag Sites				×	
Block or flag access to Sites associated with the specified categories that are allowed.					
Site example2.com	Description proxies	Z Block	Flag	Add	
Total: 1					
Sites	Description	Block 🧊	Flag 🥼	Actions	
example1.com	Illegal content	\checkmark		/ 1	
Done Cancel					

Bypass sites

You can add rules to allow specific sites within categories that are blocked. Any domain added to the **Bypass Sites** list is allowed, even if it is blocked by category or by individual URL. Enter the domain name and provide a description. Select **Active** to allow the URL.

Note

- You can only add fully qualified domain names (FQDNs), for example *somedomain.com*. You cannot add URL paths, for example - *somedomain.com/path/to/file*.
- Any domain added to bypass sites also includes its subdomains. For instance, adding *domain.com* bypasses *subdomain1.domain.com*, *subdomain2.domain.com*, and *subdomainlevel2.subdomainlevel1.domain.com*.

Bypass Sites			×
Allow access to the specified sites regardless of matching blocked categories.			
Sile 🕜 news.example.com	Description allowed for visitors		Add
Total: 1			
Site	Description	Active 🕖	Actions
good.example1.com	allowed for visitors		1
Done Cancel			
Bypass client IPs

You can add rules to bypass web filtering for specific IP addresses or subnets. You can provide either an IP address or subnet CIDR notation and a meaningful description. The web filter does not block any traffic, regardless of the blocked categories or sites. Select **Active** to allow traffic from these IP addresses.

Note

Since DHCP IPs can change, use this feature only for clients with static IPs or subnets.

Bypass Client IPs			×
Allow access for clients regardless of matchi	ing blocked categories/URLs.		
IP Address/Range	Description		
192.168.2.100	Allow user		Add
Total: 1			
IP address/range	Description	Active (j)	Actions
192.168.3.0/24	Allow sub-net	\checkmark	1
Done Cancel			

Advanced options

HTTPS options HTTPS options are considered for web filtering if SSL inspection is not configured or the traffic matches an Ignore SSL inspection rule. In these cases, while the full URL is not visible, web filtering might still be performed based on the Server Name Indication (SNI), server certificate, or IP address:

Process HTTPS traffic by Server Name indication (SNI) information if present: SNI is an
extension to the Transport Layer Security (TLS) protocol by which a client indicates the name of
the website that the user is trying to connect to at the start of the secure connection handshake
process.

This not only enables the server to provide the right certificate, but also the SD-WAN appliance to identify the target website and determine its URL category, even if the end-to-end communication is encrypted. If this option is enabled, HTTPS traffic is categorized using the SNI in the HTTPS data stream, if present.

The Process HTTPS traffic by SNI option is enabled by default.

- Process HTTPS traffic by hostname in server certificate when SNI information not present: If this option is enabled and SNI information is not present, then the certificate is fetched from the HTTPS server and the server name on the certificate is used for categorization and filtering purposes.
- Process HTTPS traffic by server IP if both SNI and certificate hostname information are not available: If this option is enabled and neither of the previous options worked, HTTPS traffic is categorized using the IP address.

Advanced Options	×
↑ HTTPS options	
Process HTTPS traffic by SNI(Server Name Indication) information if present	
Process HTTPS traffic by hostname in server certificate when SNI information not present	
Process HTTPS traffic by server IP if both SNI and certificate hostname information are not available	
✓ Safe browsing options	
✓ Block options	
Done Cancel	

Safe browsing options Under **Advanced Options**, the following safe browsing options are added that you can select/deselect as needed:

- Enforce safe search on popular search engines: Safe search is enforced on all searches using supported search engines. For example, Google, Yahoo!, Bing, Ask, and so on.
- **Enforce restrict mode on YouTube**: Restrict mode is enforced on all YouTube content. The restrict mode is an option to intentionally limit your YouTube experience.
- Force searches through kid-friendly search engine: All searches in popular search engines are redirected through kidzsearch.com. The Kidzsearch.com is a web portal powered by Google Custom Search with academic autocomplete that emphasizes safety for children.

Advanced Options	×	
 HTTPS options 		
 Safe browsing options 		
C Enforce safe search on popular search engines		
Enforce Restricted Mode on YouTube		
Force searches through kid-friendly search engine		
> Block options		
Done Cancel		

Safe Browsing only takes effect if related traffic undergoes the **SSL inspection**. Towards this end, ensure that the **SSL inspection** is turned on for the respective security profile and **Inspect** rules for search engines and YouTube are not disabled.

Block Options

- **Block QUIC (UDP port 443)**: The firewall blocks any outgoing communication on UDP port 443, which is typically used for the QUIC protocol, which cannot be processed by the web filtering module. Blocking QUIC results in the browser falling back to TCP based HTTP(S) communication.
- Block pages from IP only hosts: Users entering an IP address rather than domain name is blocked.
- Allow if referrer matches any Bypass Sites: If a page containing external content is allowed through Bypass URL, the external content is passed regardless of other block policies.

Note

Although this option allows you to access the external websites, it exposes a security risk. The referrer option in the HTTP header can be overwritten by browser add-ons and plugins. Citrix advises you to use this option judiciously.

• Close connection for blocked HTTPS sessions without redirecting to block page: The SD-WAN appliance issues an HTTP redirect to a custom block page in case the URL is blocked. However, this redirect is not possible for HTTPS sessions without resulting in a Man-in-the-Middle (MitM) session termination, displaying an invalid certificate browser warning page. This option results in the HTTPS session being terminated instead, to prevent a false warning about a potential attack on the target website.

This option is enabled by default. When enabled, not all the HTTPS traffic gets the SSL inspection treatment.

- **Custom URL for Block**: Set an external server location to redirect users when they are denied access to a website by Web Filter. If a custom URL is configured, the following query string variables are passed so that the receiving system can customize its content.
 - reason: The reason the user was denied access. This is the Category name Web-based+Email, and a longer category description. For example, Sites+offering+web+based+email+and+en (the space characters are replaced with "+") in case the site was blocked due to its category. Otherwise, if blocked due to "block URLs" it is empty.
 - **appname**: The application that is responsible for the denial (Web filtering).
 - appid: The application identifier, an internal identifier for web-filtering which can be ignored).
 - **host**: the domain-name of the URL that the end-user was denied access to.
 - clientAddress: The IP address of the end-user that was denied access.
 - **url**: The requested URL that was denied access.

Note

If you do not use your own webpage to process the denial, the built-in denial issues a redirect to a non-routable IP address.

Advanced Options	×
Process HTTPS traffic by SNI(Server Name Indication) information if present	
Block Options	
Block QUIC (UDP Port 443)	
Pass if referrer matches any Bypass Sites	
Close connection for blocked HTTPS sessions without redirecting to block page	
Custom URL for Blocked Sites	
Done Cancel	

You can view detailed web filtering reports on the Citrix SD-WAN Orchestrator service. For more details, see Reports –Web filtering

Intrusion Prevention

Intrusion Prevention detects and prevents malicious activity in your network. 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. You can choose to enable or disable **IPS** while defining a security profile. When you enable IPS, it inspects the network traffic against signatures which are site-dependent and determined by the IPS profile site mapping. For more information on creating, managing, and associating IPS profiles to sites, Intrusion Prevention.

Note

Intrusion Prevention only detects malicious traffic over the traffic captured by the respective Firewall policies.

WebFiltiring	Anti-Malware	Intrusion Prevention					
Enable Intrusion	n Prevention lobal IPS profiles v	Enabled vill be evaluated and the profile that matches a site in the firewall rule will be applied					
Profile name		Description	Status	Rules	Sites		
Profile 1		Incididunt fames vero rhoncus	Enabled	10	:	15	•••
Profile 2	rofile 2 Incididunt fames vero rhoncus Enabled 10			:	15		
Profile 3		Incididunt fames vero rhoncus	Enabled	10	:	15	
Profile 4	Profile 4 Incididunt fames vero rhoncus Enabled 10				15		
Profile 5		Incididunt fames vero rhoncus	Incididunt	fames ve to rho	ncus	15	
Create	Cancel						

You can view detailed Intrusion Prevention reports on the Citrix SD-WAN Orchestrator service. For more details, see Reports – Intrusion Prevention.

Anti-Malware

The Edge Security Anti-Malware scans and eradicates viruses, trojans, and other malware. Anti-Malware can scan HTTP, FTP, and SMTP traffic at your network and examine it against a database of known signatures and file patterns for infection. If no infection is detected, the traffic is sent to the recipient. If an infection is detected, Anti-Malware deletes or quarantines the infected file and notifies the user.

Anti-Malware uses Bitdefender's engine to scan the downloaded files using a combination of signature database, heuristics for suspicious patterns and dynamic emulator analysis. The download files are blocked if any of these tests fails.

Bypass URLs without scanning

You can bypass Anti-Malware scanning for trusted internal sites or external sites that are used for regular updates, generate more traffic, and are considered safe. By allowing trusted sites to pass through without scanning, you can reduce the resource spent on scanning these sites.

Enter the URL, provide a brief description, and add the URL to the bypass URL list.

Bypass URLs without Scanning			×
Allow access to the URLs below wit	hout being scanned for malware attacks		
URL windows-updates.com	Description trusted - frequently used		Add
URL	Description	Active	Actions
example.com	trusted	\checkmark	/ 1
abc.com	malware scan not needed		1
Done Cancel			

Scan by file types

Anti-Malware by default supports scanning of 41 file-type extensions in HTTP traffic. Anti-Malware scanning involves in depth analysis through signatures, heuristics, and emulation, making it a compute sensitive process.

You can also add a new file type. To add a new file type, click **Manage** > provide **File Types** and **Description** > click **Add**. Select the **Scan** check box to include the file type for Anti-Malware scanning. Clear the **Scan** check box for file types that need not to be scanned. You can also edit or delete the file types if necessary.

Note

The file-types that are selected by default make a balance between the Anti-Malware effectiveness and system performance. Enabling more file types, increase the Edge Security processing load and compromises the overall system capacity.

Citrix SD-WAN Orchestrator

Scan by File Types

Select below the file types that should be scanned for potential malware attack Note that scanning can have a performance impact

File Types	Description	Add		
Total: 41				Selected for Scan: 12
File Type	Description		Scan	
7z			\checkmark	
ace			\checkmark	
arj			\checkmark	
avi			\checkmark	
bat			\checkmark	
tgz			\checkmark	
vb				
vbe			\checkmark	
vbs			\checkmark	
wav				
wmf				
xls			\checkmark	
xlsx			\checkmark	
zip			\checkmark	
Done C	ancel			

Scan by MIME types

A multipurpose internet mail extension (MIME) type is an internet standard that describes the content of an internet file based on the nature and format. Similar to file types, you can also add and choose to exclude certain MIME types from Anti-Malware scanning.

To add MIME types, click **Manage** > add a MIME type in the **MIME Types** field and provide a **Description** > click **Add**. Select the **Scan** check box to include the MIME type for Anti-Malware scanning. Clear the **Scan** check box for MIME type that need not be scanned. You can also edit or delete the MIME types if necessary.

 \times

The MIME types selected by default are chosen to have balance between anti-malware effectiveness and system capacity. Enabling more file types increase the Edge Security processing load and compromises the overall system capacity.

Scan by Mime Types				×
Select below MIME types that	t should be scanned for potential	malware attack		
Mime Types	Description	Add		
Total: 10			Selected	for Scan: 9
Mime Types	Description		Scan	Actions
application/octet-stream				i
application/x-7z-compressed			\checkmark	Ī
application/x-compressed			\checkmark	Ī
application/x-gz			\checkmark	Ē
application/x-gzip			\checkmark	Ē
application/x-rar-compressed			\checkmark	Ē
application/x-tar			\checkmark	Ī
application/x-zip-compressed				1
application/zip				Ī
message/*			\checkmark	Ē
Done Cancel				

Other scan options

You can choose to enable or disable Anti-Malware scans on the following internet protocols:

- Scan HTTP: Enable Anti-Malware scanning on HTTP traffic.
- Scan FTP: Enable Anti-Malware scanning on FTP downloads.
- Scan SMTP: Enable Anti-Malware scanning on SMTP message attachments and choose the action to be performed.

- Remove Infection: The infected attachment is removed and the email is delivered to the recipient.
- Pass Message: The email is delivered to the recipient with the attachment intact.

For **Remove Infection** and **Pass Message** actions the email subject line is prepended with "[VIRUS]".

- Block Message: The email is blocked and not delivered to the recipient.

You can set an external server location to redirect users when they are denied access to a website by Anti-Malware. Select the **Block Page** check box.

- **Custom block page URL**: Creates a custom redirect page. If a custom URL is configured, the following query string variables are passed so that the receiving system can customize its content.
 - Host: The domain-name of the URL that the end-user was denied access to.
 - **URL**: The requested URL that was denied access.

NOTE

If you do not use your own webpage to process the denial, then the built-in denial issues a redirect to a non-routable IP address.

Other Scan Options		×
Scan Protocols		
Scan HTTP		
Scan FTP		
Scan SMTP	Remove Infection	
Anti - Malware Block Page		
✓ Block Page		
O Custom block page URL		
Done Cancel		

You can view detailed Anti-Malware scan reports on the Citrix SD-WAN Orchestrator service. For more details, see Reports –Anti-Malware.

SSL inspection

Secure Sockets Layer (SSL) inspection is a process of intercepting, decrypting, and scanning the HTTPS and secure SMTP traffic for malicious content. It can perform the following:

- Scan for malware
- Perform URL filtering on the full URL path rather than only the top-level domain
- Redirect users to a custom block page for HTTPS traffic similar to that of HTTP traffic

NOTE

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

You can enable SSL inspection and create SSL rules as part of the Security profiles. SSL rules provide the ability to define the conditions to handle the HTTPS and secure SMTP traffic. Before configuring the SSL rules, ensure that you have configured your organization's root CA and deployed the root CA to client devices. For information on configuring root CA, see Security.

On the **SSL Inspection** tab, select **Enable SSL Inspector** to enable SSL inspection. Click **New Rule** and provide a description. Select one of the following conditions:

- **SSL Inspector: SNI Hostname**: Defines the SSL rule based on the Server Name Indicator (SNI) host name.
- SSL Inspector: Certificate Subject: Defines the SSL rule based on the SSL certificate.
- SSL Inspector: Certificate Issuer: Defines the SSL rule based on who the certificate issuer is.

Select the **Operation** and provide a **Value** to match the condition. Select one of the following **Ac-tions**:

- **Inspect**: The traffic that meets the selected rule conditions undergoes SSL inspection.
- **Ignore**: The traffic that meets the selected rule conditions does not undergo SSL inspected and is allowed to flow unimpeded. Basic web filtering based on the SNI can still be performed.

Enable the rule and click Done.

Citrix SD-WAN Orchestrator

Security Profile	New SSL Inspection Rule	×
Profile Name test Description	Description SSL inspection rule	
Web Filtering Intrusion Prevention Anti-A Enable SSL Inspector Total: 0 Total: 0	IF THE FOLLOWING CONDITION(S) ARE MET Select a Condition Operation Value SSL Inspector: SNI Host SSL SSL	
10	THEN DO THE FOLLOWING ACTION Action Type Inspect	

Before completing the SSL inspection configuration, consider the following:

- SSL inspection is a compute-sensitive operation that can reduce Edge Security throughput by up to 70%. It is recommended that you selectively inspect rather than selectively ignore. The default configuration reflects selective inspect by having **Ignore all traffic** enabled as the fallback rule.
- Web filtering **safe browsing options** require SSL inspection of search engine and YouTube traffic. You must not disable or delete the respective default rules if you are planning to use the safe browsing options.

Edge security firewall policy

The Edge Security capabilities are triggered using firewall policies. You can define a firewall policy for the match type **IP Protocol** and map it to a security profile. If the incoming traffic matches the filtering criteria, an inspect action is triggered and the security capabilities, configured as per the selected security profile, are applied.

Citrix SD-WAN evaluates firewall policies in a "first-match" manner, where the first matching policy determines the action. Firewall policies must be configured in the following order:

1. IP protocol, Office 365, and DNS app firewall policies with non-inspect action

- 2. Edge security firewall policies (IP protocol firewall policies with inspect action)
- 3. Application firewall policies

To configure a firewall policy and enable edge security, navigate to **Configuration** > **Security** > **Firewall Profiles** and add a profile based on your preference. Click **Create New Rule**. Select the **Match Type** as **IP Protocol** and configure the filtering criteria. For more information, see Firewall profiles. Select the **Inspect (for IP Protocol)** action and select a security profile.

Profile Information			
Profile Name * profile-test Built-in Eirewall	Active Profile		
Match Criteria			_
Match Type	Routing Domain		
IP Protocol V	Default_RoutingDomain		
Filtering Criteria			
Source Zone		Destination Zone	
Any ×	~	Any ×	
Source Service Type	Source Service Name *	Source IP	Source Port
Any 🗸	Any ~	Any	Any
Dest Service Type	Dest Service Name *	Dest IP	Dest Port
Any 🗸	Any 🗸	Any	Any
IP Protocol	DSCP		
Any 🗸	Any 🗸	Allow Revers Fragments Also	e Match Established
Actions			
Action	Security Profile *		
Inspect (for IP Protocol)	daasdf 🗸 🗸		
Connection State Tracking	1		

While there is no limit on the number of security profiles you can create, you can only assign up to 32 Inspect firewall policies to a site.

Limitations

- The appliance software takes longer time to download for Citrix SD-WAN Standard Edition (SE) appliances that are upgraded to Advanced Edition (AE). The Edge Security subsystem of AE appliances is bundled separately to prevent any impact on the download size for SE appliances.
- The Citrix SD-WAN Edge Security web filtering can only check the Server Name Indication (SNI) for the HTTPS sites to decide whether to block, flag, or allow the traffic.
- External syslog server support is not available through Citrix SD-WAN Orchestrator service for Citrix SD-WAN Edge Security.

Related topics

- Intrusion Prevention
- Web filtering reports
- Anti-Malware reports
- Intrusion Prevention reports
- Security alerts
- Security logs

Firewall settings

July 29, 2021

You can configure firewall settings at a site level. These settings provide security to all the SD-WAN appliances on a specific site.

The following are the instructions to configure the Site-specific override firewall settings:

- 1. At the site level, navigate to **Configuration > Advanced settings > Firewall settings**.
- 2. Select the **Site Specific Override** option from the **Override Firewall Settings** drop-down menu. This action applies the defined firewall rules on a specific site.

If you want to switch from site-specific setting to a global default setting, select the **Global Defaults** option from the drop-down list. This action removes the site-specific configuration and retains the global specific defaults.

Firewall Settings (i)

Override Firewall Settings	
Site Specific Override V	
Firewall Actions	
Action When No Firewall Rules Match	
Allow ~	
Firewall Settings	
Default Connection State Tracking	
No Tracking V	Source Route Validation FTP ALG
Max Connections Per Source	Max New Connections Per Source
0	0
Use Global Connection Timeouts	
Denied Timeout (s)	
30	
TCP Initial Timeout (s)	TCP Idle Timeout (s)
120	7440
TCP Closing Timeout	TCP Time Wait Timeout (s)
60	120
TCP closed Timeout (s)	
10	

- Action When No Firewall Rules Match: Select an action (Allow or Drop) from the dropdown list for the packets that do not match a Firewall 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.
- **Source Route Validation**: When you select this check box, packets are dropped when they are received on an interface that is different from the packet's route, as determined by the source IP address.
- **FTP ALG**: When you select this check box, the FTP ALG (Application layer gateway) monitors connections on TCP port 21 and updates FTP messages with the appropriate NAT IP addresses.
- Max Connections per Source: Maximum number of non-established connections that each source IP address can allow. By default, each source IP address allows an unlimited number of non-established connections.

- Max New Connections per Source: Maximum number of connections that each source IP address can allow. By default, each source IP address allows unlimited number of connections.
- Use Global Connection Timeouts: When you select this check box, SD-WAN enables the global timeout settings. To configure specific timeout settings, clear this check box.
 - **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.
- 3. Click Save.

Configure firewall segmentation

November 24, 2021

Virtual Route Forwarding (VRF) firewall segmentation provides multiple routing domains accesses to the internet through a common interface, with each domain's traffic isolated from that of the others. For example, employees and guests can access the internet through the same interface, without any access to each other's traffic.

- Local guest-user Internet access
- Employee-user Internet access for defined applications
- Employee-users may continue hairpin all other traffic to the MCN
- Allow the user to add specific routes for specific routing domains.
- When enabled, this feature applies to all routing domains.

You can also create multiple access interfaces to accommodate separate public facing IP addresses. Either option provides the required security necessary for each user group.

Enabling Internet Access on Routing Domain(s)

You can enable Internet access on a routing domain through Citrix SD-WAN Orchestrator service. This option auto-creates a DEFAULT route (0.0.0.0/0) on all the routing tables of the respective routing domains. You can enable Internet access for all the routing domains, or none. It avoids the need for creating exclusive static route across all the routing domains if the Internet access is required.

Access Interfaces					
Access Interface Name	Virtual Interface *		Virtual Path Mode		
BRANCH_UTM-WL-1-AI-1	WANT	~	Primary		÷
IP Address'	● V4 ○ V6	Gateway IP Address *			
Bind Access Interface to Gateway MAC	sable Proxy ARP				
Enable Internet Access on Routing Domain(s)					
Ali v					
				Cancel	Done

For more information, see Access interface.

Use Cases

The following are the supported use cases for firewall segmentation:

- Customers have multiple routing domains at a branch site without the requirement to include all domains at the data center (MCN). They need the ability to isolate different customers' traffic in a secure manner
- Customers must be able to have a single accessible firewalled Public IP address for multiple routing domains to access the internet at a site (extend beyond VRF lite).
- Customers need an Internet route for each routing domain supporting different services.
- Multiple routing domains at a branch site.
- Internet Access for different routing domains.

Multiple routing domains at a branch site

With the Virtual Forwarding and Routing Firewall segmentation enhancements, you can:

- Provide an infrastructure, at the branch site, that supports secure connectivity for at least two user groups, such as employees and guests. The infrastructure can support up to 254 routing domains.
- Isolate each routing domain's traffic from the traffic of any other routing domain.
- Provide Internet access for each routing domain,

- A common Access Interface is required and acceptable
- An Access Interface for each group with separate Public facing IP addresses
- Traffic for the employee can be routed directly out to the local internet (specific applications)
- Traffic for the employee can be routed or backhauled to the MCN for extensive filtering (0 route)
- Traffic for the routing domain can be routed directly out to the local internet (0 route)
- Supports specific routes per routing domain, if necessary
- Routing domains are VLAN based
- Removes the requirement for the RD to have to reside at the MCN
- Routing Domain can now be configured at a branch site only
- Allows you to assign multiple RD to an access interface (once enabled)
- Each RD is assigned a 0.0.0.0 route
- Allows specific routes to be added for an RD
- Allows traffic from different RD to exit to the internet using the same access interface
- Allows you to configure a different access interface for each RD
- Must be unique subnets (RD are assigned to a VLAN)
- Each RD can use the same FW default Zone
- The traffic is isolated through the Routing Domain
- Outbound flows have the RD as a component of the flow header. Allows SD-WAN to map return flows to correct Routing domain.

Prerequisites to configure multiple routing domains:

- Internet access is configured and assigned to a WAN Link.
- Firewall configured for NAT and correct policies applied.
- Second routing domain added globally.
- Each routing domain added to a site.
- For information about configuring Internet services on the routing domains, see WAN links.

Deployment scenarios



Limitations

• The internet service must be added to the WAN link before you can enable Internet access for all Routing Domains. (Until you do, the check box for enabling this option is grayed out).

After enabling Internet access for all routing domains, auto add a dynamic-NAT rule.

- Access Interface (AI): Single AI per subnet.
- Multiple AIs require a separate VLAN for each AI.

- If you have two routing domains at a site and have a single WAN Link, both domains use the same public IP address.
- If Internet access for all routing domains is enabled, all sites can route to Internet. (If one routing domain does not require internet access, you can use the firewall to block its traffic.)
- The WAN links are shared for Internet access.
- No QOS per routing domain; first come first serve.

Link aggregation groups

November 8, 2021

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.

Earlier, only the Active-Backup mode was supported in LAG. From Citrix SD-WAN 11.3 release onwards, the 802.3AD Link Aggregation Control Protocol (LACP) protocol based negotiations are supported. The LACP is a standard protocol and provides more functionality for LAGs.

The LAG functionality is available only on the following 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 2100 SE/PE
- Citrix SD-WAN 4100 SE
- Citrix SD-WAN 5100 SE/PE
- Citrix SD-WAN 6100 SE/PE

The LACP LAG functionality is not available on the following platforms:

- Citrix SD-WAN 1000 SE / PE
- Citrix SD-WAN 2000 SE / PE
- Citrix SD-WAN 4000 SE
- VPX/VPXL platforms

While configuring Link Aggregation Groups (LAG), you can configure the **Mode** and **Transmission Policy**. Mode defines how the ports handle the traffic. The following are the supported modes:

- **Active-Backup**: In Active-Backup mode, at any time only one port is active, and the other ports are in backup mode. You can send the traffic through one port at a time. The Active-Backup mode supports rely on the Data Plane Development Kit (DPDK) package for LAG functionality.
- **LACP**: You can send the traffic through all the ports simultaneously. As a benefit, you get more bandwidth along with the link redundancy mechanism.

As LAG groups have many ports, the transmission policy helps to select the port that can be used to send traffic. The **Transmission Policy** drop-down list can be enabled only if the mode is **LACP**. The following are the supported transmission policies:

- **MAC+IP**: The link selection for a given packet is based on the layer 2 and 3 parameters. So, the source and destination MAC and IP addresses take these parameters and hash them. According to hash, it selects the port.
- **IP+L4**: The IP+L4 policy is based on the source and destination IP and layer 4 ports and protocol. The IP+L4 policy notifies which packet is going through which port. Packet with the same parameters will always be sent on one of the links. That means, the same or single flow (same source and destination Mac and IP) always goes through the same ports and not distributes across the other ports. As a benefit, the out of order packets cannot reach to the destination device.

You can create virtual interfaces using LAGs and these interfaces are further used to configure LAN/WAN links and HA.

Note

- A minimum of two ports and a maximum of four ports are supported per LAG.
- All members of LAG must be of the same type, for example 1/1 or 1/2. 1/1 and 10/1 are not supported LAG configuration.
- The Link State Propagation (LSP) feature is not supported, if LAGs are used as Ethernet interfaces in Interface Groups.
- The port priority and system priority options are not supported with the LACP implementation.
- With 11.3 release onwards, in SD-WAN with the LACP implementation, the ports are always in active mode. That means SD-WAN can always start the negotiation.

	Maximum number of LAGs					
Platform	supported	LACP supported ports				
110	1	1/1				
210	2	1/1 or 1/2				

Citrix SD-WAN Orchestrator

Platform	Maximum number o supported	of LAGs LACP supported ports
410	1	1/1 or 1/2
1100	3	1/1 or 1/2
2100	3	1/1 or 1/2
4100	4	1/1 or 1/2
5100	3	10/1 or 10/2

Citrix SD-WAN Orchestrator

	Maximum number of LAGs				
Platform	supported	LACP supported ports			
6100	4	1/1 or 1/2			

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.

L	AG (i)				
	Name	Ethernet Interfaces	Mode	Transmission Policy	
	LAGO	1/1 1/2 1/3	LACP 🗸	IP+L4 V	
	LAG1	1/1 1/2 1/3	~	~	
	Save				

Once the ports are added to the LAG, you can select the LAGs to configure interfaces under **Site Con-figuration**. 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.

_		-	-	-		
nterface A	Attributes					
eployment N	/lode [*] Interfa	ace Type *	Security *	Interface Name		
Edge (G	ateway) 🗸 W	/AN V	Untrusted	✓ WAN-1		
					-	
Physical In	terface					
Select Inter	face*			Link Aggreg	gation Group	
LAG0	1/1 1/4-MGMT LTE	-1				
/irtual Inte	erfaces					
L Out	lute of a sec					
+ Sub	-Interface					
VLAN ID	Routing Domain	Firewall Zone	IP Address	VIF Name	Actions	
	Default_RoutingDo	<default></default>	172.16.42.10/24	VIF-2-WAN-1	<u>ا</u>	
0						

In the **Interfaces** section, click **Link Aggregation Group** to quickly change the LAG configuration if necessary.

Link A	Aggregat	ion Groups		
Nar	me	Ethernet Interfaces	Mode	Transmission Policy
LAG	GO	1/1 1/2 1/3	~	~
LAG	G1	1/1 1/2 1/3	Active-Backup 🗸	None 🗸
(Cancel	Done		

You can view the details of the interfaces that are configured with LAG and LACP under **Reports > Appliance Reports > LACP LAG Group**. For more information, see Appliance reports.

Network Security ④

Certificate authentication

November 11, 2021

Secure paths are established between appliances in the SD-WAN network by using security techniques such as network encryption and virtual path IPsec tunnels. In addition to the existing security measures, certificate based authentication is introduced in Citrix SD-WAN 11.0.2.

Using Certificate authentication organizations can use certificates issued by a private Certificate Authority (CA) to authenticate appliances. The appliances are authenticated before establishing the virtual paths. For example, if a branch appliance tries to connect to the data center with a certificate that does not match with the certificate that the data center expects, the virtual path is not established.

The certificate issued by the CA maps a public key to the name of the appliance. The public key is compatible with the corresponding private key possessed by the appliance identified by the certificate.

To enable appliance authentication, at the network level navigate to **Configuration > Security > Net**work Security and select **Enable Appliance Authentication**.

Network Security Settings

Encryption

AES-128

C

Enable Encryption Key Rotation

Enable Extended Packet Encryption Header

Enable Extended Packet Authentication

Trailer

Extended Packet Authentication Trailer Type

Imable FIPS Mode

Imable Piper Mode

Imable Recent Recent

Regenerate

Inline mode

January 13, 2022

In this mode, the SD-WAN appliance appears to be an Ethernet bridge. Most of the SD-WAN appliance models include a fail-to-wire (Ethernet bypass) feature for inline mode. If power fails, a relay closes and the input and output ports become electrically connected, allowing the Ethernet signal to pass through from one port to another. In the fail-to-wire mode, the SD-WAN appliance looks like a cross-over cable connecting the two ports.

Advantages and Use-cases

The following are the advantages/use cases for the Inline mode deployment:

- Keeping the MPLS router therefore fail-to-wire is a lovely feature. Fail-to-wire capable devices enable seamless failover to underlay infrastructure if the box went down.
 - If your devices support fail-to-wire (SD-WAN 210 and above), this allows placing a single SD-WAN inline to hardware bypass the LAN traffic to the customer edge router when the SD-WAN crashes/goes down.
 - If the MPLS Links are present that yield a natural extension to the customer's LAN/Intranet, the fail-to-wire bridge-pair port is the best choice (fail-to-wire capable pairs) such that, when the device crashes or goes down the LAN traffic is hardware bypassed to the customer edge router (still maintained the next hop).
- Networking is simple.
- SD-WAN sees all traffic through the inline mode, so it is the best-case scenario for the proper bandwidth/capacity accounting.
- Few integration requirements as you need only an IP of the L2 segment. LAN segments are well known as you have an arm to the LAN interface. If you connect to a core switch, you can also run dynamic routing to get visibility to all LAN subnets.
- Customer's expectations are that SD-WAN must blend into the existing infrastructure as a new network node (nothing else changes).
- Proxy ARP In inline mode, it is a blessing for SD-WAN to proxy ARP requests to LAN next-hop if the gateway went down or the SD-WAN interface towards next-hop went down.
 - Generally, in inline mode with bridge-pair (fail-to-block or fail-to-wire) with multiple WAN connections (MPLS/Internet), it is recommended to enable Proxy ARP for the bridge pair interface that connects the LAN hosts to their next-hop gateway.
 - For any reason when the next-hop is down or the SD-WAN interface to the next-hop is down rendering the gateway unreachable, SD-WAN acts as a proxy for ARP requests allowing the LAN hosts to still seamlessly send packets and use the remaining WAN connections that keep the virtual path up.
- High availability If fail-to-wire is not an option, devices can be placed in parallel high availability (common LAN and WAN interfaces for the Active/Standby) devices to achieve redundancy.

- If your appliances don't support fail-to-wire, like the SD-WAN 110, you have to go with inline parallel high availability that enables to have a standby device kick in if the primary went down.

Recommendations

The following are the recommendations for the Inline mode deployment:

- The inline mode is best for the branches where the existing infrastructure is not to be changed and SD-WAN sits transparently inline to the LAN segment.
- Data centers can also deploy inline fail-to-wire or inline parallel high availability as it is immensely important to ensure that the data center workloads are not blackholed due to device down/crash.

Cautions

The following are the information that you need to be careful about in the Inline mode:

- Plumbing network with two arms to the SD-WAN (LAN and WAN side), needs some downtime as the network must be plumbed in two arms.
- Must ensure if fail-to-wire is used, it is behind a customer edge router/firewall in a **TRUSTED** zone so that security is not compromised.
- MPLS QoS changes a little in this as the previous QoS policies might have depended on the source IP addresses or DSCP based which will now be masked because of an overlay.
- Care must be taken to repurpose the MPLS router with a well-designed SD-WAN specific reserved bandwidth with a specific DSCP tag, such that SD-WAN's QoS takes care of prioritizing traffic and sends out high priority applications immediately followed by other classes (but be able to account for the overall bandwidth reserved for SD-WAN on the MPLS router). MPLS queues are an alternative or MPLS with a single DSCP set on the auto path group that can take care of this.
- If the Internet interfaces are **TRUSTED** as the links terminate on the customer edge router, to use Internet service, you must write an exclusive dynamic NAT rule to enable internet breakout from the appliance.
- If the Internet links are the only WAN connections and still terminate on the customer edge router, it is still fine to bypass the connections if the customer edge router takes precautions to steer the packets via their existing underlay infrastructure.
 - Proper care must be taken to account for the flow of bypassing LAN traffic over bridgepair with an Internet connection and when the appliance is down. Since this is a sensitive enterprise Intranet traffic, in the eve of failure, the customer must know how to handle it.

Before you begin

Before you begin the configuration, ensure that you have a good understanding of the network topology and gathered the details of the site.

The following is an example of an SD-WAN network where a branch is configured in inline mode.



The details of each site are provided in the following table:

Site details	Inline mode
Site Name	Branch 1
Management IP	172.30.2.20/24
Security Key	If any
Model/Edition	2100
Mode	Inline
Topology	2 x WAN Path
VIP Address	10.17.0.9/24 - MPLS, 10.18.0.9/24 - Internet, Public IP a.b.c.d
Gateway MPLS	10.17.0.1
Gateway Internet	10.18.0.1
Link Speed	MPLS - 10 Mbps, Internet - 2 Mbps
Route	No additional routes were added

Site detailsInline modeVLANsNone (default 0)

Configure inline mode

1. At the customer level configuration, navigate to **Configuration > Network Home**. Click **Add Sites**.

Site Details			
šite Name *			
Branch 1			
On-Premises Cloud Site			
Site Address*			Lat/Lng
New York, NY, USA			
lotes (Optional)			
Enter Notes for this Site			
			/

2. Click **Next** and navigate to **Site Details** tab. Select the site role as **Branch**. Click **Next** and navigate to **Device Details** tab. Enter the serial number of the appliance.

Site Profile	Site Name*		Site Address*	Lat/Lng
None	✓ Branch 1		New York, NY, USA	
Region *	Device Model *	Sub-Model*	Device Edition	
Default-Region \lor	2100 ~	BASE	✓ SE	~
Site Role *		Bandwidth Tier (Mb	ps) *	
Branch	~	1000		\sim

3. Click **Next** and navigate to **Interfaces** page. Click **+ Interface**. Select **Inline (Fail-To-Wire)** as the **Deployment mode**. Select the interfaces based on your preference and virtual IP addresses. Click **Done**.

Add two interface pairs in bridge pair mode; one for MPLS and one for Internet.

- 4. Click Next and navigate to the Interfaces tab. Click + Interface.
- 5. Select **Virtual Inline (One-Arm)** from the **Deployment Mode** drop-down list and **One-Arm** as the **Interface Type**. Select the Ethernet interface that connects to the Virtual Inline mode router. As per this topology, add two virtual LANs with the same physical interface; one for MPLS and one for Internet.

To add the first VLAN, in the **Virtual Interfaces** section, enter the VLAN ID, name for the virtual interface, and IP address. Click **Done**.

Verify Config 00 Site Details 02 Device Details 03 Interfaces 04 WAN Links 05 Routes	00 Summary
Interface Attributes	
Deployment Mode * Interface Type * Security * Interface Name	
Inline (Fail-To-Wire) V Bridge V Trusted V Bridge-1	
Physical Interface	
Link Aggregation Group	
Select Interfac	
Port Pair LSP	
1/1 1/2	
Virtual Interfaces	
VLAN ID* Virtual Interface Name*	Bridge-1 1/1 Bridge-1 1/2
0 MPLS Branch Enable HA Heartbeat	
Routing Domein* Firewall Zones Client Mode	
Default_RoutingDomain None	Branch 1 SDWAN-2100 (Primary)
DHCP IPv4 DHCP IPv6 SLAAC Directed Finabled	
+ IPv4 Addresses + IPv6 Addresses	
IP Address Identity Private Link Local	
19v4 10.17.0.9/24	
IPv6	
Eg: 2001:0db8:85a3:0000:0000:8a2a:0370:	
Done	

Verify C	onfig 01 Site	Details	Device Details 03 Interfaces	04 WAI	N Links	05 Routes	06 Summary
+ Interface							
In-band Managemen	t IP In-band Ma	anagement IPv6	In-band Management DNS	In-band Man V6 None	agement DNS		
Interface Name	Port(s)	VLAN ID	IP Address		Actions		
Bridge-1	1/1, 1/2	0	10.17.0.9/24		iii		
Bridge-2	1/3, 1/4	0	10.18.0.9/24		iii		
						-	

6. Click **Next** and navigate to **WAN Links** tab. Click **+ WAN Link** and select the **Create New** radio button. Add two WAN links; One for MPLS and one for Internet.

For the internet WAN link, select **Public Internet** as the **Access Type**. Select the **ISP Name** and the name of the WAN link gets populated automatically. Select speed and choose the required virtual interface and the gateway.

For the MPLS WAN link, select **MPLS** as the **Access Type**. Select the ISP Name and the name of the WAN link gets populated automatically. Select speed and choose the required virtual interface and the gateway.

Note

If the data center and branches have different ISPs, then you must create an autopath group and include the details of ISPs in it.

iic IPv4 Address E.g. a.b.c.d	ACT Tracking IP Addres Public IPv	Custom Custom 6 Address	Internet Category Broadband	
lic IPv4 Address E.g. a.b.c.d	ACT Tracking IP Addre Public IPv	ss 6 Address	Broadband	
lic IPv4 Address E.g. a.b.c.d	Tracking IP Addre	ss 6 Address		
lic IPv4 Address E.g. a.b.c.d	Public IPv E.g. 2	6 Address		
lic IPv4 Address E.g. a.b.c.d	Public IPv E.g. 2	6 Address		
E.g. a.b.c.d	E.g. 2			
		2001:0db8:85a3	:0000:0000:8a2e:03	70:7334
		ngress		
	Mbps 🗸	Speed*		Mbps
		2		
Auto Learn 🗹 Pł	iysical Rate	Permitted Rate	🗌 Auto Learn 🗸	Physical Ra
		2		
Virtu	al Interface*		Virtual Path Mode *	
	NET_Branch	~	Primary	
۲	V4 V6 G	ateway IP Address	*	
		10.18.0.1		
e to Gateway MA	AC Enable	Proxy ARP		
	Auto Learn Virtu	Auto Learn Physical Rate	Auto Learn Physical Rate Permitted Rate 2 Virtual Interface* NET_Branch VG Gateway IP Address 10.18.0.1 e to Gateway MAC Enable Proxy ARP	Auto Learn Physical Rate Permitted Rate Auto Learn Virtual Interface* Virtual Path Mode* INET_Branch Primary V4 V6 Gateway IP Address* 10.18.0.1 e to Gateway MAC Enable Proxy ARP

Verify Config	g 01 Site Details 02	Device Details 03 I	nterfaces	04 WAN Links	05 Routes	08 Summary			
+ WAN Link	l								
WAN Link Name	Speeds	Access Interface IP	Gateway IP	Actions					
Branch_MPLS	10 Mbps† 10 Mbps↓	10.17.0.9	10.17.0.1	Î					
INET_Branch	2 Mbps† 2 Mbps↓	10.18.0.9	10.18.0.1	Û					
					-				
						Bridge-1 1/1		Bridge-1	1/2Branch_MPLS
						Daldas 0. 40		Deldes C	ALABET Desert
Cancel	Save			Prev Next		Bridge-2 1/3		Bridge-2	1/4INET_Branch
						001	Branch 1		
						SDW	AN-2100 (Ph	mary)	

7. Click **Done** and then **Save**. Click Verify to validate the configurations. If any errors observed, fix them before proceeding further.

Virtual inline mode

January 13, 2022

In virtual inline mode, the router uses routing protocol such as PBR, OSPF, or BGP to redirect incoming and outgoing WAN traffic to the appliance, and the appliance forwards the processed packets back to the router.

Virtual inline mode is the simplest and recommended way to network SD-WAN in the data center. It allows parallel network plumbing of SD-WAN with the head-end core router while the data center is serving its existing workloads with existing infrastructure. The virtual inline mode allows us to easily define PBRs to divert LAN traffic to go through SD-WAN and get overlay benefits.

Advantages and Use-cases

The following are the advantages of Virtual Inline mode deployment:

• Seamless forwarding to SD-WAN for overlay benefits under normal conditions and seamless failover to underlying infrastructure if SD-WAN fails.

- Simple Networking and Integration requirements. The single one-arm interface from headend router to SD-WAN in virtual inline.
- Easy to deploy dynamic routing in Import only mode (export nothing) to get visibility of LAN subnets so they can be sent to remote SD-WAN peer appliances.
- Easy to define PBR on the routers (1 per WAN VIP) to indicate how to choose the physical.

Recommendations

The following are the recommendations for the Virtual Inline mode deployment:

- The virtual inline mode is best for data center networking as the SD-WAN network plumbing can be worked on parallel while the data center is serving its existing workloads with existing infrastructure.
- SD-WAN is in a one-arm interface that is managed with an SLA tracking on VIPs. If the tracking goes down, the traffic resumes routing via existing underlay infrastructure.
- Branches can also be deployed in virtual inline mode. However, they are more predominant with Inline/Gateway deployments.

Cautions

The following are the information that you need to be careful about in the Virtual Inline mode:

- Proper care must be taken to distinctly MAP the SD-WAN logical VIP of a WAN link defined to the right physical interface (else this might cause undesirable issues in WAN metric assessment and choice of WAN paths).
- Proper design considerations are to be made to know if all traffic is diverted via SD-WAN or only specific traffic.
- This means SD-WAN must be dedicated some share of bandwidth exclusively for itself that must be set on the interfaces such that SD-WAN's capacity is not used by other non-SD-WAN traffic causing undesirable outcomes.
 - Bandwidth accounting issues and congestion issues might occur if SD-WAN WAN links capacity is defined incorrectly.
- Dynamic routing can cause some issues if improperly designed where if the SD-WAN routes data center and branch VIPs are exported to the headend and if routing is influenced towards SD-WAN, overlay packets start looping and cause undesirable outcomes.
- Dynamic routing must be properly administered considering all potential factors of what to learn/what to advertise.
- One-arm physical interface might become a bottleneck sometimes. Needs some design considerations in those lines as it caters to both upload/download and also acts as LAN to LAN and LAN to WAN/WAN to LAN traffic from SD-WAN.

- Excessive LAN to LAN traffic might be a point to note during design.
- If the dynamic routing is not used, there must be proper care if administering all LAN subnets, which if not, might cause undesirable routing issues.
- There are potential routing loop issues if you define some default route (0.0.0.0/0) on the SD-WAN in the virtual inline to point back to the headend router. In such situations, if the virtual path went down, any traffic coming from the data center LAN (like monitoring traffic) is looped back to the headend and back to SD-WAN causing undesirable routing issues (If the virtual path is down, the remote branch subnets become reachable **NO** causing the default route to be HIT, that causes the loop issues).

Before you begin

Before you begin the configuration, ensure that you have a good understanding of the network topology and gathered the details of the site.

The following is an example of an SD-WAN network where the data center is configured in virtual inline mode.



The details of the site are provided in the following table:

Site details	Virtual inline mode
Site Name	San Jose Data Center
Management IP	172.30.2.10/24
Security Key	If any

Site details	Virtual inline mode
Model/Edition	4100
Mode	Virtual Inline Mode
Topology	2 x WAN Path
VIP Address	192.168.1.10/24 - MPLS, 192.168.2.10/24 - Internet, Public IP - w.x.y.z
Gateway MPLS	10.20.0.1
Gateway Internet	10.19.0.1
Link Speed	MPLS - 100 Mbps, Internet - 20 Mbps
Route	Add a route on the SD-WAN SE Appliance on how to reach the LAN Subnets through any of the physical interfaces.

VLANs

MPLS - VLAN 10, Internet - VLAN 20

Configure virtual inline mode

 At the customer level configuration, navigate to Configuration > Network Home. Click Add Sites. Enter the site name, select On-Premises check box, and add other details as required.


Site Details		
Site Name *		
San Jose Data Center		
On-Premises Cloud Site		
Site Address *		🗹 Lat/Lng
San Jose, CA, USA		
_atitude *	Longitude *	
37.3382082	-121.8863286	
Notes (Optional)		
Enter Notes for this Site		

2. Click **Next** and navigate to **Site Details** tab. Select the site role as **MCN**. select the device model, edition, and bandwidth as per your preference.

Verify Config	Site Details 02 Det	vice Details 🛛 💿 Interfac	ces 04 WAN Links	05 Routes	of Summary
Site Information					
iite Profile None V	Site Name * San Jose Data Cen	Site Address* 🗹 Lat/Lng San Jose, CA, USA	37.3382082 -121.8863286		
egion * Default-Region V ite Role *	Device Model * 4100 V	Sub-Model * BASE Bandwidth Tier (Mbps) *	Device Edition *		
MCN efault Routing Domain	~	2000			
Default Routing Domain Settings Default Routing Domain Global Default Default_RoutingDomain					
dvanced Settings Enable Source MAC Lea Preserve route to Interr	arning het from link even if all asso	pointed paths are down		1	San Jose Data Center
Preserve route to Intran	et from link even if all asso	ociated paths are down		11	SDWAN-4100 (Primary)
ontact Name Enter Contact Name for	this Site	Contact Email Enter Contact Email fo	r this Site		
lotes					
Enter Notes for this Site				A	
Cancel Save			Prev Ne	xt	

- 3. Click **Next** and navigate to **Device Details** tab. Enter the serial number of the appliance.
- 4. Click **Next** and navigate to the **Interfaces** tab. Click + **Interface**.
- Select Virtual Inline (One-Arm) from the Deployment Mode drop-down list and One-Arm as the Interface Type. Select the Ethernet interface that connects to the Virtual Inline mode router. As per this topology, add two virtual LANs with the same physical interface; one for MPLS and one for Internet.

To add the first VLAN, in the **Virtual Interfaces** section, enter the VLAN ID, name for the virtual interface, and IP address. Click **Done**.

🕜 💿 Site Details 💿 Device Details 🔯 Interfaces 🐼 WAN Links 🚳 Routes 💿 Summar	4
Interface Attributes	
Deployment Mode* Interface Type* Security* Interface Name Virtual Inline (One-Arm) One-Arm Trusted One-Arm-1	
Physical Interface	
Link Aggregation Group 1/1 1/2 1/3 1/4 10/1 10/2 10/3 10/4 10/5 10/6	
Virtual Interfaces	
VLAN ID* Virtual Interface Name* 10 MPLS Enable HA Heartbeat	1/4
Routing Domain* Firewall Zones Client Mode Default_RoutingDomain None	
DHCP IPv4 DHCP IPv6 SLAAC Directed Scleat Client Client Broadcast	
+ IPv4 Addresses + IPv6 Addresses	San Jose Data Center SDWAN-4100
IP Address Identity Private Link Local Delete	
IPv4 192.168.1.10/24	
Cancel Done	

6. Click **+ Sub-Interface** to add another VLAN and then enter the virtual interface details. Click **Done** at the bottom of the screen to navigate to the next tab.

	Attributes						
ployment M	Mode*	Interface Type *	Security*	Interface	e Name		
Virtual	nline (One-Arm) 🗸	One-Arm	∨ Trusted	✓ One	-Arm-1		
iysical In	terface						
				Link Agg	regation Group	2	
lect Interfa	ice*						
/1 1/2	1/3 1/4 10/1	10/2 10/3 1	0/4 10/5 10/6				
rtual Inte	erfaces						
+ Sub	Interface						v
/LAN ID	Routing Domain	Firewall Zone	IP Address	VIF Name	Actions	1	1/4
10	Default_Routin	<default></default>	192.168.1.10/24	MPLS	i		
		< Default>	192 168 2 10/24	Internet	m		

7. Click **Next** and navigate to **WAN Links** tab. Click **+ WAN Link** and select the **Create New** radio button. Add two WAN links; One for MPLS and one for Internet.

To add an internet WAN link, select **Public Internet** as the **Access Type**. Provide an ISP name for the WAN link, select the speed. Select **Internet** from the **Virtual Interface** drop-down list. Enter the IP address of the access interface and the gateway. Click **Done**.

WAN Link Attributes	_				
Access Type *	ISP Name *	Custom	Internet Category		
Public Internet	 ✓ ACT 	\sim	Internet	~	
ink Name *	Tracking IP Add	iress			
Internet-ACT-1					
Public IPv4	Address Public	Pv6 Address			
Auto Detect E.g. a.	b.c.d E.g	g. 2001:0db8:85a3	3:0000:0000:8a2e:	0370:7334	
Egress		Ingress			
Speed *	Mbps 🗸	Speed *		Mbps 🗸	
20		20			VLAN-20
Permitted Rate Auto Le	arn 🗹 Physical Rate	Permitted Rate	Auto Learn	Physical Rate	VLAN-10
100		100			1/4
Access Interfaces					
Access Interface Name	Virtual Interface*		Virtual Path Mode*		
AIF-1	Internet	~	Primary	~	
P Address	● V4 ○ V6	Gateway IP Address	•		San Jose Data Cente
192.168.2.10		192.168.2.1			SDWAN-4100 (Primar
Bind Access Interface to G	ateway MAC Enab	le Proxy ARP			
nable Internet Access on					
outing Domain(s)					

To add an MPLS WAN link, from the **WAN links**^{*} tab, click **+ WAN Link** and select the **Create New** radio button. Select **MPLS** as the **Access Type**. Select the ISP Name and the name of the WAN link gets populated automatically. Select speed and choose the MPLS from the **Virtual Interface** drop-down list. Enter the IP address of the access interface and the gateway. Click **Done**.

Verify Config	01 Site Details	02 Device Details	Device Details Interfaces WAN Links		05 Routes	06 Summary
+ WAN Link						
WAN Link Name	Speeds	Access Interface IF	Gateway IP	Actions		
MPLS	100 Mbps† 100 Mbps↓	192.168.1.10	192.168.1.1	Ē		
INET	20 Mbps† 20 Mbps↓	192.168.2.10	192.168.2.1	m		

 Click Next and navigate to Routes > IP Routes tab. Add a route on the SD-WAN appliance on how to reach the LAN Subnets (10.10.11.0/24, 10.10.12.0/24, 10.10.13.0/24, and so on) through any of the physical interfaces. Click Save. Repeat this step to add more routes.

Application Routes IP Routes			
Cost Ranges: Custom Application (1-20) Ap	plication (21-40) Application Group (41-	60) IP (1-65535)	
IP Protocol Match Criteria			
Destination Network*	Routing Domain		
10.10.11.0/24	<default></default>		
Traffic Steering			
Delivery Service Cost*			
Local \checkmark 5			
Eligibility Criteria			
🗹 Export Route	gibility Based on Gateway	mmary Route	
Gateway IP			
Site	Gateway IP		
San Jose Data Center	192.168.1.1		
Eligibility Based on Path			
Add Path			
Site Name	From Wan Link	To Wan Link	Actions
Cancel Save			
Application Routes IP Routes			
Cost Ranges: Custom Application (1-20) Ap	plication (21-40) Application Group	41-60) IP (1-65535)	
+ IP Route	Search for Route	Q	
No Destination Network Delivery Serv	ice Routing Domain	Sites	Cost Actions
1 10.10.11.0/24 Local	<default></default>	San Jose Data Center	5 💼
2 10.10.13.0/24 Local	<default></default>	San Jose Data Center	5 💼
5 10.10.12.0/24 LOCAL	<derault></derault>	San Jose Data Center	5 🛄

9. Click **Save** and then **Verify** to validate the configurations. If any errors observed, fix them before proceeding further.

Azure Virtual WAN

October 26, 2021

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

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

Microsoft Azure Virtual WAN offers the following advantages:

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

Hub-to-Hub communication

From 11.1.0 release onwards, Azure Virtual WAN supports hub-to-hub communication using **Standard** type method.

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

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

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

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

There are two types of Virtual WAN:

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

Create Azure Virtual WAN service in Microsoft Azure

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

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

≡	Microsoft	Azure 🔎 🤉	Search resources, ser	vices, and docs (G+/)				۶.	Ş	Q	ŝ	?
		Azure servic	es										
			_		\diamond	Ŷ	.	<·>		I			
			Virtual WANs	Resource groups	Azure Active Directory	Subscriptions	Virtual machines	Virtual networks	Virtual ne gatewa	twork ays		Policy	

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

Note

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

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

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

Home > New > Virtual WAN >			
Create WAN			
Basics Review + create			
The virtual WAN resource represents a virtu more	al overlay of your Azure n	etwork and is a collection of multiple resources.	Learn
Project details			
Subscription *	Demo Center -		\sim
Resource group *	RG_AzureVirtualWAN		\sim
	Create new		
Virtual WAN details			
Resource group location *	West US		\sim
Name *	AVWAN_USWEST		
Туре 🛈	Standard		~

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

The deployment of the resource takes less than a minute.

Note

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

Create a Hub in the Azure Virtual WAN

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

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

Home > Virtual WANs >				
Virtual WANs « Citrix Systems, Inc.	KING AVWAN_USWEST H	lubs		
+ Add ≡≡ Edit columns ····	P Search (Ctrl+/) 《	+ New Hub 💍	Refresh	
Filter by name	📀 Overview	P Search for hut	os by name Clear a	II filters
	 Activity log Access control (IAM) 	+ ₇ Add filter		
AVWAIN_03WEST	🧳 Tags	Hub	Hub status	Regio
	Settings	No results		
	e Configuration			
	Properties			
	🔒 Locks			
	Export template			
	Connectivity			
	₩ Hubs			
	VPN sites			
	LUSER VPN configurations			
	A ExpressRoute circuits			
	Φ Virtual network connections			

- 3. Under **Basic**, provide the values for the following fields:
 - **Region** –Select the Azure region from the drop-down list.
 - Name Enter the name for the new Hub.
 - **Hub private address space** –Enter the address range in CIDR. Select a unique network that is dedicated for the hub only.
- 4. Click **Next: Site to Site >** and provide the values for the following fields:
 - Do you want to create a Site to site (VPN gateway)? -Select Yes.
 - Gateway scale units –Select the scale units from the drop-down list as needed.

Home > Virtual WANs > AVWAN_USWEST Hubs >							
Create virtual hub							
Basics Site to site Point to site	ExpressRoute	Tags	Review + create				
You will need to enable Site to site (VPN gateway) before connecting to VPN sites. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. Learn more							
Do you want to create a Site to site (VPN gateway)?	Yes No						
AS Number i	65515			٥			
*Gateway scale units ①	1 scale unit - 500	Mbps x 2	2	~			

5. Click **Review + create**.

6. Review the settings and click **Create** to start the virtual hub creation.

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

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

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

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

Note

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

Perform the following steps to create an application registration:

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



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

Home > Citrix Systems, Inc. App re	gistrations >
Register an applicati	on
5	
* Name	
The user-facing display name for this a	pplication (this can be changed later).
AZUKE_API	
Supported account types	
Who can use this application or acces	s this API?
Accounts in this organizational dir	ectory only (Citrix Systems, Inc. only - Single tenant)
Accounts in any organizational dir	ectory (Any Azure AD directory - Multitenant)
Accounts in any organizational dir	ectory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
Help me choose	
Redirect URI (optional)	
We'll return the authentication response	e to this URI after successfully authenticating the user. Providing this now is optional and it can be
changed later, but a value is required for	or most authentication scenarios.
Web 🗸	https://localhost:4980
By proceeding, you agree to the Micro	soft Platform Policies 🖻
Register	

You can copy and store the **Application (client) ID** and the **Directory (tenant) ID** that can be used in the Citrix SD-WAN Orchestrator service for authentication to the Azure subscription for usage of the API.

Home > Citrix Systems, Inc. App registrations >						
🜉 Azure_api 🖉						
	💼 Delete 🌐 Endpoints					
😽 Overview	Display name : AZURE_API	Supported account types : My organization only				
📣 Quickstart	Application (client) ID : solicoper 1470 feed, and 17001 400-577	Redirect URIs : 1 web, 0 spa, 0 public client				
🚀 Integration assistant (preview)	Directory (tenant) ID : Disastelle 22 das das 34802 esteroit	Application ID URI : Add an Application ID URI				
	Object ID : 188-664955 200 4849	Managed application in I : AZURE_API				
Manage	*					
Branding						
Ə Authentication	Welcome to the new and improved App registrations. Looking to learn how it's changed from the second sec	m App registrations (Legacy)? Learn more				

The next step for the application registration, create a service principal key for authentication purposes.

To create the service principal key, perform the following steps:

- a) In the Azure portal, navigate to **Azure Active Directory**.
- b) Under Manage, navigate to App registration.

- c) Select the registered application (created previously).
- d) Under Manage, select Certificates & secrets.
- e) Under **Client secrets**, click + **New client secret**.

Home > Citrix Systems, Inc. App re	egistrations > ificates & secrets 🛛 🖈		
 <i>P</i> Search (Ctrl+/) Sverview 	Credentials enable confidential application scheme). For a higher level of assurance, to	ns to identify themselves to the authentication service w we recommend using a certificate (instead of a client sec	hen receiving tokens at a web addressable location (using an HTTPS ret) as a credential.
Quickstart Integration assistant (preview) Manage	Certificates Certificates can be used as secrets to prov	ve the application's identity when requesting a token. Al	so can be referred to as public keys.
Branding	Thumbprint	Start date	Expires
Authentication	No certificates have been added for this a	application.	
📍 Certificates & secrets			
Token configuration			
API permissions	Client secrets		
Expose an API	A secret string that the application uses to	o prove its identity when requesting a token. Also can be	e referred to as application password.
B Owners	+ New client secret		
Roles and administrators (Preview)	Description	Expires	Value
Manifest	No client secrets have been created for the	his application.	
Support + Troubleshooting			
Troubleshooting			
New support request			

- f) To add a client secret, provide values for the following fields:
 - **Description**: Provide a name for the service principal key.
 - **Expires**: Select the duration for expiration as needed.

Add a clien	t secret		
Description			
SP_KEY			
Expires In 1 year In 2 years Never Add	Cancel]	

- g) Click Add.
- h) The client secrete is disabled in the **Value** column. Copy the key to your clipboard. This is the Client Secret that you must enter into the Citrix SD-WAN Orchestrator service.



Note

Copy and store the secret key value before reloading the page because, it will no longer be displayed afterwards.

Perform the following steps to assign the appropriate roles for an authentication purpose:

- 1. In the Azure portal, navigate to the **Resource Group** where the Virtual WAN was created.
- 2. Navigate to Access control (IAM).
- 3. Click + Add and select Add role assignment.



4. To add role assignment, provide values for the following fields:

- **Role** –Select Owner from the drop-down list. This role allows management of everything including access to resources.
- Assign access to -select Azure AD user, group, or service principal.
- **Select** Provide the name of the registered application created earlier and select the corresponding entry when it appears.
- 5. Click Save.

Add role assignm	ient ×
Role 🙃	
Owner ①	~
Assign access to ①	
Azure AD user, group, or servi	ce principal 🗸 🗸 🗸
Select (i)	
Azure_API	
No users, groups, or service p	rincipals found.
Selected members:	
	Remove
Save Discard	

Lastly, you need to obtain the Subscription ID for the Azure account. You can identify your **Subscription ID** by searching for Subscriptions in the Azure portal.

Home > Subscriptions & Citrix Systems, Inc.							
+ Add							
View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, click here Showing subscriptions in Cliric Systems, Inc. directory. Don't see a subscription? Switch directories Status O Status O							
8 selected			3 selected				
Apply Showing 1 of 5 subscriptions velocited in the global subscriptions filter O							
Subscription name	Subscription ID	¢↓	My role		Current cost	Status	
😐 Demo Center - Gibise Microsoft Joint Denta			Owner		Not available	Active	

Configure Azure Virtual WAN Delivery Service in Citrix SD-WAN Orchestrator service

Microsoft Azure Virtual WAN and Citrix SD-WAN provide simplified network connectivity and centralized management across cloud workloads. This service provides automatic configuration of branch appliances to connect to the Azure Virtual WAN and configure branch traffic management policies according to your business requirements.

Provide the Azure Service Principal information to map any Citrix SD-WAN sites to Azure Virtual WAN. Before configuring the sites to an Azure Virtual WAN service, you need to create the Azure Virtual WAN Hubs with site-to-site connectivity gateway resource in your respective Azure region. Site-to-site connections are established between Citrix SD-WAN appliances and Azure.

Note

Only the Virtual WAN hubs created in the Azure portal for your subscription are listed for mapping.

As part of mapping Citrix SD-WAN branches to Azure Virtual WANs, a branch site needs to be associated with Azure WAN resources to establish IPsec tunnels with the Azure Virtual Hubs using the preselected IPsec IKE/IPsec settings. The Sites and Azure backbone routes are learned over BGP by default. When Citrix SD-WAN branch sites have multiple internet WAN links configured, two WAN links are automatically chosen to provide redundancy. The chosen Citrix SD-WAN software must have the support to switch between primary and secondary IPsec tunnels, which are supported from the 11.1 release onwards.

Note

One Citrix SD-WAN site can connect to multiple Azure Virtual Hubs in the same or different Azure regions.

Certain Citrix SD-WAN appliances have resource limitation on the number of IPsec tunnels that can be supported. Hence the configuration mapping might fail, if the Citrix SD-WAN appliance tunnel count restrictions are not met.

The following are the IPsec tunnel limit per SD-WAN platform:

SD-WAN appliances	IPsec Tunnels supported
4100, 5100, 6100	256
1100, 2100	128
110, 210, 410, 1000, 2000	8

Prerequisites

Perform the following prerequisites before beginning the configuration in the Citrix SD-WAN Orchestrator service:

- Complete setup of Azure infrastructure (peer VNet with Hub, registered application for automation, and so on)
- Obtain access to Citrix SD-WAN Orchestrator service as a cloud-hosted service. Ensure to use a Citrix Cloud account that has gone through the proper onboarding process, otherwise the authentication fails.
- Ensure that the Azure subscription is not already in use with any other Citrix SD-WAN Orchestrator service configuration.
- Have already deployed MCN and branch SD-WAN nodes and confirm Virtual Path over Internet WAN link types. Citrix SD-WAN Orchestrator service automatically enables Intranet Service through the configuration process.
- Ensure that the branch SD-WAN nodes are set to auto-learn the Internet WAN link's Public IP address.

Perform the following to complete the configuration of Azure Virtual WAN and establish the IPsec tunnels with SD-WAN devices:

On Citrix SD-WAN Orchestrator service, from the customer level, navigate to **Delivery Channels** > Bandwidth Alocation. Allocate a percentage of bandwidth for the Azure Virtual WAN delivery service (for example, 20%). You might have to subtract the allocated percentage from any of the other delivery services (for example, Virtual Path), so that the total allocated percentages equal 100.

Bandwidth Allocation

	Delivery Services	Global Service Bandwidth Defaults for each Link type								
		Internet Links		MPLS Links		Private Intranet Links		t Links		
Virt	ual Path	ţ	50	96		100	96		100	%
Inte	rnet	Ę	5	96		0	96		0	96
Sec	ure Internet Access Service	ŧ	5	96		0	96		0	%
Clo	ud Direct Service	(%		0	%		0	%
Intr	anet	4	40	96		0	96		0	96
1.	Zscaler	1	10	96		0	96		0	96
2.	Azure Virtual WAN		10	96		0	%		0	96
		-				0			0	

Note

Provide the subscription bandwidth (in %) for the Azure Virtual WAN service. You can reserve the subscription bandwidth both at global (**All Sites > Configuration > Delivery Channels > Bandwidth Allocation**) and site (**Site > Site Configuration > WAN Links > Services**) level.

Optionally, one can also allocate different bandwidth for different sites. For this, perform a link specific configuration for the selected site. To do this, select the appropriate **Site > WAN Links tab > Services** section. You can overwrite the global bandwidth allocation by selecting **Link Specific** for **Service Bandwidth Settings** and allocating the desired bandwidth.

Services			
Service Bandwidth Se	ettings : Link Specif	ic ∨	
+ Service			
Service Name	Allocation %	Actions	Services Allocation
Azure Virtual WAN	50%	ø 🖻	
Virtual Path	50 %	ø 🗊	
			Azure Virtual WAN (50%) 🗖 Virtual Path (50%)

 From the customer level, navigate to Configuration > Delivery Channels. In the SaaS and Cloud On-Ramp Services section, click the Azure Virtual WAN tile. The Azure Virtual WAN page is displayed.

You can also navigate to **Azure Virtual WAN** page from **Configuration > SaaS & Cloud On Ramp > Azure Virtual WAN**.

← Az	ure Virtual WAN				
Add Sites				Refresh Aut	thentication Delete All
Info	Site Name	Virtual WAN	Hubs	Status	Actions
0	CB210	AzureVWAN	1	Site Provisioning Success	
0	CB2100site	AzureVWAN	1	Site Provisioning Success	
0	dmzpod6 Clone 1 2 3	AzureVWAN	1	Site Provisioning Success	
				Page Size: 50 V Showing 1-3 of 3 items	Page1 of1 🚽 🕨 🕨
Done					

- 3. On the top right corner of the Azure Virtual WAN page, click the Authentication link.
- 4. Provide Azure **Subscription ID, Client ID, Client Secret,** and **Tenant ID** captured earlier during the creation of the Azure service principal. If the credentials are not correct, then the authentication fails and further action is not allowed. Click **Save**.

Azure Authentication		
Subscription ID *		
Client ID *		
Client Secret *		
Tenant ID *		
	Cancel	Save

After authentication is successful, you must associate a branch site with Azure Virtual WAN resources to establish IPsec tunnels. One Branch can be connected to multiple Hubs within an Azure Virtual WAN resource and one Azure Virtual WAN resource can be connected with multiple branch sites.

Note

You can clear the authentication settings by clicking the **Clear Authentication** link. Ensure that you delete the site mappings before deleting the authentication.

5. After successful Azure authentication, click Add Sites to add a site.

n ve	rify Config Service & Bandwidth	2			
Azure Virtu	al WAN				
+ Site				2 Ref	resh 👷 Authentication
Info	Site Name	Virtual WAN	Hubs	Status	Actions
Done					
Note					
The Add	 Sites option is disal	bled if you have not i	reserved the	subscription	bandwidth.
	6 H 1 1 1 1 1				

- 6. Provide the following details:
 - Filter by Region/Custom Groups You can select all or selective region/groups.
 - Select Sites You can select all or selective sites that you want for mapping.

	Verify Config Servi	ce & Bandwidth			
Azure \	firtual WAN				
+ Sit	e			ł	C Refresh Authentication
Info	Site Name	Virtual WAN	Hubs	Status	Actions
Don	e				

- **Azure Virtual WAN** Select the Azure Virtual WAN from the drop-down list that is associated with the subscription. Same site cannot be connected to multiple WANs.
- **Azure Hubs** Select the Azure hubs. Only Azure Virtual WANs with Azure Virtual hubs are listed for mapping. You can add multiple hubs connected to the same site.

Note

The **Azure Virtual WAN** field lists the virtual WANs that have a corresponding hub already created.

ALB Internal IP –The Azure Load Balancer (ALB) IP input is required if the particular site is an Azure VPX and deployed in a High Availability (HA) mode. Else this field is optional.

- 7. Click Save
- 8. Once the site is deployed, you can see the following information:

Note: Make sure to allocate bandwidth globally or specific to site		
🕤 Edit Azure Virtual WAN		
Azure Virtual WAN*	Azure Hubs*	
AzureVWAN V	Hub1 X	~
Site Name		ALB Internal (PC)
dmzood6 Clone 1 2 3		
Save Cancel		

The following diagram describes the high-level workflow of Citrix SD-WAN Orchestrator service and Azure Virtual WAN connection.



- Info Displays the Azure Virtual WAN Tunnel configuration details and status.
- Site Name Displays the deployed site name.
- Virtual WAN Displays the Azure Virtual WAN the corresponding site is mapped with.
- Hubs Displays the number of hubs.
- **Status** –Displays the different deployment states with the completion message. If the site is provisioned successfully, then only the IPsec tunnels can be created.
- Action You can Edit or Delete the configured site.

lit Azure Virtual	WAN			
usi wan "		Azure Hubs *		
eVWAN		V IduH X	~	
ame		ALB Internal IP()		
od6 Clone 1 2 3				
Ve Cancel				
Azure Virti	ual WAN Tunnel Conf	iouration and Status		
Larc met		iguiddon and status		
ite Info	Site : OnPrem210LTE	Local IPs : 172.17.31.2	Public IPs : 172.17.31.2	
Poor Info - Hut	Config 1 Pagion	West LIS	12 06 241 127 12 06 240 166	PCP ID 100112 100112
eer into - Huu	comg_i Region.	West 05 IF.	15.80.241.127, 15.80.240.100	DGF IF . 10.0.1.15, 10.0.1.12
	BGP ASM	1:65515		
	BGP ASM	1:65515		
	BGP ASM	1:65515		
psec Config	BGP ASM Ike Version : ikev2	I : 65515 Ike Encryption : aes256	Ike HASH Algorithm :	lke Integrity : sha256
psec Config	BGP ASM Ike Version : ikev2	I : 65515 Ike Encryption : aes256	Ike HASH Algorithm : sha256	Ike Integrity : sha256
psec Config	BGP ASM Ike Version : ikev2 DH Group : group2	I : 65515 Ike Encryption : aes256 Ike Authentication : psk	Ike HASH Algorithm : sha256 Ike DPD Timeout : 300	Ike Integrity : sha256
psec Config	BGP ASM Ike Version : ikev2 DH Group : group2	I : 65515 Ike Encryption : aes256 Ike Authentication : psk	Ike HASH Algorithm : sha256 Ike DPD Timeout : 300	Ike Integrity : sha256 Ipsec Tunnel type : esp
psec Config	BGP ASM Ike Version : ikev2 DH Group : group2 Ipsec Encryption :	I : 65515 Ike Encryption : aes256 Ike Authentication : psk PFS Group : none	Ike HASH Algorithm : sha256 Ike DPD Timeout : 300 Mismatch Behaviour : dro	Ike Integrity : sha256 Ipsec Tunnel type : esp P
psec Config	BGP ASM Ike Version : ikev2 DH Group : group2 Ipsec Encryption : aes256gcm128	I : 65515 Ike Encryption : aes256 Ike Authentication : psk PFS Group : none	Ike HASH Algorithm : sha256 Ike DPD Timeout : 300 Mismatch Behaviour : dro	lke Integrity : sha256 Ipsec Tunnel type : esp p
psec Config	BGP ASM Ike Version : ikev2 DH Group : group2 Ipsec Encryption : aes256gcm128	I : 65515 Ike Encryption : aes256 Ike Authentication : psk PFS Group : none	Ike HASH Algorithm : sha256 Ike DPD Timeout : 300 Mismatch Behaviour : dro	lke Integrity : sha256 Ipsec Tunnel type : esp P
psec Config	BGP ASM Ike Version : ikev2 DH Group : group2 Ipsec Encryption : aes256gcm128	I : 65515 Ike Encryption : aes256 Ike Authentication : psk PFS Group : none	Ike HASH Algorithm : sha256 Ike DPD Timeout : 300 Mismatch Behaviour : dro	Ike Integrity : sha256 Ipsec Tunnel type : esp

Mapping of Citrix SD-WAN sites to Azure Virtual WAN hubs might take some time since it involves downloading IPsec configuration from Azure. The branch mapping status shows as **Configuration Downloaded** after the branch configuration is downloaded. It is recommended to refresh the site status before you activate the configuration to see the updated status.

Once the site is successfully provisioned, you need to perform the **Verify, Stage,** and **Active** process to create the IPsec tunnels.

poardsdcustomer	/ All Site	tes 🗡					
Dashboard							
Reports	>	L Veri	Current Deploy	ment Deployment History Chan	ge Management Settings		
Configuration Network Config Home	~	Software Ver	rsion : 1111139				
Delivery Services	>	Stage		Activate 🗸			
Routing	>						
Link Settings	>				fite and the life and		4/4
QoS	>				Staged Appliances		
Security	>			,	Activated Appliances		4/4
Site & IP Groups	>	Total Appliance	tes	Staged	Activated	Failed	
App & DNS Settings	>	4		4	4	0	
Profiles & Templates		Online	Site	Status		HA State	Software Version
		Yes	DC	Activation Complete		Not Configured	11.1.1.39.859699
Troubleshooting	>	Yes	BR1	Activation Complete		Not Configured	11.1.1.39.859699
		Yes	Home110LTE	Activation Complete		Not Configured	11.1.1.39.859699
	/	Yes	OnPrem210LTE	Activation Complete		Not Configured	11.1.1.39.859699
Administration							

After activation, you can see the state of the tunnels for each site by navigating to **All Sites > Reports > Real Time > Statistics > IPsec Tunnel**, select the desired site, then click **Retrieve latest data**. If the configuration is not activated, the tunnels information will not be available. Two tunnels are created for the purpose of redundancy.

Customer Site onboardsdcustomer / All	Sites Y
Dashboard	Network Reports : Real Time Statistics
Alerts	ARP Routes Virtual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS IPsec Tunnel ~
Usage Inventory Security	On Prem210LTE Retrieve latest data Search Q Name State Service Type Packets Received Kbps Received Packets Sent Packets Dropped By
Quality	azureVWANSenvice_1 GOOD Intranet 17 0.50 7 0.22 0 0
Gos Historical Statistics	azureVWANSenvice_2 GOOD Intranet 16 0.47 7 0.21 0 0
Real Time Statistics Flows	1 to 2 of 2 - i < < Page 1 of 1 > >i
Firewall Connections	

Also, you can see the routes to Azure Virtual WAN for each site by navigating to **All Sites > Reports > Real Time > Statistics > Routes**, select the desired site, then click **Retrieve latest data**.

Customer onboardsdcustomer /	Site All Sit	tes 🗠												C
Dashboard		Network	Reports : Real T	ime Statistics								Site Gro	oup: All	
Alerts	~	ARP	Routes Virtual Path	Services Classes	Ethernet Observed P	rotocols Wan Path	Application Q	os Other Stats 🛩						
Usage Inventory Security Quality	>	OnPrem routes_Def	210LTE V	Retrieve latest data Gateway IP Address	Service 👃	Firewall Zone	Reachable	Site IP Address	Site	Туре	Protocol	Neighbor Direct	Search	Q, Hit Count
QoS		0	10.0.1.12/32		azure/WANService 2	Default LAN Zone	YES		OnPrem210LTE	Static			5	1961
Historical Statistics		3	13.86.240.166/32		azure/WANService_2	Default LAN Zone	YES		OnPrem210LTE	Static			6	26700
Real Time	~	9	10.0.1.0/24		acure/WANService_2	Default_LAN_Zone	YES		OnPrem210LTE	Dynamic	BGP		13	0
Statistics		1	10.0.1.13/32		acure/WANService_1	Default_LAN_Zone	YES		OnPrem210LTE	Static			5	1976
Flows		2	13.86.241.127/32		azure/WANService_1	Default_LAN_Zone	YES		OnPrem210LTE	Static			5	26695
riows		14	0.0.0.0/0		Passthrough	Any	YES			Static			65535	0
Firewall Connections		4	172.17.31.0/24		Local	Default_LAN_Zone	YES		OnPrem210LTE	Static			5	0
Cloud Direct		12	0.0.0.0/0		Internet	Untrusted_Internet_Zon	YES		OnPrem210LTE	Static			5	0
Application Quality (prev	iew)	15	0.0.0.0/0	•	Discard	Any	YES			Static	-		65535	0
O365 Metrics		5	172.16.150.0/24	•	DC-OnPrem210LTE	Default_LAN_Zone	YES		DC	Dynamic	Virtual_WAN	YES	10	0
		6	172.16.250.0/24		DC-OnPrem210LTE	Default_LAN_Zone	YES		DC	Dynamic	Virtual_WAN	YES	10	0
		7	172.16.251.0/24		DC-OnPrem210LTE	Default_LAN_Zone	YES		DC	Dynamic	Virtual_WAN	YES	10	0
Onfiguration	1	8	172.30.200.0/24		DC-OnPrem210LTE	Default_LAN_Zone	YES		DC	Dynamic	Virtual_WAN	YES	10	0
		10	172.16.1.0/24	•	DC-OnPrem210LTE	Default_LAN_Zone	YES	•	BR1	Dynamic	Virtual_WAN	NO	15	0
C Troubleshooting	>	11	172.16.100.0/24	•	DC-OnPrem210LTE	Default_LAN_Zone	YES	•	BR1	Dynamic	Virtual_WAN	NO	15	0
		13	0.0.0.0/0		DC-OnPrem210LTE	Default_LAN_Zone	YES		DC	Dynamic	Virtual_WAN	YES	11	0

During the initial configuration of Azure Virtual WAN, the 10.0.1.0/24 VNet is associated, and this route has been learned by the on-premises SD-WAN and enter into the route table with **azureVWANservice** as the delivery service type. Type indicating **Dynamic** and Protocol indicating **BGP** can be determined that the route was learned dynamically over BGP.

In the Azure portal, successfully deployed VPN sites can be monitored in the Azure Virtual WAN hub. Also, you will find the Address Space associated with the Hub that was learned by the on-premises SD-WAN device.

Microsoft Azure	و مر	earch resources, services, and de	ocs (G+/)				5 5 0 0 ?	😳 shoaib.yusuf@citrix.com
Home > Virtual WANs > Virtual WANs « Citri System, Inc. + Add III Edit columns ···	AVWAN_USWEST H Votual WAN	lubs + New Hub 🖒 Refresh						
Filter by name	Overview Activity log Access control (AMA)	P Search for hubs by name ↑ Add filter						
🐨 AVWAN_USWEST 🛛 😶	🔶 Tags	Hub	Hub status	Region	VPN sites	Address Space	Point-to-site	ExpressRoute Circuits
	Settings	★ HUB_USWEST	Succeeded	West US	2 VPN site(s)	10.0.1.0/24	No P2S gateway	No ExpressRoute gateway
	Configuration							
	Properties							
	🔒 Locks							
	Export template							
	Connectivity							
	💥 Hubs							
	VPN sites							
	Liser VPN configurations							
	A ExpressRoute circuits							
	Virtual network connections							
	Monitor							

Selecting any of the connected VPN sites provides detail of the connected SD-WAN. Including the public IP Address/FQDN that terminates the IPsec tunnel, the private IP address space, and the BGP address that would be the SD-WAN's WAN interface VIP address, and more importantly the speed and connectivity status to the hub.

Home > Virtual WANs > AVWAN_USWEST Hubs > Sites >								
• OnPrem210LTE	Â							×
P Search (Ctrl+/)		🖉 Edit site						
🔆 Overview		Name OnPrem210LTE			Private address sp 172.17.31.0/24	ace		
		Location westus			Device vendor Citrix			
		Resource group RG_AzureVirtualWAN			BGP Enabled			
		Subscription Demo Center	eccelereini - 2014					
					*			
		Connected Hubs						
		Hub name		Location		Connectivity status		
		一一 HUB_USWEST		West US		Connected		
		Links						
		Link name	Provider name	Speed	IP address / FQDN	BGP address	ASN	
		OnPrem210LTE	ISP	1 Mbps	(11) X 2 4 2 5 5 7	172.17.31.2	20334	

In Azure, virtual network connections can be added to make available resources in Azure by connecting VNets. To complete this configuration, perform the following:

- 1. In the Azure portal, select the Virtual WAN resource.
- 2. Under Connectivity, navigate to Virtual network connections.
- 3. Click + Add connection.



- 4. To add connection, specify values for the following fields:
 - **Connection name** Enter the name for the new connection.
 - Hubs Select from the available hubs in the drop-down list.

- Subscription Select from the available subscriptions in the drop-down list.
- **Resource group** –Select the resource group from the drop-down list where the Virtual WAN resource is deployed.
- Virtual network Select from the available virtual networks in the drop-down list.

Add connection			
Some of the functionality may not be access	ssible as it is currently being rolled out and exp	ected to complete in the week of Aug 3rd.	
Connection name *			
VNET2_TO_HUB			
Hubs * 🛈			
HUB_USWEST			
Subscription *			
Demo Center - Cables Editorett Bir arternet	8		$\mathbf{\vee}$
Resource group *			
RG_AzureVirtualW/AN			
Virtual network *			
VNET2_AVWAN			
Routing configuration ()			
Propagate to Route Tables			
Static routes ①			
Route name	Destination prefix	Next hop	
Create			

5. Click Create.



With the new VNet peered to the Hub, on-premises SD-WAN devices are dynamically learned the new

route through BGP. To retrieve the latest route table for the SD-WAN device in Citrix SD-WAN Orchestrator service, navigate to **All Sites > Reports > Real Time > Statistics > Routes**. Select the desired site and click **Retrieve latest data**.

Customer Sit onboardsdcustomer / A	e Il Sites	~										0
🖓 Dashboard	N	etwork R	eports : Real Ti	me Statistics						Site	Group: All	~
Alerts Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS Other Stats Vitual Path Services Classes Ethernet Observed Protocols Wan Path												
Inventory Security	Ę	OnPrem21	10LTE V Re ult_RoutingDomain	trieve latest data]						Search	٩
Quality		Num	Network Address	Gateway IP Address	Service 👃	Firewall Zone	Reachable	Site IP Address	Site	Туре	Protocol	Neigh
Q05		1	10.0.1.12/32		azureVWANService_2	Default_LAN_Zone	YES	•	OnPrem210LTE	Static	-	-
Historical Statistics	1-1	2	12 06 240 166/22		anural OAM Artical Carlos 2	Datasta LAN, Zona	724		OnBrand 210/TE	Cruzia		
Real Time 🗸		10	10.0.2.0/24		azureVWANService_2	Default_LAN_Zone	YES		OnPrem210LTE	Dynamic	BGP	
Statistics			10.0.1.0/24		azurev wansennce_2	Default_LAN_2016	TES		UNPREM 2 TULLE	Dynamic	BGP	
Flows		0	10.0.1.13/32	•	azureVWANService_1	Default_LAN_Zone	YES	•	OnPrem210LTE	Static	-	-
Firewall Connections		2	13.86.241.127/32	•	azureVWANService_1	Default_LAN_Zone	YES	•	OnPrem210LTE	Static	-	
Priewaii Conneccions		9	10.0.2.0/24		azureVWANService_1	Default_LAN_Zone	YES	•	OnPrem210LTE	Dynamic	BGP	
Cloud Direct		16	0.0.0.0/0		Passthrough	Any	YES	•	•	Static		
Application Quality (preview)		4	172.17.31.0/24	•	Local	Default_LAN_Zone	YES	•	OnPrem210LTE	Static		
0365 Metrics		14	0.0.0.0/0	•	Internet	Untrusted_Internet_Zon	YES		OnPrem210LTE	Static		
sees months		17	0.0.0.0/0		Discard	Any	YES			Static	-	
		5	172.16.251.0/24		DC-OnPrem210LTE	Default_LAN_Zone	YES		DC	Dynamic	Virtual_WAN	YES
Onfiguration >		6	172.16.150.0/24		DC-OnPrem210LTE	Default_LAN_Zone	YES		DC	Dynamic	Virtual_WAN	YES
		7	172.16.250.0/24		DC-OnPrem210LTE	Default_LAN_Zone	YES		DC	Dynamic	Virtual_WAN	YES
Troubleshooting >		8	172.30.200.0/24		DC-OnPrem210LTE	Default_LAN_Zone	YES	•	DC	Dynamic	Virtual_WAN	YES
					0.0 0 0 040 FF		1.000			A		

Citrix SD-WAN deployed VPN sites can access resources deployed in VNets peered to the Azure Virtual WAN Hubs through the previously mentioned configuration steps.

Citrix SD-WAN integration with Google Network Connectivity Center

October 27, 2021

Google Network Connectivity Center (NCC) provides a mechanism for enterprises to connect Onpremises, Virtual Private Clouds(VPCs) on Google Cloud, and other enterprise networks and manage them as spokes to a centralized logical hub on Google Cloud.

Citrix SD-WAN's integration with Google NCC provides a fast, secure, and resilient on-ramp for organizations to connect and migrate data from their branch offices, remote sites, and on-premises networks to Google Cloud. In addition, enterprises can use Google's high-speed internet backbone to connect to workloads and other branch offices.

For information on how to integrate Citrix SD-WAN with Google NCC, see Citrix SD-WAN for Google Network Connectivity Center Deployment Guide.

SD-WAN configuration for Citrix Virtual Apps and Desktops Standard for Azure integration

March 8, 2021

Citrix SD-WAN is a next-generation WAN edge solution that accelerates digital transformation with flexible, automated, and secure connectivity and performance for SaaS, cloud, and virtual applications to ensure an always-on workspace experience.

Citrix SD-WAN is the recommended and best way for organizations to connect to Citrix Virtual Apps and Desktops Standard for Azure with a quick and easy set-up. For more information, see Citrix blog.

Benefits

- Easy to set up SD-WAN in Citrix Virtual Apps and Desktops Standard for Azure through a guided and automated workflow
- Always-on, high performance connectivity through advanced SD-WAN technologies
- Benefits across all connections (VDA-to-DC, user-to-VDA, VDA-to-cloud, and user-to-cloud)
- Reduces latency compared to backhauling traffic to the data center
- Traffic management to ensure Quality of Service (QoS)
 - QoS across HDX/ICA traffic streams (single-port HDX AutoQoS)
 - QoS between HDX and other traffic
 - HDX QoS fairness between users
 - End-to-end QoS
- Link bonding delivers more bandwidth for faster performance
- High Availability (HA) with seamless link failover and SD-WAN redundancy on Azure
- Optimized VoIP experience (packet racing for reduced jitter and minimal packet loss, QoS, local break-out for reduced latency)
- Major cost savings and much faster and easier to deploy compared to ExpressRoute

Pre-requisites

To evaluate these new capabilities, the following pre-requisites must be adhered to:

 You must have an existing SD-WAN network with Citrix SD-WAN Orchestrator service entitlement. If you don't have an existing SD-WAN network then you must set up one using Citrix SD-WAN Orchestrator service. For more details, see configuring a Master Control Node (MCN).

- 2. You must have a subscription to Citrix Virtual Apps and Desktops Standard for Azure.
- 3. Currently, this integration support is only available for customers. If you are a partner or an MSP and must try this service then you must subscribe to Citrix Virtual Apps and Desktops Standard for Azure as a customer. Only then this integration can be enabled.
- 4. To use SD-WAN features (such as QoS for MSI, application visibility), the Network Location Service (NLS) must be configured for all the SD-WAN sites in your network.
- 5. You must have a DNS server and AD either deployed where the client endpoints are present (colocated in your data center environment, which would also have the MCN) or you can also utilize Azure Active Directory (AAD).
- 6. The DNS server must be capable of resolving both internal (private) and external (public) IPs.
- 7. Make sure that the FQDN sdwan-location.citrixnetworkapi.net is whitelisted in the firewall. This is the FQDN for network location service which is critical in sending traffic over the SD-WAN virtual path.

For the list of cloud services that has to be whitelisted on the firewall, see Prerequisites for Citrix SD-WAN Orchestrator service usage.

Deployment architecture



Any deployment would feature the following entities:

• An on-premises location hosting the SD-WAN appliance which can either be deployed in branch mode or as an MCN. This location contains the client machines, active directory, and DNS. How-

ever, you can also choose to use Azure's DNS and AD. In most scenarios the on-premises location serves as an on-prem data center and houses the MCN.

- Citrix Virtual Apps and Desktops Standard for Azure cloud service: This entity provides:
 - The UI for enabling and monitoring SD-WAN connectivity for Citrix Virtual Apps and Desktops Standard for Azure.
 - Creates SD-WAN virtual machine instances in Azure.
 - Manages their lifetime.
 - Bundles SD-WAN instance costs with Citrix Virtual Apps and Desktops Standard for Azure costs for customer billing.
 - Configures the local networking environment (subnets, local routing, firewall rules and so on) for SD-WAN instances.
 - Supplies SD-WAN instance information to the Citrix SD-WAN Orchestrator service to provide and consume SD-WAN monitoring and other operational data.
- **Citrix SD-WAN Orchestrator service**: Citrix SD-WAN Orchestrator service provides the UI for SD-WAN management:
 - Including management of instances deployed in Citrix Virtual Apps and Desktops Standard for Azure.
 - Implements initial provisioning for Citrix Virtual Apps and Desktops Standard for Azure SD-WAN instances.
 - Implements restrictions on SD-WAN instance management to reflect the Citrix Virtual Apps and Desktops Standard for Azure configuration.
 - Integrates with Citrix Virtual Apps and Desktops Standard for Azure to provide and consume SD-WAN monitoring and other operational data.
- Virtual and physical SD-WAN appliances: Virtual and physical SD-WAN appliances run as multiple instances within the cloud (VMs), on-premises in the data center, and in the branches (physical appliances or VMs) to provide connectivity among these locations and to/from the public Internet.

SD-WAN instance in Citrix Virtual Apps and Desktops Standard for Azure subscription is created as a single or a set of virtual appliances (if there was HA deployment) by Citrix Virtual Apps and Desktops Standard for Azure cloud service in Azure within the realms of Citrix Virtual Apps and Desktops Standard for Azure subscription. SD-WAN appliances in other locations (DC and branches) are created by the customer. All of these SD-WAN appliances are managed (in terms of configuration and software upgrades) by SD-WAN administrators through the Citrix SD-WAN Orchestrator service.

• Citrix Virtual Apps and Desktops Standard for Azure VDA, Connector - Uses the Citrix Virtual Apps and Desktops Standard for Azure SD-WAN appliance as a gateway to all resources outside

of the Citrix Virtual Apps and Desktops Standard for Azure VNet, including enterprise on-prem resources, certain Azure services, and SaaS applications on the public Internet.

User roles

- 1. **Citrix Virtual Apps and Desktops Standard for Azure Administrator**: Decides to use SD-WAN connectivity and obtains the necessary networking information from the SD-WAN administrator (or another network administrator role):
 - Starts the configuration of SD-WAN connectivity through Citrix Virtual Apps and Desktops Standard for Azure UI.
 - Once SD-WAN connectivity is fully enabled, manages Citrix Virtual Apps and Desktops Standard for Azure catalogs using SD-WAN connectivity.
 - Together with the SD-WAN Administrator, monitors SD-WAN connectivity and takes more actions as necessary.
- 2. **SD-WAN administrator**: Provides SD-WAN configuration information to Citrix Virtual Apps and Desktops Standard for Azure Administrator:
- Activates SD-WAN instances in Citrix Virtual Apps and Desktops Standard for Azure to enable connectivity to other network elements, and performs extra configuration activities.
- Together with the SD-WAN administrator, monitors SD-WAN connectivity and takes extra actions as necessary.



Access management for SD-WAN Citrix Virtual Apps and Desktops Standard for Azure integration

- Both Citrix Virtual Apps and Desktops Standard for Azure and Citrix SD-WAN Orchestrator service rely on Citrix Cloud IDAM to identify users as having **Read-Only** or **Read-Write** access.
- In addition, the Citrix SD-WAN Orchestrator service has the capability to assign similar access
 rights to users exclusively within the Citrix SD-WAN Orchestrator service. The two authorization
 mechanisms are combined with the OR logic: it is sufficient to have admin access rights either
 in Citrix Cloud or in Citrix SD-WAN Orchestrator service to get access to SD-WAN configuration
 management.



Deployment and configuration

In a typical deployment a customer would have the Citrix SD-WAN appliance (H/W or VPX) deployed as an MCN in their data center/large office. The customer data center would usually host on-prem users and resources such as AD and DNS servers. In some scenarios the customer can use Azure Active Directory services (AADS) and DNS, both of which are supported by Citrix SD-WAN and Citrix Virtual Apps and Desktops Standard for Azure integration.

Within the Citrix Managed Azure subscription, the customer needs to deploy the Citrix SD-WAN virtual appliance and VDAs. The SD-WAN appliances are managed through the Citrix SD-WAN Orchestrator service. However, for the purpose of this integration the SD-WAN appliance within the Citrix Managed Azure subscription is configured via Citrix Virtual Apps and Desktops Standard for Azure UI/workflow. Once the SD-WAN appliance gets configured it connects to the existing Citrix SD-WAN network and further tasks such as configuration, visibility, and management are handled through the Citrix SD-WAN

Orchestrator service. Both Citrix SD-WAN Orchestrator service and Citrix Virtual Apps and Desktops Standard for Azure communicate with each other using APIs.

The third component in this integration is the network location service which allows internal users to bypass the gateway and connect to the VDA's directly, reducing latency for internal network traffic. For phase 1 of this integration the network location service needs to be configured manually. For more information, see Network location service (NLS).

Configuration

 After you followed all the pre-requisites highlighted in the pre-requisites section, the first item that must be configured is the DNS. This must be configured in the Citrix SD-WAN Orchestrator service. You need admin rights to configure DNS on the Citrix SD-WAN Orchestrator service. To configure DNS, navigate to **Configuration > App & DNS Settings > DNS Servers** in the Citrix SD-WAN Orchestrator service GUI and click **+DNS Server**. Enter the primary and secondary DNS in the ensuing screen.

2	Dashboard		Network	c Conf	iguration	n : DNS Ser	rvers	
<u></u>	Reports	>	*	Verify C	onfig DNS	Servers		
٥	Configuration	~	+ DI	NS Serv	e r	Primary DNS	Secondary DNS	Artions
	Delivery Services	>	1	cD	NATestD	10.0.3.4	Secondary DNS	
	Link Settings QoS Security	>	Note: DN	S Proxy &	Forwarder s	ettings are availa	able as part of Site Co	onfig
	Site & IP Groups	>						
	App & DNS Settings Custom Apps	~						

As highlighted in the Deployment and configuration section above, the AD and DNS is present in the on-premises location acting as the data center and in a deployment featuring SD-WAN it is available behind the SD-WAN that is on the LAN network. It's the AD/DNS IP that you must configure here. In case you are using Azure Active Directory service/DNS, configure 168.63. 129.16 as the DNS IP.

If you are making use of an on-premises AD/DNS, check if you can ping the IP of your DNS from your SD-WAN appliance. You can do this by navigating to **Troubleshooting > Diagnos**-

tics. Check the check box against **Ping** in the ensuing screen and initiate a ping from the LAN interface/Default interface of the SD-WAN appliance to the IP of your AD/DNS.

Dashboard	Network TroubleShooting : Diagnostics
LIII Reports	Ping Traceroute Packet Capture Bandwidth Test
Configuration	Source Site
Troubleshooting Audit Logs Device Logs Diagnostics	Source Site CDNTestCMD PING IP Address Interface Gateway IP (Optional)
Administration 2	Default Default Routing Domain Default Packet Size (KB) VIF-WAN-1: 70

If the ping succeeds then it signifies that your AD/DNS can be reached successfully. If not, then there is a routing issue in your network which is preventing reachability to your AD/DNS. If possible, try to host your AD and SD-WAN appliance on the same LAN segment. In case there is still an issue, reach out to your network admin. Without completing this step successfully, the catalog creation step will not succeed and you are likely got an error message stating **Global DNS IP not configured**.

Note

Ensure that the DNS is capable of resolving both internal and external IPs.

2. Log in to the Citrix Virtual Apps and Desktops Standard for Azure UI. You can view the following screen:



Click **Network Connections** to create network connectivity between your on-prem resources and Citrix Virtual Apps and Desktops Standard for Azure subscription. Click **+ Add Connection**.



The SD-WAN option is only be enabled if you meet the following requirements:

- You must have an existing SD-WAN network with Citrix SD-WAN Orchestrator service entitlement. If you don't have an existing SD-WAN network then set up one using Citrix SD-WAN Orchestrator service. For more details, see Configuring a Master Control Node (MCN).
- You must have a subscription to Citrix Virtual Apps and Desktops Standard for Azure.
- Currently, this integration support is only available for customers. If you are a partner or an MSP and must try this service then you must subscribe to Citrix Virtual Apps and Desktops Standard for Azure as a customer, only then this integration can be enabled. Otherwise, this option remains disabled.
In case you want to try this integration and need trial access for the Citrix SD-WAN Orchestrator service then request a trial by visiting citrix.cloud.com or sdwan.cloud.com.

3. Once you meet the conditions highlighted in the pre-requisites, click the **SD-WAN** tab to view the overall workflow:



- 4. Enter the following details to configure the SD-WAN:
 - **Deployment mode**: You can see two deployment mode options Standalone and High Availability.
 - **Standalone**: The deployment mode for SD-WAN can either be standalone where a single SD-WAN instance is deployed. If the SD-WAN instance fails due to either an issue with the SD-WAN firmware or the underlying Azure infra you cannot reach out to the resources deployed behind the SD-WAN instance in Azure. In other words, the instance behaves in a fail to block mode.
 - **High Availability**: To guard against software failure of the SD-WAN instance you might choose to deploy the instance in high availability mode which deploys two SD-WAN instances in active standby mode. Citrix recommends deploying instances in high availability mode for production networks.
 - **Enter SD-WAN site name**: Enter the site name to identify a site in your SD-WAN network. Make sure that the name you choose is unique and easy to recall.
 - **Throughput and number of offices**: Currently, only D3_V2 option is supported. D3_V2 supports up to 200 Mbps of throughput and can establish direct connectivity to 16 sites. The connections that are not direct go through the MCN.
 - **Region**: Select the Azure region where you want to deploy the SD-WAN instance. This needs to be the same region where you intend to deploy your Citrix Virtual Apps and Desktops Standard for Azure resources.

- **VDA subnet**: VDA subnet is the subnet where you want to deploy your VDA and other Citrix Virtual Apps and Desktops Standard for Azure resources in Azure.
- **SD-WAN subnet**: SD-WAN subnet is the subnet where you want to deploy your SD-WAN appliance/s.

Note

This integration only supports domain joined catalogs, non-domain joined aren't supported as of today.

- 5. Once you provide all the information that asked for in the previous step, the provisioning and deployment ensues and it takes around 20 odd minutes for the process to complete. During this time, the following steps take place behind the scenes:
 - A virtual SD-WAN appliance (VPX) starts to get provisioned in Azure based on the configuration chosen by you. Once provisioning succeeds, the SD-WAN VPX comes up with the chosen CPU and memory profile along with the network configuration supplied during the previous step.
 - Once provisioning succeeds, the VPX appliance reaches out to the Citrix SD-WAN Orchestrator service over public Internet to request for the configuration package.

	~	The SD-WAN branch has been confinistatus until the SD-WAN administrat	gured and will remain in a pending tor activates the branch.
There are no catalor Why not start one? Create a catalog → Great or POCs and non-domain joined Add users using our managed Microsoft Add users using our managed Microsoft Connect your network → Setup an Azure Vivet Bring users from Microsoft AD or Azure J	1 2 3	s next: A machine will be created to host the SD-WAN branch in the Citrix managed subscription. Once the machine is running, it will wait activate the branch. Once the branch is active the SD-WAN connection card will change to a green status, and you will be able to create catalogs using network connectivity	SD-HAN

6. Once the SD-WAN branch is configured, you can view the configuration details.

	Midilli brancii	
	Machine creation complete in 23 minutes Now creating virtual machines_	
	Configuration details	
O. Creating catals	IP ADDRESS RANGE 10.1.00 - 10.1.0.255	
	IP ADDRESSES AVAILABLE 247 / 251	
	VDA (LAN) SUBNET 10.0.0.0/24	
	REGION U.S. East	
	WAN SUBNET 10.0.0.0/25	
	DEPLOYMENT MODE High Availability (2VMs)	
	DISK ASSIGNED 250 GB	
	MACHINE TYPE	

7. Once the instance is provisioned, you can see the following screen. At this point the network administrator must log into the Citrix SD-WAN Orchestrator service to allow the addition of the SD-WAN VPX appliance to the network.



8. The network administrator must log in to the Citrix SD-WAN Orchestrator service and navigate to Network configuration home page, where you can see a line item for the SD-WAN site in Citrix Virtual Apps and Desktops Standard for Azure.

2	Dashboard		Networ	k Configurat	ion : Home	1					Site Group:	All		~
<u>.u.</u>	Reports	>	Software Ve	ersion : 10.2.5	i.6 V									
\$	Configuration	~	+ Add Si	Batch Add	Sites Deplo	y Config/Softw	are Back U	p/Review Che	ckpoints	More Actions	Deployment Tracker	Sea	rch	Q
	Network Config Home										Deployment Indoker			
	Delivery Services	>	Availability	Cloud Connectivity	Site Name	Site Role	Device Model	Serial No	Ser.No.Status	Bandwidth Tier	Management IP	Action	5	
	Douting			Inactive	CMD	Branch	210-SE			20		11		
	Routing	,		Online	Azure_Eas	MCN	VPX-SE	0000-0010		1000	10.53.11.100	11		
	Link Settings	>		Online	Azure_We	Branch	VPX-SE	0000-0011		1000	10.53.27.100	11	• •••	
	QoS	>		Online	AWS_US	Branch	VPXL-SE	ec291542		1000	10.53.165.176	11		
	Security	>		Online	AWS_US	Branch	VPXL-SE	ec23ad0a		200	10.53.161.170	11		
	Site & IP Groups	>		Online	LAB_Brian	Branch	210-SE	JHNVXCX4	~	200	23.115.253.195	11	• •••	
				Online	LAB_Stagi	Branch	210-SE	K8VFXCX4	~	200	12.42.9.137	11		
	App & DNS Settings	,		Online	AWS_Eu	Branch	VPXL-SE	ec25d258		200	10.53.169.183	11	• •••	
	Profiles & Templates			Offline	EBC_S (HA)	Branch	210-SE	KU15RCX4	~	200	10.53.129.15	11		
				Online	Azure We	Branch	VPX-SF	0000-0011		1000	10 53 35 100	11		

9. The network administrator must deploy the sites at this stage. Click the **Deploy Config/Software** to deploy.

2	Dashboard		Network Configura	ation : Deployment T	racker			
<u></u>	Reports	>	Current Depl	loyment Deployment Histo	ory			
۵	Configuration Network Config Home Delivery Services Routing Link Settings	* > >	Software Version : Verify	1025.6 Stage	Activate			
	QoS Security	>	/17		Staged A	ppliances		
	Site & IP Groups	>			Activated	Appliances		
	App & DNS Settings Profiles & Templates	>	Total Appliances 17	Staged O		Activated	Failed	

10. Once the **Deploy Config/Software** step succeeds, you can see that the status on the Citrix Virtual Apps and Desktops Standard for Azure screen changes to **you can now create catalogs using SD-WAN**.

Network location service

With the **Network Location** service in Citrix Cloud, you can optimize internal traffic to the apps and desktops you make available to subscribers' workspaces to make HDX sessions faster.

Users on both internal and external networks have to connect to VDAs through an external gateway. While this is expected for external users, internal users experience slower connections to virtual resources. The **Network Location** service allows internal users to bypass the gateway and connect to the VDAs directly, reducing latency for internal network traffic.

Configuration

To set up the **Network Location** service, you configure network locations that correspond to the VDAs in your environment using the **Network Location** service PowerShell module that Citrix provides. These network locations include the public IP ranges of the networks where your internal users are connecting from.

When subscribers launch Citrix Virtual Apps and Desktops Standard for Azure sessions from their workspace, Citrix Cloud detects whether subscribers are internal or external to the company network based on the public IP address of the network from which they are connecting.

- If a subscriber connects from the internal network, Citrix Cloud routes the connection directly to the VDA, bypassing Citrix Gateway.
- If a subscriber connects externally, Citrix Cloud routes the subscriber through Citrix Gateway as expected and then redirects the subscriber to the VDA in the internal network.

Note

The public IP that needs to be configured in the network location service needs to be the public IP assigned to the WAN links.

Public IP assigned to the SD-WAN appliance

The public IP that needs to be configured in NLS needs to be the WAN link IPs of all the links used to send traffic over the virtual path. You can find this information by navigating to **Site > Reports > Real time > Statistics > Access Interfaces**.

Dashboard		Site Report : Real Time	Statistics						
Ltd Reports	~	ARP Routes Virtual	Path Services Classes	Elhernet Observed Prot	locols Wan Path	Application QOS Access In	iterfaces ~		
Alerts									
Usage		Retrieve latest data							
Quality									
QoS		Virtual Path Service Data Rate	Access Interface	Service Name	Direction	Virtual Path Service Packets	Virtual Path Service kB	Delta Virtual Path Service Packets	Virtual Path Service k8
Historical Statistics		Azure_EU-Internet-INET-1	AIF-1	Azure_East_US-Azure_EU	Recv	9988111	14.27	77.85	743501.57
Real Time	~	Azure_EU-internet-INET-1	A/F-1	AWS_EU-Azure_EU	Recv	2127527	0.00	0.00	276741.78
Statistics		Azure_EU-Internet-INET-1	AIF-1	Azure_EU-GCP_EU	Recv	8752343	19.74	107.69	744129.42
Flows		Azure_EU-Internet-INET-1	AIF-1	Azure_East_US-Azure_EU	Send	11563443	25.07	136.79	1281114.25
Firewall Connections		Azure_EU-Internet-INET-1	AIF-1	AWS_EU-Azure_EU	Send	1921041	1.02	5.59	195640.75
		Azure_EU-Internet-INET-1	AIF-1	Azure_EU-GCP_EU	Send	8075291	15.36	83.81	564051.32
Cloud Direct (preview)									1 to 6 of 6
Configuration	>	WAN Link	Access Interface	Service Name	Direction	Internet Packets	Internet kB	Delta Internet Packets	Delta Internet kB
		Azure_EU-Internet-INET-1	AIF-1	Internet	Recv	525025		64	2.69
F Troubleshooting	>	Azure_EU-Internet-INET-1	AIF-1	Internet	Send	34540		5	0.25
		Access Interface Statistics	Access Interface 10 &	direct	Prove Address	Provy APP State	MAC	. Last ADD Benk Ane (ms)	1 to 2 of 2
						The state		and her nepty rige (ma)	
		Azure_EU-Internet-INET-1	AIF-1 10.5	3.27.5	51.105.212.77	DISABLED	N/A	N/A	

Integration of Citrix SD-WAN Orchestrator with Check Point CloudGuard Connect

December 3, 2020

Integration topology



Configuration on Check Point portal

- 1. Add a Site on the Check Point portal.
 - a) Log into the Check Point portal and add a site.



A pop-up window to create a site appears. Provide the required general details and click Next

CLOUDGUARD CONNECT	
Sites 1 GENERAL + Name	
Citrix Tunnel	
To it's Site Address 0	
CONNECTION Bangalore, Kamataka, India	
DETAILS	
Adia: India	
STELES	
Number of users (Estimation) @	
(I) INTERNAL SUB-	
NETWORKS	
CREATION	
CANCEL NEXT	

b) Provide the connection details. Select the **Device Type** as **Citrix** and **External IP addresses** as **Static IP Address**.

Note

Provide the branch WAN Link public IP address as the **External IP Address**. It is "x.x.33.83" as per the topology.

If you are using multiple internet WAN links, click **Add another external IP address** to specify the Public IP address associated with those WAN links.

CREATE NEW SITE		×
GENERAL	* Device Type Citrix	~
2 CONNECTION DETAILS	Tunnel Type IPsec - Pre-Shared Key Monitor branch connectivity using dead peer detection (DPD)	~
3 AUTHENTICATION	External IP Addresses Dynamic IP Address Static IP Address 	
(4) INTERNAL SUB- NETWORKS	.33.83 External IP must be unique + Add another external IP address	
5 CONFIRM SITE CREATION		
	BACK NEXT	



c) In the **Authentication** section, define the pre-shared key or auto-generated the key.

d) Provide the Internal subnetwork. It is the LAN subnets behind the SD-WAN appliance, which goes through the tunnel, called as **Protected Networks** in the Citrix SD-WAN Orchestrator service. It must match at both the Citrix SD-WAN Orchestrator service and the Check Point end to ensure that the tunnel is established.

CREATE NEW SITE		×
GENERAL	Enter site sub-networks that will be routed to the CloudGuard Connect Sub-Networks 10.4.1.0/24	+
INTERNAL SUB- NETWORKS		
5 CONFIRM SITE CREATION		
	BACK NE	хт

e) Validate the configuration and click **FINISH AND CREATE SITE**.



A site tile is added with the status **GENERATING SITE**.



Check Point takes around 20 minutes to generate a site. After the site is generated, the tile status changes to **WAITING FOR TRAFFIC**.



2. Click Configure branch device to view tunnel details. It includes details of the tWO IPsec tun-

nels towards Check Point Cloud.

In this example, the tunnel destination is mentioned in FQDN format. Resolve this FQDN to get the tunnel destination IP address that can be used in the Citrix SD-WAN configuration.

For example- C:\Users\john>ns lookup g-d87e003fdd8d3717d8a534551ccd77a2.checkpoint.cloud

Server: router

Address: 192.168.0.1

Non-authoritative answer: Name: g-d87e003fdd8d3717d8a534551ccd77a2.checkpoint.cloud Address: 52.66.199.169

Configuration on Citrix SD-WAN Orchestrator service

Use the Tunnel destination and IPsec parameters to build a configuration on the Citrix SD-WAN Orchestrator service.

1. Create an IPsec encryption profile.

a) In the Citrix SD-WAN Orchestrator service UI, at the network level, navigate to **Configura**tion > IPsec Encryption Profiles and click +IPsec Encryption Profile.

Citri	x Systems Inc. /	oustonia RavitAz	ureLab	~	$\stackrel{\rm HTS}{\rm All Sites} \sim$				 angenat C ()
Ģ	DASI IDDARD	Í	Ì	\sim	The local data	for a second			
-	REPORTS	>	۱.	لما	insection of the section of the sect	anayoun roma			
٢	CONFIGURATION	~	14	+ IPS Potie	ec Encryption Profile	Action			
	Network Config Fiom								
	Delivery Services	~							
	Service & Handwi	w							
	Dynamir Virtual Pitta	-1							
	IPSec Encryption Profiles								
	Routing	>							

b) Configure the IKE and IPsec settings as per the Check Point configuration.

Ç	DASHBOARD			Verify Config IPSe	c Encryptic	on Profiles						
), III	REPORTS	>		IPSec Encryption Profile Info	rmation							
				Profile Name *	MTU					IKE Version		
¢	CONFIGURATION	~		CheckPointProfile	1500			✓ Keep Alive		IKEv2		~
	Network Config Home Delivery Services	•		IKE Settings				Dess Authentication				
	Service & Bandwid Dynamic Virtual Paths	lth		Pre-Shared Key			~	Pre-Shared Key				~
	IPSec Encryption Profiles			Identity			\sim	Peer Identity Disabled				
	Routing	>		DH Group	Hash Algori	thm		Integrity Algorithm		Encryption M	Node	
	Link Settings	>		Group2(MODP1024) V	SHA-1		\sim	SHA-1	~	AES 25	i6-Bit	, ,
	QoS	>		Lifetime (s)		Lifetime (s) Max			DPD timeou	t (s)		
	Security	>		3600		86400			300			
	Site & IP Groups	>										_
	App & DNS Settings	>		IPSec Settings								
	Profiles & Templates	- 1		Tunnel Type PFS G	oup	1	Encryptio	n Mode Ha	ash Algorithm		Network Mism	natch
n		>		ESP+Auth V N	one	\sim	AES 2	256-Bit 🗸	SHA-1	\sim	Drop	`

- 2. Add IPsec tunnel towards Check Point Cloud.
 - a) Navigate to **Configuration** > **Delivery Services** > **Service & Bandwidth** and add an Intranet service.

DASHBOARD	With Cards Service & Bane	dwidth							
REPORTS >									
CONFIGURATION	Delivery Service								
Network Config Home	Virtual Path		100	s	100	s	100	s	
Delivery Services 🤍	Internet	0 8	0	s		s	0	×	
Service & Bandwidth	Cloud Direct Service	0 8		S		8		8	
Paths	Intranet . Service			s		\$			
IPSec Encryption Profiles	1. Zsteler	0 8	0	s				s	
Routing >	2. Againt Virtual KIAN	0 8	0	s		s		s	
tini Settings >	5. Ner3009934a	0 8	0	s	0	s	0	×	
tanó > Security > Site & IP Groups >	Save								
App & DNS Settings									

b) Select the Service type as IPsec Service.

PROV Citri	ider x Systems Inc. /	CUSTOMER RaviAzureL	ab ∨ / All Sites ∨
Q	DASHBOARD	^	Virty Leaves Service & Bandwidth
ай л	REPORTS	>	
Ô	CONFIGURATION	~	Service type
	Network Config Hom Delivery Services	e V	Intranat V
	Service & Bandwi	dth	IPSec Service
	Dynamic Virtual Paths		
	IPSec Encryption Profiles		
	Routing	>	

c) Configure IPsec Tunnel towards Check Point Cloud. Click **+End Point** to add the Check Point end point information.

Citri	ider x Systems Inc. /	customer RaviAzureLal	b 🗸 / All Sites 🗸										
Q	DASHBOARD	^	Verify Config Service 8	& Bandwidth									
.	REPORTS	>	<u> </u>										
٢	CONFIGURATION	~	Service Details										
		_	Service Name *	Service Type *		Routing Domain	Firewall Zone						
	Network Config Home		CheckPointTunnel	Intranet	~	Default_RoutingDomain ~	<default></default>						
	Delivery Services	~				- /							
	Service & Bandwid	ith	Tunnel End Points Across Netwo										
	Dynamic Virtual Paths		+ End Point										
	IPSec Encryption Profiles	11	Name	Peer IP		IPsec Profile	Actions						
	Routing	>											
	Link Settings	>	Map Sites to Tunnel End Points										
	QoS	>											
	Security	>	+ End Point Mapping										
	Site & IP Groups	>	Name		No of Sites		Actions						
	App & DNS Settings	>											
	Profiles & Templates		Cancel Save										

- d) Provide the following details:
 - Peer IP(Check Point FQDN IP address that was resolved)
 - IPsec Profile that we have created in the previous step
 - Pre-shared key that you got from Check Point.

C DASHBOARD	Verify Config Service	& Bandwidth		
, REPORTS >				
ONFIGURATION ~	Service Details			
Network Config Home Delivery Services V	Service Name * CheckPointTunnel	Service Type *	Routing Domain Default_RoutingDomain	Firewall Zone
Service & Bandwidth	Tunnel End Points Across Netwo			
Dynamic Virtual Paths	Name*	Peer IP *	IPsec Profile + IPsec Profile	Pre Shared Key
IPSec Encryption Profiles	CheckPointTun1	52.66.199.169	CheckPointProfile 🗸 🗸	LLdwQ815JJ
Network Location Service	Peer Pre Shared Key	Identity Data	Peer Identity Data	Certificate
Routing >	sb9VrweZjUjhY1zs1LdwQ8I5J			~
Link Settings >	Cancel Done			

Similarly, add the second tunnel end point towards Check Point cloud for redundancy.

C DASHBOARD	Verify Config Se	rvice & Bandwidth		
∰ REPORTS >	Service Details			
CONFIGURATION V	Service Name	Service Type *	Routing Domain	Firewall Zone
	CheckPointTunnel	Intranet	✓ Default_RoutingDomain	× V
Network Config Home Delivery Services	Tunnel End Points Across N	Network		
Service & Bandwidth	+ End Point			
Dynamic Virtual Paths	Name	Peer IP	IPsec Profile	Actions
IPSec Encryption Profiles	CheckPointTun1	52.66.199.169	CheckPointProfile	<u>i</u>
Network Location Service	CheckPointTun2	15.207.222.114	CheckPointProfile	iii
Routing >				
Link Settings >	Map Sites to Tunnel End Po	oints		

e) Click + End Point Mapping to add an End Point mapping.

Citri	ix Systems Inc. /	RaviAzureLab	o ✓ / All Sites ✓					
Q	DASHBOARD	Â	Verify Config Service & B	Bandwidth				
	REPORTS	> -	ш <u>—</u>					
٥	CONFIGURATION	~	Service Details					
	Network Config Home Delivery Services	~	Service Name * Service Name *	iervice Type * Intranet	Routing	Domain fault_RoutingDomain	Firewall Zone	~
	Service & Bandwic	đth	Tunnel End Points Across Network					
	Dynamic Virtual Paths		+ End Point					
	IPSec Encryption Profiles		Name	Peer IP		IPsec Profile	Ac	tions
	Routing	>	CheckPointTun1	52.66.199.169		CheckPointProfile	đ	I
	Link Settings	>						
	Q05	>	Map Sites to Tunnel End Points					
	Security	> T	+ End Point Mapping					
	Site & IP Groups	> L	end tonit mapping					
	App & DNS Settings	>	Name		No of Sites		Ac	tions
	Profiles & Templates							
Z	TROUBLESHOOTING	>	Cancel Save					

Choose the End Point as **CheckPointTun1**, the one created in the previous step and click **+ Bindings** to bind a site. Similarly, add **CheckPointTun2** as the second end point.

Citr	ix Systems Inc. /	customer RaviAzureLal	b ✓ / All Sites ✓					
Q	DASHBOARD	^	Weilly Config Service	ce & Bandwidth				
1	REPORTS	>	<u> </u>					
0	CONFIGURATION	~	Service Details					
		- 1	Service Neme*	Service Type *	Routing Domain		Firewall Zone	
	Network Config Home	e	CheckPointTunnel	Intranet	V D	efault_RoutingDomain V	<default></default>	~
	Delivery Services 🗸 🗸							
	Service & Bandwidth		Tunnel End Points Across Net	work				
	Dynamic Virtual Paths		+ End Point					
	IPSec Encryption Profiles		Name	Peer IP		IFsec Profile	Actions	
	Routing	>	CheckPointTun1	52.66.199.169		CheckPointProfile	8	
	Link Settings	>						
	QoS	>	Map Sites to Tunnel End Poin					
	Security	>	Choose Endpoint					
	Site & IP Groups	>	CheckPointTun1	~				
	App & DNS Settings	> 1						
	Profiles & Templates	- 84	+ Bindings					
			Cancel Done					

Bind the tunnel to a branch site (For example- BranchAzure) and provide the protected network details.

Note

The protected network has to be the branch site that is configured in the Check Point portal. The Public IPs must match.

In this case, the protected network's source network is the LAN network of the branch and the destination as is any. The source network must match the network configured in the Check Point portal. Click **Done**.

0	DASHBOARD	^	Tunnel End Points Across Netwo	rk		
		-1.	+ End Point			
í,	REPORTS	>	Name	Peer IP	Prec Profile	Actions
0	CONFIGURATION	~	CheckPointTun1	52.66.199.169	CheckPointProfile	8
	Network Config Home		Map Sites to Tunnel End Points			
	Delivery Services	~	Choose Endpoint			
	Service & Bandwic	Ith	CheckPointTun1	~		
	Dynamic Virtual Paths		Bindings			
	IPSec Encryption Profiles		Site Name*	-		
	Routing	>	Branch2Azure v			
	Link Settings	>	Protected Networks			
	Q05 Security	>	+			
	Site & IP Groups	>	Source Network IP/Prefix	Destination Network IP/Prefix		
	App & DNS Settings Profiles & Templates	>	10.4.1.0/24	Any	-	
2	TROUBLESHOOTING	>	Cancel Done			

Click **Save** to save IPsec Tunnel configuration. check-point-generating-site.png

Citri	ix Systems Inc. /	RaviAzureLat	b 🗸 / All Sites	~					
Q	DASHBOARD	Â	Verify Config	Service & Bandwidth					
*	REPORTS	>							
٢	CONFIGURATION	~	Service Details	Service Type *		Routing Domain	Firewall Zone		
	Network Config Home		CheckPointTunnel	Intranet	\sim	Default_RoutingDomain	n ∨ <defau< th=""><th>it> ~</th><th></th></defau<>	it> ~	
	Delivery Services 🗸		Tunnel End Points Acr	oss Network					l
			+ End Point						
	Dynamic Virtual Paths		Name	Dear ID		IDroc Brofile		Artionr	
	IPSec Encryption Profiles		CheckPointTun1	52.66.199.1	69	CheckPointProfile	1		
	Routing	>							
	Link Settings	>	Map Sites to Tunnel E	nd Points					l
	QoS	>							1
	Security	>	+ End Point Mapp	ving					
	Site & IP Groups	>	Name		No of Site	5		Actions	
	App & DNS Settings	>	CheckPointTun1		1				
	Profiles & Templates								
Z	TROUBLESHOOTING	>	Cancel Sa	ave					

f) After the CheckPointTunnel delivery service is added, allocate the bandwidth share for the service to be applied to the site to which the end point is mapped.

Note

The bandwidth percentage allocated here is the guaranteed bandwidth share for this Checkpoint Delivery service when in contention.

DASHBOARD	Virily Coulding Service & Bandwi	idth								
REPORTS >										
CONFIGURATION	Delivery Services									
Network Config Home	Virtual Path		70	x	100	5	100	- 5		
Delivery Services 🗸 🗸	Internet	0 🕀	0	x		8	0	8		
Service & Bandwidth	Cloud Direct Service	• =		s		5		8		
Dynamic Virtual Paths	Intranet + Service			s		s		s		
IPSec Encryption Profiles	1. Zscaler	0 0	0	s	0	8				
Routing >	2. Azure Virtual W/N	0 🗄	0	5	0	5		-		
Link Settings >	3. Non_SOWAN_Sites	0 0	0	N	0	8	0	8		
Q05	 CheckPointTunnel 	0 🛱	20	x	0	8	0	8		
,										

- 3. Deploy the configuration on the Citrix SD-WAN Orchestrator service through staging and activation.
- 4. Check the Tunnel status towards Check Point Cloud from the branch site.

Dashboard	-	Network Reports: Real Tin	ne Statisti	cs						Site Group:	All	~
REPORTS	~	ARP Routes Virtual Path S	ARP Routes Virtual Path Services Classes Ethernet Observed Protocols Wan Path Application QOS IPsec Tunnel ~									
Alerts	Alerts											
Usage		Azure Branch UK	~	Retrieve	alatest data						Search	Q
Security	>	Name	State	Service Type	Packets Received	Kbps Received	Packets Sent	Kbps Sent	Packets Dropped	Bytes Dropped	MTU	
HDX (preview)		CheckPointTunnel_CheckPointTun1	GOOD	Intranet	0	0.00	0	0.00	0	0	1434	
Quality		CheckPointTunnel_CheckPointTun2	GOOD	Intranet	0	0.00	0	0.00	0	0	1434	
QoS										1 to 2 of 2	IC < Page 1 of 1	
Historical Statistics												
Real Time	\sim											
Statistics												
Flows												
Firewall Connection	ons											

Monitoring

Access Internet from a branch site host through the Check Point Cloud over the IPsec Tunnel. For example, try accessing salesforce.com.

This application is reported in firewall connections with the destination service as **CheckPointTun**.

trix Systems Inc. /	RaviAz	ureLab 🗸 / All Si	tes 🗸							E	Thange Role 🗳
DASHBOARD	Í	Network Repo	rts: Real Time	e Firewall Conn	ections					Site Group. A	
REPORTS	~	Branch2Azure		~	Retrieve latest	data			sales Q,	Cust	Contante Columns
Alerts		Connections Display Connections In Use:	ed: 124 124/129000								
Usage			1			Source			Destination		
Inventory		Application	Family	Rauting Domain	IP Addr	Service Type	IP Addr	Service Type	Service Name	State	Is NAT
Security	\rightarrow	Salesforce(salesfor	Web	Default_RoutingD	10.4.1.5	Local	136.147.42.135	Intranct	CheckPointTunnel_CheckPointTun1	ESTABLISHED	No
HUX(proving)		Salesforce(salesfor	Web	Default_RoutingD	10.4.1.5	Local	13.110.63.111	Intranct	Checi@ointTunnel_CheckPointTun1	CLOSED	No
Quelity		Salesforce(salesfor	Web	Default_NoutingD	10.4.1.5	Local	3.6.119.69	Intranet	Checkfoin/Tunnel_Checkfoin/Tun1	CLOSED	No
		Salesforce(salesfor	Web	Default_RoutingD	10.4.1.5	Local	101.53.160.164	Intranet	CheckPointTurnel_CheckPointTurt	ESTABLISHED	No
Gus		Salastorce(salestor	Web	Detault_RoutingD	10.4.1.5	Local	101.53.160.164	Intranct	CheciPointTunneLCheckPointTun1	CSTABUSHED	No
Historical Statistics										1 to 5 of 5 icit	Page 1 of 1 > >1
Real Time	~										
Statistics											
Flows											
Firewall Connect	tions										
Cloud Direct											
Application Quality											
PETER Resolution											-

This traffic is updated in the IPsec Tunnel statistics (Packets sent and received).

PROVIDER Citrix Sy	stems Inc. /	customer RaviAzu	reLab 🤝 / 🖁 All Sites 🗸									Change Role	<i>Q</i> ()
ΩD	ASHBOARD	Â	Network Reports: Real Ti	me Statistics							Site Group:	All	~
៍ ខ	EPORTS	~	ARP Routes Virtual Path	Services Classes	Ethernet	Observed Protocols	Wan Path Applie	ation QOS	iec Tunnel 🗡				
Ab Us Im	ierts sage ventory		Branch2Azure	~	Retrieve	latest data						Search	Q
Se	scurity	· ·	Name	State	Service Type	Packets Received	Klaps Received	Packets Sent	Klops Sent	Packets Dropped	Bytes Dropped	MTU	
H	DX(preview)	· ·	CheckPointTunnel_CheckPointTun1	GOOD	Intranet	4148	1.39	3171	0.35	2	80	1434	
0	sality		4										•
Q	a5	- 1									1 to 1 of 1	C Regell of 1	- 21
Hi	istorical Statistics	- 1											
Re	eal Time	~											
- Г	Statistics	- 1											
	Flows												
	Firewall Connecti	ons											

Logs

Logs related to IPsec Tunnel creation can be found in the SDWAN_security.log file.

DASHBOARD		Netwo	ork TroubleShooting: E	Device Logs						
REPORTS	>	Select 5	ite							
ONFIGURATION	>	Az	ure Branch UK)					Secur	Q
() ALERTS	>		Name		Last Modified	Size				
🖒 troubleshooti	NG \checkmark		SDWAN_security.log		November 3, 2020 9:50 PM	27.27 KB				
Audit Logs							Page Size: 25 ∨	Showing 1 - 1 of 1 items	Page1 of1	
Device Logs										
Diagnostics										
	>									

The site status on the Check Point portal is updated as **Active**.

$\leftrightarrow \rightarrow$	C portal.checkpoint.com/D	ashboard/CloudGuardConnect#/assets/sites			
 -	CLOUDGUARD CONNECT			0 🛛 🖉	Ravisar
ASSETS .	Sites (1)	+ Add Q Search by Name, IP	Ţ	II = 0	
POLICY LOGS LOGS SETTINGS	+	CITRIX TUNNEL Q Asia: India Q ACTIVE			

Try to access a website (for example - Facebook.com) you can able access through Check Point Cloud. You can now modify the Check Point Access Control policies by adding a policy to block the Facebook application.

$\leftarrow \ \rightarrow $	C	ê por	tal.checkpoint.com	n/Dashboard/CloudG	uardConnect#/policy/access-co	ntrol Q 🖈 🏚
·	Ļ.	CLOUD	GUARD CONNECT			🔯 🏮 Ravisankar Pegada 🚇 🗸 🔛 Ch
ASSETS	÷	A	ccess Control	× = :=	🍕 Manage Objects 🔍 Sear	changes 🕢 🔹 Install Policy
U.		*	Action	Name	Source	Destination
PORT	*	1	G Block		* Any site	Facebook
1053		2	🖨 Block	Malicious content	* Any site	Anonymizer Spyware / Malicious Sites Botnets Span Phishing Hacking
		3	O Block	Explicit content	* Any site	Wolence Nudity Pornography Child Abuse Gambling Hate / Radom Illegal / Questionable Illegal Drugs Weapons

After the policy is installed, Facebook.com is blocked.

🕲 ficebook.com 🗙 🕂		
← → C (① facebook com		
	μ.	
	This site any't be uppelled	
	This site can't be reached	
	The connection was reset.	
	Try:	
	Checking the connection Checking the provide the formula	
	 Checking the proxy and the mewant 	
	ERR_CONNECTION_RESET	
	Reload	Details

It shows that the Internet traffic is redirected from SD-WAN, towards the Check Point Cloud through the IPsec tunnel. The action was taken as per the policy definition on the Check Point Cloud.

Deploy Citrix SD-WAN Standard Edition instance on Azure

November 8, 2021

Citrix SD-WAN Standard Edition (SE) for Azure logically bonds multiple network links into a single secure logical virtual path. The solution enables organizations to use connections from different service providers including Broadband, MPLS, 4G/LTE, Satellite, and point-to-point links to get high resiliency virtual WAN paths. Citrix SD-WAN for Azure enables organizations to have a direct secure connection from each branch to the applications hosted in Azure, eliminating the need to backhaul cloud bound traffic through a data center. Some of the benefits of using Citrix SD-WAN in Azure are:

- Create direct connections from every location to Azure.
- Ensure an always-on connection to Azure.
- Extend your secure perimeter to the cloud.
- Evolve to a simple, easy to manage branch network.

For more details on topology, use case and manually provisioning an SD-WAN SE instance on Azure, see Deploy Citrix SD-WAN Standard Edition Instance on Azure.

Citrix SD-WAN Orchestrator service allows deploying a Citrix SD-WAN instance in Azure quickly and easily. Citrix SD-WAN Orchestrator service automates the process of provisioning a virtual machine in Azure while defining a cloud site. A new and unique resource group, specified by the user, is created in Azure for every cloud site. You can either choose the existing VNets/subnets under the resource group or create VNets/subnets used for provisioning. You can use a virtual machine instance template to deploy Citrix SD-WAN VPX directly from Citrix SD-WAN Orchestrator service. The interfaces and WAN link configurations are auto populated on the Orchestrator configuration based on the resources created in Azure. You can then stage and activate the configuration on the VPX instance through Citrix SD-WAN Orchestrator service.

As a prerequisite for deploying SD-WAN VPX instance on Azure, ensure that you have a Citrix SD-WAN Orchestrator service subscription and a Microsoft Azure service subscription.

To deploy an SD-WAN VPX instance on Azure:

 On the Network Dashboard, click + New site to create a cloud site. Provide a name for the site and select Cloud Site. Select Azure as the Cloud Provider and select the Azure Region where you want to deploy the SD-WAN instance.

Site Details			
ite Name *			
Branch1			
On-Premises Oloud Site			
Cloud Provider *		Region *	
Azure	\sim	Central US	~

2. Provide the site details. For more details on site roles and advanced settings, see Site details.

Note

The **Enable Source MAC Learning** option stores the source MAC address of the received packets so that outgoing packets to the same destination can be sent to the same port.

		Device Details	Cloud Details	04 Interfaces	05 WAN LINKS
Site Information					
Site Profile		Site Name *		Site Address*	Lat/Lr
None	~	Branch1		Central US	
Region *	Device Mode	el*	Sub-Model *	Device E	dition *
Select Region	✓ VPX	\sim	BASE	✓ SE	×
Site Role *		Bandwidth Tier (Mbps) *		Select Tag	Create Ne
Branch	\sim	20	~		×

3. Enable High Availability (HA), if necessary. If HA is enabled, two virtual machines, a primary and a secondary virtual machine is created on Azure. You do not have to provide the device serial numbers. The device serial numbers are fetched automatically during provisioning. For more details on Advanced HA settings, see Device details. To allow traffic through HA on the Azure portal, see Internet breakout for Azure HA site.

Verify Config III Site Details 02 Device Details	03 Clou	d Details	04 Interfaces	05 WAN Links	06 Routes	07 Sumr
Device Information						
✓ Enable HA						
Primary Device Serial Number	5	Short Name				
		Primary				
Secondary HA Device Serial Number	ŀ	HA Device Sho	ort Name (Optional)			
Enter HA Device Serial		Seconda	ry			
Advanced HA Settings						•
Failover Time (ms)	5	Shared Base N	IAC			
1000		AA:AA:A	A:00:00:00			
Primary Reclaim						
HA Fail-to-Wire Mode						
Disable Shared MAC						
Cancel Save					Prev	Next

4. Provide the Cloud service subscription details and the virtual machine configuration parameters.

Verity Config 01 Site Deta	ils 🔞 Device Details 🔤	Cloud Details 04 In	nterfaces	05 WAN Links	06 Routes	07 Sum
Cloud Information						
Subscription ID *	Azure Region*		Res	source Group *		
	Central US		\sim	mcn_azure_dev		
Create Subscription ID						
Virtual Machine						
Instance Type *						
Standard_D3_v2, 4 Cores, 1047552	2MB OS DiskSize, 204800MB Res	ource Disk Size				\sim
Username *	Password *		Co	nfirm Password *		
	Enter Password	t		Enter Password		
Network Settings						
VNet	LAN Subnet		WA	N Subnet		
azure_dev_auto_vnet	~ azure_dev_mc	n_lan	\sim	azure_dev_mcn_wan		\sim
Create New VNet	Create LAN Subn	et	C	Create WAN Subnet		
🗹 Enable Public IP For Management						
Deploy Configuration Dele	ete Configuration					
Cancel Save						

a. Click **Create subscription ID**. Provide the Subscription ID, Tenant ID, Application ID, and Secret key as available on your Azure portal. For information on where to find the subscription details on the Azure portal, see Identify Ids.

Manage Subscription	
Subscription ID *	Tenant ID *
Application ID*	Secret Key*
	Oracle Oracle
	Cancel Create

You can add multiple subscriptions. After the subscription details are saved, you can select a subscription ID. Specify the **Azure region** where you want to deploy the instance and provide a name for the new **Resource Group**.

Cloud Information		
Subscription ID	Azure Region	Resource Group*
~	Central US 🗸 🗸	Branch1
contract on the state of the		

b. Select one of the following virtual machine instance types as per your requirement and provide the login credentials.

- Instance type D3_V2 for max uni-directional throughput of 200 Mbps with 16 max virtual path-s/branches.

- Instance type D4_V2 for max uni-directional throughput of 500 Mbps with 16 max virtual path-s/branches.

- Instance type F8 standard for max uni-directional throughput of 1 Gbps with 64 max virtual paths/branches.

- Instance type F16 standard for max uni-directional throughput of 1 Gbps with 128 max virtual paths/branches.

Virtual Machine					
Instance Type					
Standard_D3_v2, 4 Cores, 1047552MB OS DiskSize, 204800MB Resource Disk Size					
Username *	Password *	Confirm Password *			
		••••••			

Note

You cannot provision the instance with the user name admin, as it is a reserved name. However, to get admin access after provisioning the instance, use admin as the user name and the password created while provisioning the instance. If you use the user name created while provisioning the instance, you get read-only access.

Guidelines for user name:

- User name must only contain letters, numbers, hyphens, and underscore and must not start with a hyphen or number.
- User names must not include reserved words.
- The value is in between 1 and 64 characters long.

Guidelines for Password:

- The value must not be empty.
- Password must have three of the following:

- One lower case character
- One upper case character
- One Special character
- The value is in between 12 and 72 characters long.

c. Create a New VNet or select an existing VNet. Existing VNets are displayed based on the selected cloud subscription. For the selected VNet you can either select existing LAN and WAN subnets or create subnets. Ensure that the **Enable public IP for Management** option is selected and click **Save**.

Note

The LAN and WAN subnets must not be the same.

Network Settings							
VNet	LAN Subnet	WAN Subnet					
azvwan_dmz-vnet V	default 🗸 🗸	default 🗸					
Create New VNet	Create LAN Subnet	Create WAN Subnet					
Enable Public IP For Management							
Deploy Configuration Delete Con	figuration						

d. Click **Deploy Configuration** to create an SD-WAN VPX instance in Azure with the specified virtual machine and network settings. This would take about 10-15 minutes. The deployment status is displayed in the UI.



Note

 After the instance is created in Azure, proceed with the Stage and Activate process to upgrade the Azure VPX to the desired software version and configuration as defined in Orchestrator.

- After the deployment is initiated, you cannot make any changes to the Cloud site settings such as resource-group, VNets, subnets, user name, and password for VPX. If the deployment fails, you can provide revised settings before initiating the deployment.
- To remove the SD-WAN VPX instance from Azure and proceed with a clean deployment, click **Delete Configuration**. This does not delete the site from Citrix SD-WAN Orchestrator service. It only removes the SD-WAN VPX instance. You can provide revised cloud site details and proceed with deploying the configuration.
- To delete the virtual machine on Azure and free up resources, click **Delete Configura-***tion*.
- 5. The interfaces, WAN links, and routes are auto-created based on the resources provisioned on Azure. You can navigate to the **Interfaces**, **WAN links**, and **Routes** tab to view the settings.

Note

IPv4 addresses are used for the LAN, WAN, and access interface settings. IPv6 addresses are not yet supported.

Verify Cor	nfig 01 Site [Details 0	2 Device Details	03 Cloud Details	04 Interfaces	05 WAN Links	06 Routes	07 Sum
+ Interface								
InBand Management IF		InBand Ma	nagement DNS					
None	~	None		~				
Interface Name	Port(s)	VLAN ID	IP Address				Act	tions
LAN-1	1	0	10.54.53.4/24				Ē	
WAN-1	2	0						
Cancel	Save						Prev	Next

U III	D Site Details	Device Details	Cloud Details	(1) Interfaces	05 WAN Links	🔘 Routes	Summary			
+ WAN Link										
AN Link Name		Speeds	1	Access Interface IP			Gateway IP			Actio
roadband-Azure-1		10 Mbps† 10	Mbps]							8
Cencel Seve	te Details 💿 Devicr	e Details 💿 Cloud Deta	ails 🕡 Interface	əs 👩 WAN Links	(6) Routes (7)) Summary				Prov N
et Bangaou - Custam Applicati	ion (1.20) Application (21.401 Application Crown (d	11 CO) ID /1 CEE2E1							
Application Dest	Application (2	Application Group (4	Canada (an Da							
+ Application Route			Search for Route			ч				
o Match Type	Name	Delivery Service	Routing Domain	Sites				Cost	Actions	
Application Group	Default Cloud Dir	Cloud Direct Service	Any	Global				45		
Application Group		Nocuro Internet Access	Any	Global				45		
Application Group	Default SIA App	Secure Internet Access						50	~	
Application Group Application Group Application Group	03650ptimize_In	Internet Breakout	Any	Global				50		

6. After the virtual machine is deployed successfully, it takes about 5–10 min for the virtual machine to be up and running.

The **Summary** section provides a summary of the site details, interface details, and WAN link details. Click **Save**. Click **Verify Config** to populate the device serial number.

Verify C	onfig 💿 Site) Details 💿 Devi	ce Details 💿 Cloud Details	Interfaces	O WAN Links	🐼 Routes	07 Summary		
Site & Device D	etails								
Site Name	Device Model	Site Role	Serial Number						Bandwidth Tier
test_branc	VPX	Branch	0000-0000-9062-08	77-9962-6990-44					20 Mbps
LAN-1-1 • VLANO-VI WAN-1-2 • VLANO-VI	LAN-1-1 • VLAN0-VIF-LAN-1-Default_RoutingDomain-10.52.7.4/24 WAN-1-2 • VLAN0-VIF-WAN-1-Default_RoutingDomain-DHCP Enabled								
Broadband AIF-1-VIF-	-Azure-1 - 10 WAN-1 - primary	Mbps† 10 Mbps↓ v							
Cancel	Save			Save as F	Profile			1	Prev Done

The Azure virtual machine is created and the configuration is ready. However, the configuration is not applied to the SD-WAN instance.

 To push the configuration to the provisioned SD-WAN instance in Azure, navigate to Network Configuration: Home. Select the required software version and click Deploy Config / Software. For more details on staging and activation see, Deployment tracker.

Network	Configuration	: Home						Site Group:	All		\sim
Software Ve	rsion : 11.3.0.16	8 🗸									
+ Add Sit	e Batch Add Si	tes Deploy Config/Software Back Up/Review Checkpoi	nts More Ac	tions			Deployme	nt Tracker Search			Q
Availabilit y	Cloud Connectivity	Site Name	Site Role	Device Model	Serial No		Bandwidth Tier	Management IP	Action	8	
•	 Online 	Branch1	Branch	VPX-SE			20	10.54.82.5	an'	6	
•	 Offline 	brnch3	Branch	VPX-SE			20	Unknown	ø	0	
•	 Inactive 	descent the set of	Branch	VPX-SE			20	Unknown	ø	0	
•	Online	100 AUG 100	MCN	VPX-SE			20	10.62.100.5	ø	6	
•	Online		Branch	VPX-SE			20	10.54.81.4	ø	0	
						Page Size: 50	Showing 1-	5 of 5 items Pa	gel of		

After the Staging and Activation process is complete and the virtual paths are established. You can now manage and monitor the instance using Citrix SD-WAN Orchestrator service.

Create a service principal for deploying VPX in Azure

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

- Subscription ID
- Client ID

- Client Secret
- Tenant ID

Note

After creating the service principal to allow Azure API communication, ensure to associate appropriate roles at the subscription level. Otherwise, Citrix SD-WAN Orchestrator service will not have sufficient permissions to authenticate and deploy resources using Azure APIs that enable automated connectivity.

Perform the following steps to create an application registration:

- 1. In the Azure portal, navigate to **Azure Active Directory**.
- 2. Under Manage, select **App registration**.

3. Click + New registration.



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

• Click Register.

Home > Citrix Systems, Inc. App registrations >
Register an application
* Name
The user-facing display name for this application (this can be changed later).
AZURE_API
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (Citrix Systems, Inc. only - Single tenant)
Accounts in any organizational directory (Any Azure AD directory - Multitenant)
Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
Help me choose
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Web V https://localhost/4980 V
By proceeding, you agree to the Microsoft Platform Policies 🖉
Register

You can copy and store the **Application (client) ID** and the **Directory (tenant) ID** that can be used in the Citrix SD-WAN Orchestrator service for authentication to the Azure subscription for usage of the API.

Home > Citrix Systems, Inc. App registra	ations >	
₽ Search (Ctrl+/) «	🗊 Delete 🜐 Endpoints	
😽 Overview	Display name : AZURE_API	Supported account types : My organization only
📣 Quickstart	Application (client) ID : Clickles, List free, door Trock (clickles)	Redirect URIs : 1 web, 0 spa, 0 public client
🚀 Integration assistant (preview)	Directory (tenant) ID : 03585666 2261488246145 348626696861	Application ID URI : Add an Application ID URI
	Object ID : rateds49cs 200 4a49 col_ascaless90ce	Managed application in I : AZURE_API
Manage		
Branding		
Authentication	Welcome to the new and improved App registrations. Looking to learn how it's changed from the second sec	m App registrations (Legacy)? Learn more

The next step for the application registration, create a service principal key for authentication purposes.

To create the service principal key, perform the following steps:

a) In the Azure portal, navigate to **Azure Active Directory**.

- b) Under Manage, navigate to App registration.
- c) Select the registered application (created previously).
- d) Under Manage, select Certificates & secrets.
- e) Under Client secrets, click + New client secret.

Home > Citrix Systems, Inc. App regist				
AZURE_API Certifie	cates & secrets 🛛 🖈			
	Credentials enable confidential appli scheme). For a higher level of assura	ications to identify themselves to the authentication sen ince, we recommend using a certificate (instead of a clier	vice when receiving tokens at a web addressable location (using nt secret) as a credential.	an HTTPS
🛎 Quickstart	Certificates			
💅 Integration assistant (preview)	Certificates can be used as secrets to	p prove the application's identity when requesting a toke	en. Also can be referred to as public keys.	
Manage	T Upload certificate			
Branding	Thumbprint	Start date	Expires	
Authentication	No certificates have been added for	this application.		
Y Certificates & secrets				
Token configuration				
API permissions	Client secrets			
Expose an API	A secret string that the application u	ises to prove its identity when requesting a token. Also o	can be referred to as application password.	
Owners	+ New client secret			
Roles and administrators (Preview)	Description	Expires	Value	
Manifest	No client secrets have been created	for this application.		
Support + Troubleshooting				
Troubleshooting				
New support request				

- f) To add a client secret, provide values for the following fields:
 - **Description**: Provide a name for the service principal key.
 - **Expires**: Select the duration for expiration as needed.

Add a clie	nt secret		
Description			
SP_KEY			
Expires In 1 year In 2 years Never			
Add	Cancel		

- g) Click Add.
- h) The client secrete is disabled in the **Value** column. Copy the key to your clipboard. This is the Client Secret that you must enter into the Citrix SD-WAN Orchestrator service.

Home > Citrix Systems, Inc. App registra	tions >								
AZURE_API Certifica	ates & secrets 👒								
	Copy the new client secret value. You won't be able to retri	eve it after you perform another ope	eration or leave this blade.						
 Overview Quickstart 	Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.								
💋 Integration assistant (preview)									
Manage	Certificates	dontitu when nonvertices a token	Also can be referred to as nublic loss:						
Branding	Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.								
Output Authentication	Thumberint	Upload certificate							
Y Certificates & secrets		Start date	Expires	-					
Token configuration	No certificates have been added for this application.								
API permissions									
Expose an API	Clast secole								
Owners	A secret string that the application uses to prove its identity w	when requesting a token. Also can	n be referred to as application password.						
Roles and administrators (Preview)	+ New client secret								
Manifest	Description	Expires	Value						
Support + Troubleshooting	SP_KEY	7/28/2021							
// Troubleshooting									
New support request									

Note

Copy and store the secret key value before reloading the page because, it will no longer be displayed afterwards.

Role assignments

You can assign appropriate roles for an authentication purpose at the subscription-level. Perform the following steps for role assignment:

1. On the Azure portal, navigate to the profile name. Right-click the profile name and select My permissions.

2	Ţ	Ω	\$?	ন্থ	
			(Ditrix		Sign out
				8,	Sign in w	My permissions Submit an idea View my bill My contact information

2. On the My permissions page, select the Click here to view complete access details for this subscription link.

My permissions	
P* Resource provider status	
NSDev SDWAN CA	
You have the following access:	
Your account	has been assigned the role 'Owner' (type BuiltInRole) and has access to NSDev SDWAN CA
Click here to view complete access details for	this subscription.

3. On the left navigation section go to Access control (IAM) and select the Role assignments tab and click +.

,P Search (Cmd+/) «	+ Add 🛓 Download role assignments	🎫 Edit columns 🙁 Refresh 🖂 R	ernove 🛛 💙 Got feedback?		
† Overview	Automa Aleximeter A	las Balas Marcial Barrandara	Course and a laboration		
Activity log	Check access Role assignments Ro	ites Koles (Classic) Deny assignment	s Classic administrators		
R Access control (IAM)	Number of role assignments for this subs	cription 💿			
Tags	12	2000			
Diagnose and solve problems					
Security	Search by name or email Type : A	Role : All Scope : All scopes	Group by : Role		
🗲 Events	48 items (25 Users, 5 Groups, 15 Service Pri	ncipals, 2 Unknown, 1 Managed Identities)			
Cost Management	Name Name	Type	Role	Scope	Conditio
	Contributor				

- 4. For "Add role assignment", pick role = "Contributor", Assign access to = "User, group or service principal" and for third drop-down list for Select = Azure App name and then "Save". This grants enough privileges for making API call to Azure using service principal.
- 5. On the Add role assignment page, select the following options:
 - Role: Contributor
 - Assign access to: User, group, or service principal
 - Select: Provide the name of the Azure app.

Add role assignment				
Role ①				
Contributor ①	~			
Assign access to (i)				
User, group, or service principal	\sim			
Select ①				

6. Click **Save**. These steps grant enough privileges for Citrix SD-WAN Orchestrator service to make an API call to Azure using service principal.

Internet breakout for Azure HA site

To configure internet breakout for Azure HA site:

- 1. In the site appliance, configure DHCP IP on the WAN interface with Public IP configured for the WAN link.
- 2. Configure Internet service on the Site.
- 3. Add an Outbound Dynamic port restricted NAT with the inside service as Internet.
- 4. Add a firewall policy on the site to allow Azure load balancer health probes on port number 500.

~	PEPOPTS	<u>\</u>	Built-in Firewall	~		
.1111	IIII REPORTS 7		Match Criteria			
\odot	CONFIGURATION	~	Match Type	Routing Domain		
	Natural Castin Hama	-1	IP Protocol 🗸	Default_RoutingDomain \lor		
)	Delivery Services	>	Filtering Criteria			
	Routing	>	Source Zone		Destination Zone	
	Link Settings	>	Any ×	~	Any X	~
	QoS	>	Source Service Type	Source Service Name*	Source IP	Source Port
	Security	~	Any 🗸	Any \checkmark	Any	Any
	Network Security		Dest Service Type	Dest Service Name*	Dest IP	Dest Port
	Ssid Profiles		Any 🗸	Any 🗸	Any	500
	Radius Profiles		IP Protocol	DSCP		
	Firewall Defaults		TCP (6) 🗸	Any 🗸	Allow Fragments Reverse Als	o Match Established
	Firewall Profiles		Actions			
	Security Profiles					
	SSL Inspection		Action			
		*	Allow 🗸			

5. Add another load-balancing rule on the Azure external load balancer for TCP on port number 80, with direct server return disabled.

Protocol	
• TCP UDP	
Port *	
80	\checkmark
Backend port * ①	
80	\checkmark
Backend pool ①	
sdwan-ext-backendpool (2 virtual machines)	\sim
Health probe ①	
sdwan-ext-tcprobe (TCP:500)	\sim
Session persistence ①	
None	\sim
Idle timeout (minutes) ①	
0	4
TCP reset	
Disabled Enabled	
Electing ID (direct converteture)	
Disabled Enabled	
Yes No	
OK	

6. On the end client machine that must breakout to the internet, set the route next hop IP address to the Internal Load Balancer private IP address. The load balancer IP address is configured as LAN VIP in the site.

Citrix Cloud and Gateway Service optimization

January 28, 2021

With the **Citrix Cloud and Gateway Service optimization** feature enhancement, you can detect and route traffic destined for the Citrix Cloud and Gateway Service. You can create policies to either break the traffic out to internet directly or, to send it via a backhaul route over the virtual path. In the absence of this feature, when the default route is virtual path, gateway service will hairpin back to the customer's Data Center and then would go out to Internet adding unnecessary latency. In addition

to that, you now get visibility into Citrix Gateway service and Citrix Cloud traffic and can create QoS policies to prioritize it over the virtual path.

The **Citrix Cloud and Gateway Service breakout** feature is enabled by default in Citrix SD-WAN software version 11.2.1 and above.

For Citrix SD-WAN software version below 11.3.0, the first packet detection and classification of Citrix Cloud and Gateway Service traffic is performed only if the **Citrix Cloud and Gateway Service break-out** feature is not disabled.

For Citrix SD-WAN software version 11.3.0 and above, the first packet detection and classification of Citrix Cloud and Gateway Service traffic is performed irrespective of whether the **Citrix Cloud and Gateway Service breakout** feature is enabled or not.

Note

- You can configure the Citrix Cloud and Gateway Service optimization only through the Citrix SD-WAN Orchestrator service.
- **Citrix SD-WAN Orchestrator traffic optimization** is introduced from Citrix SD-WAN software version 11.2.3 or higher. The goal is to provide a more granular classification, and thus, separately identify Citrix SD-WAN Orchestrator traffic and other dependent services' traffic from Citrix Cloud, and provide an Internet breakout option. As a result, customers can now choose to optimize only the Citrix SD-WAN Orchestrator traffic.

On selecting the **Citrix Cloud** check box, the **Citrix SD-WAN Orchestrator and dependant critical services** check box is preselected. This allows all Citrix Cloud Web UI and API traffic (including that of Orchestrator and dependent services) in the firewall and takes internet breakout.

Also, you can choose to select only **Citrix SD-WAN Orchestrator and dependant critical services** check box and disable other traffic to give the privilege of bypassing firewall just to Orchestrator related traffic seamlessly.

Cost Ranges: Custom Application (1-20) Application (21-40) Application Group (41-60) IP (1-65535)					
Application Group Match Criteria					
Match Type Application Group*					
Application Group \checkmark Citrix_Cloud_and_Gateway_service \checkmark					
Scope					
Global Route Site / Group Specific Route					
Traffic Steering					
Delivery Service					
Internet Breakout					
Citrix Gateway and Citrix Cloud Optimization settings					
Citrix Cloud (Enable to detect and route traffic destined for Citrix cloud Web UI and API.)					
Citrix SD-WAN Orchestrator and dependent critical services					
Citrix Gateway Service (Enable to detect and route control and data traffic destined for Citrix Gateway Service.)					
Cancel Save					

Citrix Cloud and Gateway Service categories

Following are the traffic categories used for classification and optimization purposes:

- Citrix Cloud: Enable to detect and route traffic destined for Citrix Cloud Web UI and APIs.
 - Citrix SD-WAN Orchestrator and dependant critical services:
 - * **Citrix SD-WAN Orchestrator**: Enables direct internet breakout of heartbeat and other traffic required to establish and maintain connectivity between Citrix SD-WAN appliance and Citrix SD-WAN Orchestrator.
 - * **Citrix Cloud Download Service**: Enables direct internet breakout for download of appliance software, configuration, scripts, and other requirements onto the Citrix SD-WAN appliance.
- **Citrix Gateway Service**: Enable to detect and route traffic (control and data) destined for Citrix Gateway Service.
 - **Gateway Service Client Data**: Enables direct internet breakout of ICA data tunnels between clients and Citrix Gateway Service. It requires high bandwidth and low latency.
 - Gateway Service Server Data: Enables direct internet breakout of ICA data tunnels between Virtual Delivery Agents (VDAs) and Citrix Gateway Service. It requires high band-
width and low latency and only relevant in VDA resource locations (VDA to Citrix Gateway Service connections).

- Gateway Service Control Traffic: Enables direct internet breakout of the control traffic. No specific QoS considerations.
- **Gateway Service Web Proxy Traffic**: Enables direct internet breakout of the Web proxy traffic. It requires high bandwidth but latency requirements might vary.

Prerequisites

Ensure that you have the following:

- 1. To perform the Citrix Cloud and Gateway Service breakout, an Internet service has to be configured on the appliance. For more information on configuring an Internet service, see Internet access.
- 2. Ensure that the Management interface has internet connectivity. If the dedicated management interface is not connected, ensure that in-band management is enabled and outbound management traffic has internet connectivity.
- 3. You can use the Citrix SD-WAN web interface to configure the management interface settings.
- Ensure that the management DNS is configured. To configure management interface DNS, at site level navigate to Configuration > Appliance Settings > Network Adapter. Under the DNS Settings section, provide the primary and secondary DNS server detail and click Save.

Site Configuration : Appliance Settings

	made wethow host settings wetwork Adapters Ap	
IP Address		
Enable DHCP		
IP Address *	Subnet Mask * Gateway	IP Address *
DNS Settings		
DNS Settings Primary DNS	Secondary DNS	
DNS Settings Primary DNS	Secondary DNS	
DNS Settings Primary DNS	Secondary DNS	
DNS Settings Primary DNS Save	Secondary DNS	

How Citrix Cloud and Gateway Service optimization works

1. The Citrix SD-WAN appliance downloads a list of application signatures using the cloud service API.

- 2. When a request for the Citrix Cloud and Gateway Service application arrives, the application is classified on the first packet using the signatures.
- 3. Once the Citrix Cloud and Gateway Service traffic is classified, the auto created application route and firewall policies take effect and breaks out the traffic directly to the Internet.
- 4. The Citrix Cloud and Gateway Service use Quad9 by default for forwarding DNS requests.

Traffic flow with/without breakout enabled

- . **Control Traffic:** SD-WAN Branch 2 Data Traffic: CMD / CVAD Service 5) Virtual Path Gateway S (4) 3 2 1 Virtual Path MCN SD-WAN Branch 1 ce Clien
- Without breakout enabled:

• With breakout enabled:



If you use a cloud security stack (for example - Zscaler, Check Point, Palo Alto) to process internet traffic, the Gateway Service receives packets from the public IP address of that security stack, instead of the SD-WAN branch. This defeats Direct Workload Connection and thus, packets to the cloud-hosted SD-WAN will not be able to take Virtual Path. For more information, see <u>Direct Workload Connec-</u> tion.

By enabling breakout, the Gateway Service receives packets directly from the SD-WAN branch. Dynamic Virtual Paths come up between the SD-WAN branch and the cloud-hosted SD-WAN and the traffic goes via this virtual path between the two sites. For more information on enabling the Dynamic Virtual Paths, see Setup dynamic paths for branch to branch communication.



By enabling breakout, traffic required to establish and maintain connectivity between Citrix SD-WAN devices and Citrix SD-WAN Orchestrator will no longer be backhauled through the data center. The traffic reaches Citrix SD-WAN Orchestrator by directly breaking out to internet from the branches where the Citrix SD-WAN devices are located.



Configure Gateway Service breakout

The Citrix Cloud and Gateway Service breakout policy allows you to specify which category of Citrix Cloud and Gateway Service traffic you can directly break out from the SD-WAN branch.

The Citrix Cloud and Citrix Gateway Service options are available under Citrix Gateway and Citrix Cloud Optimization settings.

Citrix applications can access several services in the Citrix Cloud. For details, see System and Connectivity Requirements.

In the Citrix SD-WAN Orchestrator service, by-default every network has the Citrix Cloud and Gateway Service route. To navigate, go to **Network Configuration > Routing > Routing Policies > Application Routes**.

	Verify Config Appli	cation Routes IP Ro	outes				
Cost Ran	ges: Custom Application	(1-20) Application (21	L-40) Application Group (41-	60) IP (1-65535)			
+ Ap	oplication Route		Search for Route		Q		
No	Match Type	Name	Delivery Service	Routing Domain	Sites	Cost	Actions
1	Application	Facebook	Local	Any	Delhi_Br1	21	
2	Application	Youtube.com	Local	Any	Bengaluru	21	İ
3	Application Group	Default Cloud Dir	Cloud Direct Service	Any	Global	45	
4	Application Group	O365Optimize_In	Internet Breakout	Any	Global	50	Ŵ
5	Application Group	Citrix_Cloud_and	Internet Breakout	Any	Global	50	Î

You cannot delete the route but you can configure the settings as required. The **Citrix Cloud and Gateway Service** are enabled by-default.

Verify Config Application Routes IP Routes
Cost Ranges: Custom Application (1-20) Application (21-40) Application Group (41-60) IP (1-65535)
Application Group Match Criteria
Match Type Application Group* Application Group Citrix_Cloud_and_Gateway_service
Scope
Global Route O Site / Group Specific Route
Traffic Steering
Delivery Service
Citrix Gateway and Citrix Cloud Optimization settings
 Citrix Cloud (Enable to detect and route traffic destined for Citrix cloud Web UI and APL) Citrix SD-WAN Orchestrator and dependent critical services Citrix Gateway Service (Enable to detect and route control and data traffic destined for Citrix Gateway Service.)
Cancel Save

Transparent forwarder for Citrix Cloud and Gateway Service

The SD-WAN branch breaks out for the Citrix Cloud and the Gateway Service begins with a DNS request. The DNS request going through the Citrix Cloud and Gateway Service domains have to be steered locally. If Citrix Cloud and Gateway Service Internet break out is enabled, the internal DNS routes are determined. Citrix Cloud and Gateway Service DNS requests are forwarded to open source DNS service Quad 9 by default. Quad 9 DNS service is secure, scalable, and has multi pop presence. You can change the DNS service if necessary.

To add a DNS server, at site level, navigate to **Configuration > Advanced Settings > DNS**. Under **Site Specific DNS Servers** section, click **+ DNS Server**.

1 •	/erify Config	Virtual Paths	NAT	DHCP	VRRP	Routes	Multicast Groups	DNS	LAG	WAN Optimiz
ite Spec	ific DNS Serve	ers								
+ DN	IS Server									
No	DNS Server	Name		Primary Di	NS		Secondary DNS			Actions
NS Prox	ties									
NS Prox + DN	ties IS Proxy									
NS Prox + DN	I <mark>S Proxy</mark> DNS Proxy 1	Name				Default DNS Se	rver			Actions
NS Prox + DN	I <mark>S Proxy</mark> DNS Proxy 1	Name				Default DNS Sei	rver			Actions
+ DN No	IS Proxy DNS Proxy 1	Name				Default DNS Se	rver			Actions
NS Prox + DN No NS Tran	S Proxy DNS Proxy I Sparent Forw	Name				Default DNS Se	rver			Actions
+ DN + DN No NS Tran + Ap	sparent Forw	Name arders S Forwarding	Rule			Default DNS Se	rver			Actions
 NS Prox + DN No NS Tran + Ap • Top c 	SProxy DNS Proxy DNS Proxy Sparent Forw Specific DN Of List Bot	Name arders S Forwarding tom of List	Rule	ow Numbe	er Ro	Default DNS Se	rver			Actions

Site Configuration : Advanced Settings

Transparent forwarders for Citrix Cloud and Gateway Service applications are created at every SD-WAN branch that has Internet service and Citrix Cloud and Gateway Service breakout enabled.

To add a specific DNS forwarding rule, click **+ App Specific DNS Forwarding Rule** under **NDS Transparent Forwarder** section. With this configuration, you can choose to change the default Quad9 DNS transparent forwarder for Citrix Cloud and Gateway Service Applications.

DNS Transpare	nt Forwarder		
Application *			DNS Server *
Citrix Gateway	service Control Traffic	\sim	
Cancel	Save		

• Application: Select the Citrix Cloud and Gateway Service application from the Application

drop-down list.

• **DNS Server**: Select the DNS server that you created under **Site Specific DNS Servers** from the drop-down list.

Monitoring

You can monitor the Citrix Cloud and Gateway Service real-time statistics and usage report as the following:

Real-time Statistics

Network Reports : Real Time Statistics

ARP	Routes Virtual Path Services	Classes Ethern	et Obse	erved Protocols	Wan Path	Application QOS	Application	n Routes 🗡	
Branch	1_Site	✓ Retrieve	latest data	1					
Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Туре	Cost	Hit Count
0	row_index	app_name	gw_ip	service	firewall_zon	e reachable	site_name	route_type	cost
0	O365Optimize_InternetBre		Internet	Internet_Zone	YES	Branch1_Site	Static	50	0
1	NGS_WebProxy_Breakout	•	Internet	Internet_Zone	YES	Branch1_Site	Static	50	0
2	NGS_ServerData_Breakout	•	Internet	Internet_Zone	YES	Branch1_Site	Static	50	0
3	NGS_ControlTraffic_Breako	•	Internet	Internet_Zone	YES	Branch1_Site	Static	50	0
4	NGS_ClientData_Breakout	•	Internet	Internet_Zone	YES	Branch1_Site	Static	50	398
5	CitrixCloud_Breakout	•	Internet	Internet_Zone	YES	Branch1_Site	Static	50	21
()									

Network Reports : Real Time Statistics

ARP	Routes Virtual Path Service	s Classes Etherne	t Observed	Protocols Wan Path	Applicatio	n QOS Ap	oplication I	Routes 🗡		
azure0	7	 Retrieve 	atest data							
dianeo	,									
Num	Application Object	Gateway IP Address	Service	Firewall Zone	Read	hable Si	te	Туре	Cost	Hit Count
0	row_index	app_name	gw_ip	service	firew	vall_zone re	achable	site_name	route_type	cost
0	O365Optimize_InternetBre	•	Internet	Untrusted_Internet_Zon	YES	az	ure07	Static	50	1917
1	NGS_WebProxy_Breakout	•	Internet	Untrusted_Internet_Zon	YES	az	zure07	Static	50	0
2	NGS_ServerData_Breakout	•	Internet	Untrusted_Internet_Zon	YES	az	zure07	Static	50	9361
3	NGS_ControlTraffic_Breako	•	Internet	Untrusted_Internet_Zon	YES	az	zure07	Static	50	18105
4	NGS_ClientData_Breakout	•	Internet	Untrusted_Internet_Zon	YES	az	zure07	Static	50	0
5	CitrixCloud_Breakout	•	Internet	Untrusted_Internet_Zon	YES	az	ure07	Static	50	222

Network	Reports: Real Time Statis	stics									Site G	Broup: All	~
ARP	Routes Virtual Path Services	Classes Interfac	es Observ	ed Protocols	Wan Path A	pplication QOS Appl	ication Rout	tes 🗡					
BRANG	CH1_KVMVPX	 ✓ Ret 	rieve latest d	ata									Q
Num	Application Object	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Туре	Cost	Hit Count	Eligible	Eligible Type	Eligible Value	
0	CitrixSdwanOrchestrator_Breakout	•	Internet	Internet_Zone	YES	BRANCH1_KVMVPX	Static	50	41	YES	N/A	N/A	
1	CitrixCloudDownloadSvc_Breakout	•	Internet	Internet_Zone	YES	BRANCH1_KVMVPX	Static	50	8	YES	N/A	N/A	

Real-time Firewall Connections

Network Reports : Real Time Firewall Connections

Branch1_Site V Retrieve late Connections Displayed: 32 Connections In Use: 32/128000	st data											-Int
						S	ource					Destination
Application	Family	Routing Domain	IP Protocol	IP Addr	Port	Service Type	Service Name	Zone	IP Addr	Port	Service Type	Service Name
Domain Name Service(dns)	Network Service	Default_Routing	UDP	10.23.1.5	64091	Local	VIF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet
Citrix Cloud Web UI and API(citrix_cloud_web_ui_api)	Custom Application	Default_Routing	TCP	10.23.1.5	49967	Local	VIF-1-LAN-1	Default_LAN_Zone	52.177.206.73	443	Internet	Branch1_Site-Internet
Domain Name Service(dns)	Network Service	Default_Routing	UDP	10.23.1.5	61865	Local	VIF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet
Domain Name Service(dns)	Network Service	Default_Routing	UDP	10.23.1.5	60077	Local	VIF-1-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	Branch1_Site-Internet
Citrix Gateway service Client Data(ngs_client_data)	Web	Default_Routing	TCP	10.23.1.5	49974	Local	VIF-1-LAN-1	Default_LAN_Zone	13.93.207.26	443	Internet	Branch1_Site-Internet
Citrix Cloud Web UI and API(citrix_cloud_web_ui_api)	Custom Application	Default_Routing	TCP	10.23.1.5	49749	Local	VIF-1-LAN-1	Default_LAN_Zone	52.177.88.75	443	Internet	Branch1_Site-Internet
Citrix Gateway service Client Data(ngs_client_data)	Web	Default_Routing	UDP	10.23.1.5	60079	Local	VIF-1-LAN-1	Default_LAN_Zone	13.93.207.26	443	Internet	Branch1_Site-Internet

Network Reports : Real Time Firewall Connections

Site Group: All

Site Group

azure07 V Retrieve latest o	lata											-Internet
Connections Displayed: 170 Connections In Use: 170/768000												
							Source					Destination
Application	Family	Routing Domain	IP Protocol	IP Addr	Port	Service Type	Service Name	Zone	IP Addr	Port	Service Type	Service Name
Citrix Gateway service Control Traffic(ngs_control_traffic)	Web	Default_RoutingDomain	TCP	172.16.70.4	64280	Local	VIF-LAN-1	Default_LAN_Zone	40.112.143.211	443	Internet	azure07-Internet
Citrix Gateway service Control Traffic(ngs_control_traffic)	Web	Default_RoutingDomain	TCP	172.16.70.4	49615	Local	VIF+LAN-1	Default_LAN_Zone	40.112.143.211	443	Internet	azure07-Internet
Citrix Gateway service Control Traffic(ngs_control_traffic)	Web	Default_RoutingDomain	TCP	172.16.70.4	49622	Local	VIF-LAN-1	Default_LAN_Zone	40.112.143.211	443	Internet	azure07-Internet
Citrix Gateway service Control Traffic(ngs_control_traffic)	Web	Default_RoutingDomain	TCP	172.16.70.5	49281	Local	VIF-LAN-1	Default_LAN_Zone	40.112.143.211	443	Internet	azure07-internet
Citrix Gateway service Control Traffic(ngs_control_traffic)	Web	Default_RoutingDomain	TCP	172.16.70.4	49620	Local	VIF-LAN-1	Default_LAN_Zone	40.112.143.211	443	Internet	azure07-Internet
Citrix Gateway service Control Traffic(ngs_control_traffic)	Web	Default_RoutingDomain	TCP	172.16.70.5	49287	Local	VIF+LAN-1	Default_LAN_Zone	40.112.143.211	443	Internet	azure07-Internet
Citrix Gateway service Control Traffic(ngs_control_traffic)	Web	Default_RoutingDomain	TCP	172.16.70.5	49283	Local	VIF+LAN-1	Default_LAN_Zone	40.112.143.211	443	Internet	azure07-Internet
Citrix Gateway service Control Traffic(ngs_control_traffic)	Web	Default_RoutingDomain	TCP	172.16.70.5	64006	Local	VIF+LAN-1	Default_LAN_Zone	40.112.143.211	443	Internet	azure07-Internet
Citrix Gateway service Control Traffic(ngs_control_traffic)	Web	Default_RoutingDomain	TCP	172.16.70.5	49285	Local	VIF-LAN-1	Default_LAN_Zone	40.112.143.211	443	Internet	azure07-Internet
Citrix Gateway service Control Traffic(ngs_control_traffic)	Web	Default_RoutingDomain	TCP	172.16.70.4	49618	Local	VIF-LAN-1	Default_LAN_Zone	40.112.143.211	443	Internet	azure07-Internet
Domain Name Service(dns)	Network Service	Default_RoutingDomain	UDP	172.16.70.5	61863	Local	VIF-LAN-1	Default_LAN_Zone	9.9.9.9	53	Internet	azure07-Internet

Network	Reports:	Real	Time	Firewall	Connections

BRANCHI_KVMVPX ~ Maximu	n number of Connection	is to display	 Retrieve lat 	est data Se		Q Customize Columns		
				Source		Destina	tion	
Application	Family	Routing Domain	IP Addr	Service Type	IP Addr	Service Type	State	Is NAT
Citrix Cloud Download Service(citrix_cloud_download_svc)	Web	Default_RoutingDomain	172.16.30.30	Local	34.226.77.219	Internet	SYN_SENT	YES
Citrix SD-WAN Orchestrator(citrix_sdwan_orchestrator)	Web	Default_RoutingDomain	172.16.30.30	Local	18.213.26.194	Internet	CLOSED	YES
Domain Name Service(dns)	Network Service	Default_RoutingDomain	172.16.30.30	Local	9.9.9.9	Internet	ESTABLISHED	YES
Domain Name Service(dns)	Network Service	Default_RoutingDomain	172.16.30.30	Local	8.8.8.8	Virtual Path	ESTABLISHED	NO
Domain Name Service(dns)	Network Service	Default_RoutingDomain	172.16.30.30	Local	9.9.9.9	Internet	ESTABLISHED	YES
Google Generic(google_gen)	Web	Default_RoutingDomain	172.16.30.30	Local	172.217.167.142	Virtual Path	CLOSED	NO

1 to 6 of 6 - I < < Page 1 of 1 > >I

Site Group: All 🗸

• Usage

Application Usage t Type op Apps windows_marketplace op Applications Applications	Apps Apps All e (72%) windows_update (14%)	microsoft (5%) windows_az	Top Applications	S		
t Type op Apps windows_marketplace op Applications Applications	Apps All e (72%) windows_update (14%)	microsoft (5%) windows_az	Top Applications	5		
windows_marketplace op Applications Applications	All e (72%) windows_update (14%)	microsoft (5%) windows_az	Top Application:	s		
windows_marketplace op Applications	e (72%) 👅 windows_update (14%) 📕	microsoft (5%) windows_az	Top Application:	s		
windows_marketplace op Applications	e (72%) 📕 windows_update (14%) 📕	microsoft (5%) 💼 windows_az				
Applications			ure (4%) 📕 https (3%) 📕 Others ((2%)		Search
	Total Data	Upload Data	Download Data	Total Bandwidth	Upload Bandwidth	Download Bandw
windows_marketpla	lace 1.4 GB	475.78 MB	926.1 MB	3.46 Mbps	1.17 Mbps	2.29 Mbps
windows_update	274.18 MB	93.3 MB	180.89 MB	1.11 Mbps	376.95 Kbps	730.86 Kbps
microsoft	88.2 MB	40.54 MB	47.66 MB	103.15 Kbps	47.41 Kbps	55.74 Kbps
windows_azure	78.34 MB	31.25 MB	47.09 MB	86.33 Kbps	34.43 Kbps	51.89 Kbps
https	56.67 MB	29.18 MB	27.49 MB	78.72 Kbps	40.53 Kbps	38.18 Kbps
ldap	15.06 MB	7.43 MB	7.64 MB	24.8 Kbps	12.23 Kbps	12.57 Kbps
ngs_control_traffic	11.57 MB	1.79 MB	9.78 MB	37.63 Kbps	5.81 Kbps	31.82 Kbps
cedexis	2.86 MB	1.22 MB	1.64 MB	9.53 Kbps	4.07 Kbps	5.46 Kbps
windowslive	1.39 MB	600.36 KB	786.1 KB	6.38 Kbps	2.76 Kbps	3.61 Kbps
) ngs_server_data	1.31 MB	1.01 MB	298.02 KB	9.72 Kbps	7.51 Kbps	2.21 Kbps
ngs_client_data	1.26 MB	232.74 KB	1.03 MB	10.51 Kbps	1.94 Khor	8 57 Khos

Troubleshooting

The connectivity errors are logged in **SDWAN_dpi.log** file. To download the log file, navigate to **Troubleshooting > Device Logs**, select the required site, choose the log file, and click **Download**.

Customer / Site / All Sites >					?
DASHBOARD	Network TroubleShooting : Device Logs				
REPORTS >	Select Site				
CONFIGURATION >	🕁 Download (1.24 MB / 1 GB)				Q
\gtrsim troubleshooting \sim	SDWAN_dpi.old.log	Last Modified July 25, 2020 4:14 PM	Size		
Audit Logs	SDWAN_dpillog	July 27, 2020 12:36 PM	1.24 MB		
Device Logs			Page Size: 25 V Showing 1 - 2 o	f 2 items Page 1 of 1	< ►
Diagnostics					
ADMINISTRATION >					

You can also verify the device alerts. To verify, navigate to **Network > Alerts**.

Customer Site SDWAN / All Sites	s ~						0
DASHBOARD		Netwo	ork Reports	: Alerts			Site Group: All 🗸
REPORTS	~	t.	Delete Alerts			Q	1455 250 797 408 TOTAL HIGH MEDIUM LOW
Alerts			Severity	Site	Source	Message	Time
Usage			😑 High	Branch1_Site	APPLIANCE	Failed to connect to the CGS service API	Jul 15th 2020, 5:40 pm
Inventory							
Security	>						Showing 1-1 of 1 items Page 1 of 1 < 🕨
HDX	>						

PE support: WAN optimization configuration

July 28, 2021

You can configure and deploy Citrix SD-WAN Premium Edition (PE) through Citrix SD-WAN Orchestrator service. You can now configure WAN Optimization Configurations like Features, Tuning, Applications, and Rules through SD-WAN Orchestrator. Deployment of SD-WAN PE appliances is also now possible through Orchestrator.

NOTE

The Citrix SD-WAN PE is only supported on Citrix SD-WAN 1100, 2100, 5100, and 6100 platforms.

The WAN optimization features can be applied per site wise or globally to all the sites of the network. Citrix SD-WAN Orchestrator service provides step-by-step instructions for enabling and configuring the PE WAN Optimization features for your Virtual WAN.

Note

You must have a Citrix SD-WAN PE license installed to access, enable, configure, and activate WAN Optimization features in your Virtual WAN.

To globally configure PE WAN Optimization features, navigate to **Configuration > WAN Optimization** at network level. You need to configure the following features to complete the global WAN optimization configuration:

- Features
- Tuning
- WAN Opt Apps
- WAN Opt App Groups
- Rules

Features

To enable the WAN Optimization in the Features settings, navigate to **Configuration > WAN Optimiza-tion > Features**.

You can also accept the default settings pre-selected in the form, or customize the settings. Click the check boxes to select or deselect an option.

VAN Optimization Features	
WAN Optimization	SSL Optimization
RPC Over HTTP	SCPS
User Data Store Encryption	Native MAPI
HDX QoS Priorities	MAPI Cross Protocol Optimization
IFS Optimization Protocols	
SMB1	
SMB2	
SMB3	

The Features configuration page contains the following two sections:

- WAN Optimization Features
- CIFS Optimization Protocols

WAN Optimization Features

- **WAN Optimization**: Enable WAN Optimization for this configuration. This also enables compression, deduplication, and TCP Protocol Optimization.
- **SSL Optimization**: Enable optimization for traffic streams with SSL encryption.
- **RPC Over HTTP**: Enable optimization of Microsoft Exchange traffic that uses RPC over HTTP.
- **SCPS**: Enable TCP Protocol optimization for Satellite Links.
- User Data Store Encryption: Enable enhanced security of data through the encryption of WAN Optimization compression history.
- Native MAPI: Enable optimization of Microsoft Exchange traffic.

- HDX QoS Priorities: Select the check box to enable optimization of ICA traffic based on prioritization of HDX subchannels.
- **MAPI Cross Protocol Optimization**: Enable cross-protocol optimization of Microsoft Outlook (MAPI) traffic.

CIFS Optimization Protocols

The CIFS Optimization Protocols options are as follows:

- SMB1: Select the check box to enable Optimization of Windows File Sharing (SMB1).
- SMB2: Select the check box to enable Optimization of Windows File Sharing (SMB2).
- **SMB3**: Select the check box to enable Optimization of Windows File Sharing (SMB3). You must first select the SMB2 option before you can select SMB3.

Click **Save** to enable and add the selected Features to the configuration package.

Tuning

To configure the WAN Optimization Tuning settings, navigate to **Configuration > WAN Optimization > Tuning**.

MAN Optimization		
Aaximum MSS	Default MSS	
1350	1350	
Enable Connect	on Timeout	
3600		

The **Tuning** settings options are as follows:

- **Maximum MSS**: Enter the maximum size (in bytes) for the Maximum Segment Size (MSS) for a TCP segment.
- Default MSS: Enter the default size (in octets) for the MSS for TCP segments.
- **Enable Connection Timeout**: Select the check box to enable automatic termination of a connection when the idle threshold is exceeded.
- **Idle Timeout (s)**: Enter a threshold value (in seconds) to specify the amount of idle time permitted before an idle connection is terminated.

NOTE

You must first select the Enable Connection Timeout check box before the Idle Timeout (s) field can be configured.

Click **Save** to apply the **Tuning** settings to the global configuration.

WAN Opt Apps

In the Citrix SD-WAN on-premises appliances, you can see the **WAN Opt Apps** option as **Application Classifiers** under the configuration editor. The **Application Classifiers** option name is changed to **WAN Opt Apps** in SD-WAN Orchestrator.

To configure the WAN Optimization Applications, navigate to **Configuration > WAN Optimization > WAN Opt Apps**.

Verify Config	NAN Opt Apps				
+ WAN Opt App					
Name	Description	Application Group	Classifier Type	PORT	Action
Echo	Echo Protocol	network management	TCP	7	Û
Daytime	Daytime	network management	TCP	13	Û
FTP data (clear)	FTP data transport channel	ip protocols	TCP	20	11
FTP command (clear)	File Transfer Protocol command ch	ip protocols	TCP	21	Î
SSH	Secure Shell remote login protocol	security protocols	TCP	22	iii
Telnet	Telnet terminal service group	session	TCP	23	II
SMTP (clear)	Mail transmission	email and collaboration	TCP	25	Û
Time Server	Time Server	servers, network management	TCP	37	Û
TACACS	Login host protocol	directory services	TCP	49	Û
DNS	Domain Name Service	directory services, infrastructure	TCP	53	Û
WHOIS	WHOIS service	directory services	TCP	63	Î
Gopher	Search application	servers	TCP	70	Î
Finger	Finger User Information Protocol	directory services	TCP	79	Î

The WAN Optimization Applications page displays some default set of applications.

You can also add a new application.

1. Click + WAN Opt App option.

Verify Config WAN Opt Ag	aps		
Name *	Description		
site1			
Classification Type	Port *	Application Groups	
ТСР	5411	citrix protocols	\sim
Cancel Save			

- 2. Enter an application name and description.
- 3. Provide the port number for the application.
- 4. Select the application group from the drop-down list.
- 5. Click Save.

You can delete an existing application using the trashcan icon under the Action column.

WAN Opt App Groups

The **WAN Optimization Application Groups** page displays the default set of application groups. Instead of having a large applications list, you can now create an application group with similar application class. For example, ICA application group contains ICA and ICA CGP applications. This page displays the default set of application groups.

You can also create an application group.

1. Click the + WAN Opt App Group option to create an application group.

+ WAN Opt App Group	Reset to Defai
	Reset to Defat
Name	Action
ICA	±
Web (Private)	
Web (Private-Secure)	
Web (Internet)	a
Web (Internet-Secure)	±
CIFS	
NFS	Û
Microsoft Exchange (MAPI)	a
Mail (Other)	Ê
VOIP and Multimedia	a
FTP Data	a
FTP Control	
	•

2. Provide a name to your application group. Search the application from the drop-down list and click **Add**.

Actions	
Ê	
Ê	
Ê	
Ê	
1	
â	
	Actions

3. Click Save.

You can also edit the existing application group. Click the application group row in the existing table to edit. You can add more such applications or delete any application.

Click the **Reset to Defaults** button to retrieve the list of default WAN optimization application groups. This action deletes the previously created WAN optimization application groups and the modified WAN optimization application groups.

Rules

In the Citrix SD-WAN on-premises appliances, you can see the **Rules** option as **Service Classes** under the configuration editor. The **Service Classes** option name is changed to **Rules** in SD-WAN Orchestrator. The **Rules** page displays the default set of pre-created rules. You can also create rule for the application group.

1. Click + **Rule** to create a rule.

Verify Config Rule	-			
+ Rule				Reset to Defaul
Order Number	Name	Status	Acceleration	Action
100	ICA	Enabled	none	₿.
200	Web (Private)	Enabled	none	Ê
300	Web (Private-Secure)	Enabled	none	Ē
400	Web (Internet)	Enabled	none	Ē
500	Web (Internet-Secure)	Enabled	none	Ê
600	CIFS	Enabled	none	Ê
700	NFS	Enabled	none	Ē
800	Microsoft Exchange (MAPI)	Enabled	none	Ê
900	Mail (Other)	Enabled	none	Ē
1000	VOIP and Multimedia	Enabled	none	Ē
1100	FTP Data	Enabled	none	Ē
1200	FTP Control	Enabled	none	Ê
1300	Instant Messaging	Enabled	none	Ē
1400	Session Applications	Enabled	none	Ē
1500	Directory and Security	Enabled	none	Ē

2. Provide the details for the following basic settings:

- Name: Provide a name to the application.
- **Order**: Provide the order number.
- **Enabled**: Select the check box to enable the rule.
- **Acceleration Policy**: Select a policy from the drop-down list. You can select one of the following options as needed:
 - none: Select none if you do not want to enable an acceleration policy for this Rule.
 A policy of none is generally used only for uncompressible encrypted traffic and realtime video.
 - flow control only: Select the flow control only policy to disable compression but enable flow-control acceleration. Select this for rules that are always encrypted, and for the FTP control channel.
 - disk –Select the disk policy to specify the appliance disk as the location for storing the traffic history used for compression. This enables Disk Based Compression (DBC) policy for this Rule. Generally, a policy of disk is usually the best choice, as the appliance automatically selects disk or memory as the storage location, depending on which is more appropriate for the traffic.

- **memory**: Select the memory policy to specify memory as the location for storing the traffic history used for compression.
- **Enable AppFlow Reporting**: Select the check box to enable AppFlow reporting for this Service Class. AppFlow is an industry standard for unlocking application transactional data processed by the network infrastructure. The WAN Optimization AppFlow interface works with any AppFlow collector to generate reports. The collector receives detailed information from the appliance, using the AppFlow open standard.
- **Exclude from SSL Tunnel** –Select the check box to exclude traffic associated with the Service Class from SSL Tunneling.

Verify Config	Rules

Rules						
Name*	Order Number* 123456		Enabled			
Acceleration policy disk ~						
Enable AppFlow Reporting Exclude from SSL Tunnel Application Group Rules						
+ Application Group Ru	le					
Application	Source IP Address	Destination IP Address	Direction	Action		
Cancel Save						

- 3. Click **+ Application Group Rule** to attach the pre-created application group and provide the necessary details for the following fields:
 - **Direction**: Select direction as **BIDIRECTIONAL** or **UNIDIRECTIONAL** from the drop-down list.
 - Application Group: Select an application group from the drop-down list.
 - **Source IP**: Enter the source IP address. Click **+ Source IP Address** to add multiple source IP addresses. Select the **Exclude** check box to exclude the specified source IP address from this rule. Clear the check box to include the address.
 - Destination IP: Enter the destination IP address. Click + Destination IP Address to add multiple destination IP addresses. Select the Exclude check box to exclude the specified

source IP address from this rule. Clear the check box to include the address.

Application Group Rules				
Direction	Application Group			
BIDIRECTIONAL	ICA			~
+ Source IP Address				
Source IP		Exclude	Delete	
Source IP				
+ Destination IP Address				
Destination IP		Exclude	Delete	
Destination IP				
Cancel Done				

4. Click Done.

Click any rule row from the existing table that you want to edit. Make the change as needed and click **Save**. Also, you can delete the existing Rule.

Click the **Reset to Defaults** button to retrieve the list of default rules. This action deletes the previously created rules and the modified rules.

Custom rules that are created cannot have an order value greater than 2000. Following are the default pre-defined rules that have fixed order values, and are non-editable:

- Other TCP traffic 2000
- Unclassified Traffic 2100

Deployment

All of the **WAN optimization configuration** settings are entitled to change management. Once the WAN Optimization configuration is done, you can proceed with **Staging** and **Activation** to start the virtual machine.

As the WAN optimization runs as a virtual machine, it has a different binary file that has to be downloaded to start the virtual machine. In Citrix SD-WAN Orchestrator service, the binary file transfer happens during the staging in the background and it is tied to the change management.

Note

As the binary file download happens during the staging, it takes some additional time to down-

load.

Prerequisites

To perform the change management, ensure that the following actions are completed:

- 1. To configure an appliance as PE, the device edition must be set as **PE**.
- 2. Apply for a PE license. An appliance must have an appropriate PE license. The license code is provided by the Citrix team.

Go to the **Administrator > Licensing**. Click **Retrieve Licenses** option, provide the code, and click **Submit**.

Retrieve Licenses		
+ License Access Code		
	Submit	Cancel

You can see the number of licenses available with the associated device model.

Network A	dministrati	on: Licens	ing					Licensing Model	l: Prepaid Annual An	d Perpetual
Retrieve L	icenses	Upgrade	to Production							
License View	v Site View								Search	Q
SDWAN Entitle	ements									
Device Model	Device Edition PE	Bandwidth	Expiration Date	Licens SD-W	se Type VAN softwar	License Access Code	Licenses Available 49	Assigned To Sites	Actions Assign Unassign	
						Page Size:	200 V Show	wing 1 - 1 of 1 items	Page1 of1	\rightarrow
Add-On Entitle Bandwidth	ements Expiration Date		License Type		License Access	Licenses	Assigned To Si	tes Type	Actions	
					code	Page Size:	200 V Show	wing 0 - 0 of 0 items	Page1 of1	< ►
Orchestrator E Total : 50 Expires : May 2	<u>Entitlements</u> 5, 2021 5:30 AM									
License Access Co	ode		Licenses Available							
1598961422			49							
Page	Size: 200 V	Showing 1	1 of 1 items Pa	agel ofl 🛛 🔍	Þ					

You can **Assign** or **Unassign** the license to the PE configured site as needed. You can also get an option to view the licensed and unlicensed site. By default, when you create a site, you get a Standard Edition (SE) grace license for 20 days.

Note

To apply the PE license, it has to match with the site properties (Device Model, Device Edition, and Bandwidth Tier).

Details	s of Licensed Site	25					
View:	All Licensed All	Unlicensed					
	Site	Device	Device Model	Configured Bandwidth	Expiration Date		
\checkmark	petest2100	primary	CB2100	500	16205616000	000	
			Page Size:	200 V Showing 1 - 1	of 1 items	Page1 of1	<>
				Car	rel	LinAssi	an -
				Cal		UllAssi	911

Once you configure the site as PE, select the software version as 11.2.2.14 and click **Deploy Config/-Software**.

Note

Citrix SD-WAN PE Support through SD-WAN Orchestrator is currently only available for SD-WAN software version of 11.2.2.14.

Software Ver	rsion : 11.2.2.14	~]	_								
+ Add Sit	e Batch Add Sit	es Deploy Config/Software	e Back Up/R	eview Checkp	oints	More Actions	De	ployment Tracker	Search		Q
Availability	Cloud Connectivity	Site Name	Site Role	Device Model	Serial 1	No	Bandwidth Tier	Management IP	Actio	ns	
•	 Inactive 	satest	Branch	2100-PE			500	Unknown	ø	G	
•	Online	petest2100	MCN	2100-PE	✓ 4	29A7CZX6S	500	10.102.78.77	Ø	٥	
						Page Size: 200 ∨	Showing 1 - 2	of 2 items Pa	ge1 of1		• •

Click **Stage** and then **Activate**. The **Activate** button is available after the staging is completed. It might take some time to complete the staging activity as a binary file around 200 MB gets downloaded in the back end.

Verify	Config Current Deploy	yment [Deployment History	Change Management Settings					
Software Versi Stage	on: 11.3.0.143	Activate	✓ □ Ig	nore Incomplete					
1/1 Staged Appliances 1/1									
Total Appliances		Stage	ed	Activated		Failed			
1		1		1		0			
Online	Site		Status		HA Sta	te	Software Version		
Yes	petest2100		Activation Complete		Not C	onfigured	11.3.0.143.888881		
				Page Size: 2	00 V Showing 1	-1 of 1 items	Page1 of1 <		

Once the staging and activation process is completed, the WAN optimization virtual machine will not activate immediately. You have to set the scheduling information as part of the **Change Management Settings**.

Click **Change Management Settings** and click the pencil icon under the **Action** column.

Verify Config	Current Deployment	Deployment History	Change Management Settings		
Scheduling Informatio	n				
Site Name	HA State	Scheduling Inform	ation	Maintenance Mode	Actions
petest2100 (Primary)	Not Configured	2020-11-25 at 2	21:20:00 (Maintenance window of 0 hours and repeated every 1 day)		Ø

Provide the schedule information and click **Save**.

You can enter/edit the following parameters:

- Site Name: Appliance name as given by the user during the site configuration.
- **Date**: Date on which scheduled installation/upgrade will start from. Also, mention the local time of the appliance when the installation must being once the files are received. Valid Format is HH:MM:SS.
- **Maintenance Window**: The amount of time given by the user for installation. If the value is provided as 0, then the provision starts immediately after the files are present on the appliance irrespective of the date and time values given in the **Date** field.
- **Repeat Window**: Frequency with which the system checks for a new upgrade version and performs the upgrade only when a new version is available.

Site Name
petest2100
Date:
2020-11-25 21:20:00
Maintenance Window (hours):
1
Repeat Window:
1
Unit:
Davs
56/5

• Unit: Unit chosen to check for new versions can be any one of Hours/Days/Weeks/Months.

The WAN Optimization provision happens as part of the time/date mentioned in the scheduled window. Once the virtual machine is UP, only then the WAN Optimization capabilities can be applied.

Save

NOTE

SD-WAN Orchestrator doesn't provide the provisioning status of the WAN Optimization Virtual Machine and the WAN Optimization Version. You must use the Citrix SD-WAN appliance UI to view the version and provisioning status.

Limitations

PE Appliance Settings, Monitoring, and Statistics features support will only be available in the upcoming release of SD-WAN Orchestrator.

WAN optimization

December 2, 2020

After the global configuration is completed, you have the option of customizing the sets and settings for each of the sites.

The WAN Optimization global settings that you just configured are automatically applied to each site of the network. You can elect to accept the defaults, or customize the configuration for any site. The procedures for configuring settings for a site are the same as for configuring the global, with a few minor differences.

Perform the following steps to customize the configuration for a specific PE site:

- At site level, navigate to Configuration > Advanced Settings > WAN Optimization. You can also directly click the configured PE site from the Network level then select Advanced Settings > WAN Optimization.
- 2. Select **Override** check box to enable editing. If the Override check box is not selected, all settings configured under global are applied to this site by default.

WAN Optimization (i)								
Tuning	Features	Apps	App Groups	Rules				
✓ Overri	ide							
WAN O	ptimization T	uning Set	tings					
Maximur	n MSS		Default MSS					
135	0		1350					
Ena	ble Connectio	n Timeout						
Idle Time	eout (s)							
360	0							
Save	e							

3. Enter your changes and click Save.

The **Override** option is available for all the WAN Optimization features configuration.

You have now completed configuring the settings for your Virtual WAN.

WAN-Optimization settings

May 3, 2022

You can configure WAN Optimization settings like KeyStore, Windows Domain, SSL Profiles, CA Certificates, Certificate Key Pairs, and Secure Peering for each site, through Citrix SD-WAN Orchestrator ser-

vice. To configure WAN optimization settings, from the site-level, navigate to **Configuration** > **WAN-OP Settings**.

Citrix SD-WAN Orchestrator service supports WAN Optimization settings for SD-WAN PE appliances running the software version 11.3.1 or higher.

Note

The option to configure WAN optimization settings is not available while creating or editing a site template.

KeyStore Settings

You can enable KeyStore settings by selecting the **Enable KeyStore Password** check box. Set the Key-Store password by updating the **KeyStore Open Password** and the **Confirm New Keystore Password** fields and then click **Save**. To disable KeyStore settings, clear the **Enable KeyStore Password** check box.

The key store password secures the security keys and settings of the SD-WAN appliance. Every time the SD-WAN appliance restarts, the key store is automatically closed. You must then open the key store for secure acceleration to resume.

Configuration / WAN-OP Settings	Verify Configuration Software Version : A									
WAN Optimization Settings ③										
KeyStore Settings Windows Domain SSL Profiles CA Certificates Certificate Key Pairs Secure Peering										
Security keys and settings are secured by the key store password. Each time the appliance restarts, the key store is closed automatically, and must be opened manually for	secure acceleration to resume.									
Keystore Status : Opened										
Enable Keystore Password										
Keystore Open Password*										
Password										
Confirm New Keystore Password										
Password										
Save										

Windows Domain

You can join the server-side Citrix SD-WAN appliance to a domain that the Windows file server and Exchange server are a part of. This makes the SD-WAN appliance a trusted member of the Windows security system.

To add a server-side SD-WAN appliance to a domain name:

- 1. In the Windows Domain section, update the Domain Name, User Name, and Password fields.
- 2. Click Save.

WAN Optimiza	ation Settings	; (i)			
•					
KeyStore Settings	Windows Domain	SSL Profiles	CA Certificates	Certificate Key Pairs	Secure Peering
Windows Domain					
Join the server-side	Citrix SD-WAN appliance	e to a domain that	the Windows file ser	ver and Exchange server	are a part of. Joining the domain makes the appliance a trusted member of the Windows security system.
Domain Name *					
Domain Name					
User Name *					
User Name					
Password *					
Password					
Save					

To add the users to a domain name:

- 1. In the **Delegate Users** section, click **Add**.
- 2. Update the Domain Name, User Name, and Password fields.
- 3. Click **Save**. The user profile appears in the list with basic information such as the domain to which the user is connected, and so on.

You can also edit or remove an end-user profile by navigating to the **Actions** column and clicking the 3 dots.

Delegate Users			
Add			
User Name	Domain Name	Status	Actions
admin	GOOGLE.COM	Unable to resolve domain name	
admin1	ABC.COM	Unable to resolve domain name	•••

SSL Profiles

Citrix SD-WAN Orchestrator service supports all SSL related configuration of the SD-WAN PE appliances for security and usability. On the SD-WAN Premium (Enterprise) Edition, service classes are configured by Citrix SD-WAN Orchestrator service and therefore, you cannot attach any SSL profiles. To accommodate the expression of SSL profile mapping to a service class, the work flow for SSL profiles is changed to allow for attaching Service classes in the profile node.

To create SSL profile on a new SD-WAN PE appliance:

- 1. Navigate to **Configuration** > **WAN-OP Settings** > **SSL Profiles** and then click **Add**. Create the SSL Profile.
- 2. On the **SSL Profile** page, provide a profile name and select the Service Classes that are associated to this profile. Choose the Proxy Type and provide relevant data.
- 3. Provide all the other data on the **SSL Profile** page.

4. Click Save.

Configuration / WAN-OP Settings				Verify Configuration Software Version :
WAN Optimization Settings	(i)			
	-			
KeyStore Settings Windows Domain	SSL Profiles	CA Certificates	Certificate Key Pairs	Secure Peering
SSL Profile				
Profile Name*				
Profile Name				
Profile Enabled				
Parse Subject Alternative Names				
Virtual Host Name				
Profile Name				
Service Classes				
Service Classes			~	
Proxy Type				
Split Transparent				
Enable Exclude List				
Certificate Verification*				
Signature/Expiration			~	
Certificate Verification Common Names				
Certificate Verification Common Name				
Samuer Side Dreuw Configuration				
Verification Store				
Verification Store				
Vernication Store			÷	
Authentication Required				
Protocol Version				
TLS 1.2 Only			~	
Cipher Specification *				
Renegotiation Type *				
Old Style Renegotiation Disabled			~	
Client-Side Proxy Configuration				
Certificate/Private Key*				
Certificate/Private Key			~	
Disable Session Re-use				
Build Certificate Chain				
Certificate Chain Store				
Certificate Chain Store			~	
Protocol Version*				
TLS 1.2 Only			~	
Cipher Specification *				
Renegotiation Type*				
Old Style Renegotiation Disabled			\sim	
Cancel Save				

After you create the SSL profile and associate it with a service class, you can view the SSL profile information as shown below.

Configuration / W	AN-OP Settings							Verify Configuration Software V	ersion : 11.3.1.53-G/
WAN Optimiza	ation Settings	i)							
KeyStore Settings	Windows Domain	SSL Profiles	CA Certificates	Certificate Key Pairs	Secure Peering				
Add									
Profile Name			Praxy Type			Protile in Use	Profile Enabled		Actions
deltest789			transparent			Yes	No		•••
helootest			transparent			Yes	No		•••
hvhfxgcf			split			Yes	No		•••
nametest123			transparent			Yes	No		•••
onetest34			split			Yes	No		•••
orchtest1			split			Yes	No		•••
orchtest12			transparent			No	No		•••
orchtest12_test			split			Yes	No		•••
test1348s97			transparent			Yes	No		•••
test31234			split			Yes	No		•••
test34			transparent			No	Yes		•••
test34897			transparent			Yes	No		•••
testbidir_error			split			No	No		
testnoclass			transparent			No	No		•••

Limitation

While configuring an SSL profile, the SSL profile gets attached to all rules in a service class. If you need to attach the SSL profile selectively to a particular rule, the service class configuration is split into detailed rules for further selection.

CA Certificates

You can install CA certificates through Citrix SD-WAN Orchestrator service. To add a CA certificate:

- 1. In the CA Certificates section, click Add.
- 2. Update the Certificate Key Pair Names field.
- 3. Choose an input method –File Upload or Paste Text based on your requirement.
- 4. Click Save.

Configuration / WAN-OP Settings	Verify Configuration Software Version : 11.3.1.53-GA							
WAN Optimization Settings ^①								
KeyStore Settings Windows Domain SSL Profiles CA Certificates Certificate Key Pairs Secure Peering								
CA Certificate								
Name								
Certificate Name								
Input Method								
○ File Upload								
Input Text*								
Certificate								
Cancel Save								

You can also edit or remove a CA certificate by navigating to the **Actions** column and clicking the 3 dots.

Configuration / WAN-OP Settings							
WAN Optimization Settings O							
KeyStore Settings Windows Domain SSL Profiles <u>CA Certificates</u> Certificate Key Pairs Secure Peering							
Add							
Name	Expiry Date	Actions					
PrivateRootCA	Jul 5 05:51:23 2030 GMT						
TestFileUpload	Oct 21 11:08:42 2022 GMT	Edit					
orchtest1	Oct 21 11:08:42 2022 GMT	Delete					
test	Jun 117:28:39 2021 GMT						
test123	Oct 21 11:08:42 2022 GMT	•••					
test123_viv	Jul 5 05:51:23 2030 GMT	•••					
testfile1	Oct 21 11:08:42 2022 GMT	***					
testfileupload	Oct 21 11:08:42 2022 GMT	•••					

Certificate Key Pairs

You can add Certificate Key pairs through Citrix SD-WAN Orchestrator service.

To add an SSL Certificate key pair:

- 1. In the Certificate Key Pairs section, click Add.
- 2. Update the Certificate Key Pair Names and the Key Password fields.
- 3. Choose an input method –File Upload or Paste Text based on your requirements. When you select the **File Upload** method, you can select a configuration file to upload the Certificate key and the Private key. The allowed file types are .pem, .der, .pfx, and .crt.

Configuration / W	AN-OP Settings					
WAN Optimization Settings ③						
KeyStore Settings	Windows Domain	SSL Profiles	CA Certificates	Certificate Key Pairs	Secure Peering	
SSL Certificate/Key	Pair					
Certificate Key Pair Names* Cert_Key_Pair						
Input Method						
File Upload Pa Input Format	ste Text					
Combined Certificat	e/Private Key 🔵 Sej	parate Certificate	/Private Key			
Click here or drag a Allowed file types a	nd drop a configuration re .pem, .der, .pfx	on file to upload	Certificate Key.			
Upload						
Key Password						
Cancel	Save					

When you choose the **Paste Text** method, you can update the Certificate key and the Private key details manually.

- 4. Choose an input format –**Combined Certificate/Private Key** or **Separate Certificate/Private Key** based on your requirement. In case of .pem and .der file formats, there are separate upload boxes for certificate and key.
- 5. Click Save.

Configuration / WAN-OP Settings	Verify Configuration Software Version : 11.31.53-64
WAN Optimization Settings ①	
KeyStore Settings Windows Domain SSL Profiles CA Certificates Certificate Key Pairs Secure Peering	
SSL Certificate/Key Pair	
Certificate Key Pair Names *	
satest	
Input Method	
C File Upload C Paste Text	
Input Format	
Combined Certificate/Private Key Certificate/Private Key	
Certificate*	
BEGIN CERTIFICATE	
•	
Key Password	
Key Password	
Cancel Save	

You can also edit or remove a Certificate-key pair by navigating to the **Actions** column and clicking the 3 dots.

Configuration / WAN-OP Settings	Verify Config	uration Software Version : 11.3.1.53-GA				
WAN Optimization Settings ①						
KeyStore Settings Windows Domain SSL Profiles CA Certificates Certificate Key Pairs Secure Peering						
Add						
Name	Expiry Dete	Actions				
satest	2023-07-29 07:37:33	Edit				
test12	2023-07-29 07:37:33	Delete				

Secure Peering

Secure communications with the Citrix SD-WAN WANOP appliances require that you generate OpenSSL credentials, including a CA Certificate and a Certificate/Key pair, and select a verification method. You can optionally change the OpenSSL cipher specification.

You can enable the secure peering settings by clicking the edit icon in the **Secure Peering Certificate and Keys** section and selecting the **Enable Secure Peering** check box.

- Certificate Configuration
 - Private CA: When you choose this option, Citrix SD-WAN Orchestrator service automatically generates the certificates and keys. You can securely connect to the peer SD-WAN appliances of other sites by providing the appliance details in the Connected Peers section.

Configuration / WANOP Settings	Verify Configuration Software Version : 11.3.1.53-GA
WAN Optimization Settings ①	
NeyStare Settings Windows Domain SSL Profiles CALCentificates Centrularities Becam Prening	
Secure communications with the Otion SD-10441100 partner explanate requires the you generate OpenSSL condential.circluloring GL CentTotate and a CentTotate Intel CentTotate Intel Action method tou can optionally charge the OpenSSL, other spectroation. If Private-CA is selected, centTotates and lays are generated automatically,	
Secure Reering Certificate and Keys IP	
Endia Sacare Nerrog Contros Congrutum	
Phylate CA C CACettificate	
Caroel Save	
Connected Poers.	
0 Atten*	
IP Address	
Userana"	
Liker Hanne	
Pennet*	
Pessed	
Caroti Correct	

- **CA Certificate**: When you choose this option, you can install the certificates and keys as per your requirements.

Configuration / WAN-OP Settings	Verify Configuration Software Version : 11.3.1.53-6/
WAN Optimization Settings ③	
KeyStore Settings Windows Domain SSL Profiles CA Certificates Certificate Key Pairs S	iecure Peering
Secure communications with the Citrix SD-WAN WO partner appliance requires that you generate OpenSSL creden selected, certificates and keys are generated automatically.	tials including CA Certificate and a Certificate/Wey pair, and select a verification method You can optionally change the OpenSSL cipher specification. If PrivateCA is
Secure Peering Certificate and Keys 🤌	
Enable Secure Peering	
Certificate Configuration	
Private CA CA Certificate	
Certificate / Key Pair Name *	
Select Certificate / Key Pair Name	~
CA Certificate Store Name	
PrivateRootCA	\checkmark
Certificate Verification	
Signature/Expiration	×
SSL Cipher Specification	
Cipher List	
	Y Y
Cancel Save	

In the **Listen On and Connect To** section, you can connect multiple SD-WAN appliances by providing the IP address and port details. Click **+Connect To** and provide the details as required, and click **Connect**.

+ Connect To		
Connect To IP	Connect To Port	Delete
1.1.1.2	2344	Û

Provider dashboard

October 21, 2020

When you log in as a Citrix partner, the **Provider Dashboard** appears. It offers a bird's eye view of all the SD-WAN customers managed by a service provider.

Provider Dashboard		New Customer
2 0 0 2 0 Total Customers Critical Warning Inactive Norma	al Search	
customer2 INACTIVE ····	customer1 INACTIVE ····	
O O O O O O O O O O O O O O O O O O O	O O O O O O Total Sites Critical Warning Inactive Normal	

A color-coded health snapshot of each customer's SD-WAN network is provided, with a provision to drill down into any of them for customer specific details. The dashboard is available in both **Tile View** and **List View**.

The color-coding criteria used for the customer's network are:

- Critical (Red): One or more sites are down
- Warning (Orange): No sites are down but there are one or more critical alerts.
- Normal (Green): No sites are down and there are no critical alerts.
- Inactive (Gray): The network is being configured, but has not been deployed yet.

The color-coding criteria allows administrators to focus on the customers that need their attention.

Customer/Network dashboard

March 30, 2022

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 dashboard lists the total number sites in the network and also segregates the sites based on their connectivity status. Select the numbered links to view the sites based on the following status categories:

- **Critical** –Sites that have all the associated virtual paths down.
- Warning Sites that have at least one virtual path down.
- Normal All virtual paths and associated member paths of the site are up.
- Inactive Sites that are in the undeployed and inactive state.
- **Unknown** Status of the site is unknown.

Clicking the status filters the sites based on their status and displays the details. You can also use the **Search** bar to view the details of a site based on the site name, role, overlay connectivity, model, bandwidth tier, and the serial number parameters.



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
_	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
	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.

Network Dashboard 🛛 🕄			Relative Tim	ne 🗸 Interval:	Last 1 Hour 🖂 Site Group:	All 🗸
Palents See All 79 Critical	O UPTIME See D. Overlay Underlay 80.0% 75.0%	etails TOP APP	'S	<u>See All</u>	© TOP SITES SantaClara 0.21 % 0.16 %	<u>See All</u> Kansas 0.12 %
5 1 1 TOTAL SITES CRITICAL WARNIN	NG NORMAL INACTIVE UNKNOWN		Search	(2	
					E	sport as CSV Export as PDF
Site Name		Role Over State	lay Model us	Bandwidth Tier	Orchestrator Connectivity	Serial No
myLTE		Branch	ICAL 210-SE	20	PRIMARY ACTIVE ONLINE	
SantaClara		MCN WAR	NING VPX-SE	50	PRIMARY ACTIVE ONLINE	C 10547436-040
Boston		Branch	MAL VPX-SE	50	PRIMARY ACTIVE ONLINE	C + 386 84 3C + 54
Kansas		Branch	VPX-SE	20	PRIMARY ACTIVE ONLINE	C AC 754 335 7084
Dallas		Branch	VPX-SE	20	PRIMARY ACTIVE ONLINE	C #E945004 DE3
			Page	e Size: 50 🗸	Showing 1-5 of 5 items	Page1 of1

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 Dash-board**.

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.



Record device mismatch

Citrix SD-WAN Orchestrator service reports a mismatch that is identified between the appliance reported platform model and the user reported platform model.

When the platform model and the sub-model provided by a user during site configuration does not match the platform model and sub-model provided by the appliance during the initial registration with Citrix SD-WAN Orchestrator service, a notification about the mismatch is displayed on the network dashboard. In such a scenario, ensure to configure the platform model reported by the appliance.

Click **View more** for a tabular representation of the platform model mismatch for each site.

A Identified platform m	odel mismatch for some sites. <u>View more</u>			
Network Dashboard	c	Relative Time V Interval: Las	st 1 Hour 🗸 Site Groups 🛛 All	- v
	© UPTIME See Petals No Statistics Available	TOP APPS See All Unknown o KB	© TOP SITES site120 site1 0.01% 0.01%	<u>See All</u> 21
		Search	۹.	<u>&</u> III

The **Platform Mismatch Details** provides information such as site name, appliance reported platform model and sub-model, and user reported platform model and sub-model.

	Platform Misma	atch	Details			
	Site Name		Device Platform	User Reported Platform	Device Submodel	User Reported Submodel 🤤
	site120		CBVPX	CB110		



Site dashboard

September 15, 2021

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

Site Dashboard 🛛 🕄					Relative	Time \vee Interval:	Last 1 Hour 🗸
Image: Contract of the second seco	() UPTIME No Statistics Available	<u>See Details</u>	TOP APPS Unknown 0 KB	Se	не All 🔡 Т Non о КВ	OP APP CATEGORIE	S <u>See All</u>
WAN DEVICES Solution Virtual Path Conn	ections	1 Total	0 Critical	0 • Warning	1 ● Normal]	
		VPX_BR	ANCH_MAA				
		VPX_I	MCN_BLR				1-1 of 1

Тір

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.

	4:18pm	4:23pm	4:28pm	4:33pm	4:38pm	4:43pm	4:48pm	4:53pm	4:58pm	5:03pm	5:08pm	5:13pm	5:18p
	1												
/PX_MCN_BLR-	0.75												
	0.5												
	0.0												
	0.25												
	0												
PX_MCN_BLR-Broadband-ACT-	1												
VPX_BRANCH_MAA-Broadband-	0.75												
CT-1	0.5												
	0.05												
	0.25												

Devices

The **Devices** tab displays details associated with the site's devices, interfaces, and disk temperature. You can also reboot the appliance, reset the appliance configuration or download device logs.

The **Temperature** section displays the temperature of the system, CPU, and the disks in degree Celsius.

WAN DEVICE	ES								
evice Info									
Orchestrator Connectivity	Uptime	Short Name	Device Model	Device Edition	Serial N	No.	Bandwidth	Management IP	Actions
Yes	1 month 22 days 54 minutes	Primary	210	SE	820	KCX45J	20 Mbps	10.217.110.33	⊕
iterfaces (P	Primary)								
STATUS	Interface Port		Bytes Sent			Bytes Received		Errors	
Down	1/1		117056			0		0	
Down	1/2		117056			0		0	
Up	LTE-1		2595352			7122		0	
emperature									
Device Name	e : Primary								
Serial No :	DZXXCX45J								
Name	Temp	erature (C)							
System	58								
cpu0	58								

You can also click the graph icon in the **Temperature (C)** column and view the information in graphical form.

Temperat	ure	DZXXCX45	i adhi											×
	100	10:00	10:05	10:10	10:15	10:20	10:25	10:30	10:35	10:40	10:45	10:50	10:55	
Disk Temp (C)	60 40 20													
	0													

Provider Troubleshooting

October 14, 2021

sda sdb

The Provider audit logs page displays provider-level logs and device logs, enabling quick troubleshooting.

76 🗠

Audit logs

Audit logs capture the action, time, and result of the action performed by the providers. Navigate to **Troubleshooting > Audit Logs** to view the **Provider Troubleshooting: Audit Logs** page.

The Provider Audit logs page displays the following information:

- Search bar: Search for an audit activity based on a keyword.
- Filtering options: Run an audit log search by filtering based on the following criteria:
 - User
 - Feature
 - Time range
- **Export as CSV**: When you click this option, the audit log entries are exported to a CSV file.
- Audit Info: Click the icon on the Action column to navigate to the Audit Info section. This section provides the following information:
 - Method: HTTP request method of the invoked API.
 - **Status**: Result of the API request.
 - **Response**: Error response when the API request fails. This field is displayed only when the API request fails.
 - **Payload**: Body of the request sent through API.
 - URL: HTTP URL of the revoked API.
 - Source IP: The IP address of the endpoint from which the SD-WAN features are configured. This field is displayed on the Provider Troubleshooting: Audit logs page and on the Audit Info page.

Λ	di+	Info
Au	απ	IIIIO

Method	POST
Status	Failure (404)
Payload	
Response	{"type": "https://errors-api.cloud.com/common/notFound", "detail": "Multi-MCN not found", "parameters": [{"name": "id", "value": "22afd958-617c-4295-8d56-98cdc7331613"}, {"name": "entityType", "value": "Msp"}]}
URL	/policy/v1/msp/22afd958-617c-4295-8d56-98cdc7331613/domainName
Source IP	

- Close
- Log payloads: By default, this option is disabled. When enabled, the request body of the API message is displayed in the **Audit Info** section. For more information about API, refer to API guide for Citrix SD-WAN Orchestrator.

Provider Tro	ubleshooting: Auc	lit Lo	gs	Log Payloads	Search		Q
User		\sim	Feature	✓ Start [Date	End Date	
							Export as CSV
Feature	Message		User	Created At		Source IP	Action
🔵 Base Msp	Create Customers			Septembe	er 30, 2021 3:51		0
🛑 Base Msp	Create Customers			May 26, 20	021 11:30 PM		0
				Sho	owing 1-2 of 2 iten	ns Page 1	of 1

Device logs

Providers can view the device logs that are specific to customers. You can also filter device logs by site name.

You can select specific device logs, download it, and share it with customers if necessary.

Dashboard		Provider TroubleShooting : Device Logs		
LIII Reports	>	Select Sustomer Select Site Select Site San Francisco		
Configuration	>	🛓 Download (0 Bytes / 1 GB)		Search Device Logs Q
		Name	Last Modified	Size
F Troubleshooting	~	ps.1.log	February 25, 2020 10:13 AM	23.03 MB
Audit Logs		init.log	February 25, 2020 10:13 AM	2.66 MB
Device Logs		SDWAN_filetransfer.log	February 25, 2020 10:13 AM	1.09 MB
		SDWAN_ip_learned.log	February 25, 2020 10:13 AM	662.44 KB
•		SDWAN_snmp_poll.log	February 25, 2020 10:13 AM	1.08 MB
Administration	>	SDWAN_config_update.old.log	February 25, 2020 10:13 AM	1.91 MB
		SDWAN_snmp_poll.old.log	February 25, 2020 10:13 AM	1.91 MB
		SDWAN_dynamic_virtual_path.old.log	February 25, 2020 10:13 AM	7.63 MB
		SDWAN_management.log	February 25, 2020 10:13 AM	1.32 MB
		launch_proc.log	February 25, 2020 10:13 AM	42.54 KB
		SDWAN_filetransfer.old.log	February 25, 2020 10:13 AM	1.91 MB
		SDWAN_common.old.log	February 25, 2020 10:13 AM	3.81 MB
		SDWAN_dynamic_virtual_path.log	February 25, 2020 10:13 AM	1.09 MB

Network Troubleshooting

October 14, 2021

Customers can view logs of all the network appliances, enabling quick troubleshooting.

Audit logs

Audit logs capture the action, time, and result of the action performed by users on a customer network. Navigate to **Troubleshooting** > **Audit Logs** to view the **Audit Logs** page.

The Audit logs page displays the following information:

- Search bar: Search for an audit activity based on a keyword.
- Filtering options: Run an audit log search by filtering based on the following criteria:
 - User
 - Feature
 - Site
 - Time range
- Export as CSV: When you click this option, the audit log entries are exported to a CSV file.
- Audit Info: Click the icon on the Action column to navigate to the Audit Info section. This section provides the following information:
 - Method: HTTP request method of the invoked API.

- **Status**: Result of the API request. You see the following error response when the API request fails.
- **Response**: Error response when the API request fails. This field is displayed only when the API request fails.
- **Payload**: Body of the request sent through API.
- **URL**: HTTP URL of the revoked API.

Audit Info

Method	PUT
Status	Success (200)
Payload	{"gre": [{"greService": {"mtu": 1500, "checksum": false, "serviceName": "GRELan", "serviceType": "lan", "firewallZone": "", "routingDomain": "Default_RoutingDomain", "keepalivePeriod": 10, "keepaliveRetries": 3}, "greSiteBindings": []}, {"greService": {"mtu": 1500, "checksum": false, "serviceName": "GREINtranet", "serviceType": "intranet", "firewallZone": "", "routingDomain": "Default_RoutingDomain", "keepalivePeriod": 10, "keepaliveRetries": 3}, "greSiteBindings": []}}
URL	/policy/v1/customer/3102986d-26ab-48cd-ae22-ee126dbcb341/config/gre

- **Source IP**: The IP address of the endpoint from which the SD-WAN features are configured. This field is available on the **Audit logs** page and the **Audit Info** page.
- What Changed: This section displays the logs of all the changes made to the SD-WAN features through the UI. Enable the Log Payloads toggle button to view the changes on the Audit Info page.

Source IP	
	{
	1 gre: [
	2 {
	3 greService: {
	4 mtu: 1500,
	5 checksum: false,
	6 serviceName: "GRELan",
	<pre>7 serviceType: "lan",</pre>
	<pre>8 firewallZone: "",</pre>
What Changed	9 routingDomain: "Default_RoutingDomain",
	10 keepalivePeriod: 10,
	11 keepaliveRetries: 3
	12 },
	13 greSiteBindings: [
	14]
	15 },
	10 + ()

• Log payloads: By default, this option is disabled. When enabled, the request body of the API message is displayed in the **Audit Info** section. For more information about API, see API guide for Citrix SD-WAN Orchestrator.

Audit Logs ①					
	•	Log Payloads	Search		Q
User	✓ Feature ✓	Site	✓ Start Date	End Date	
					Export as CSV
Feature	Message	User	Created At	Source IP	Action
GRE GRE	Update Config Gre		October 6, 2021 12:15 AM		0
GRE	Update Config Gre		October 6, 2021 12:15 AM		0
Base Security	Update Config Ipsec Tunnels		October 6, 2021 12:14 AM		0
Site	Update Siteapi testB		October 5, 2021 2:57 AM		0
Site	Update Config Site testB Wan Link Provisioning Settings		October 5, 2021 2:57 AM		(i)
Site	Update Config Site testB Wan Links		October 5, 2021 2:57 AM		0
Site	Create Config Site testB Lag Groups		October 5, 2021 2:57 AM		(i)
Site	Update Config Site testB Interface Groups		October 5, 2021 2:57 AM		0
Site	Update Config Site testB Ha		October 5, 2021 2:57 AM		0
Site	Update Config Site testB Wifi Settings		October 5, 2021 2:57 AM		0
Site	Update Config Site DC_MCN Ha	the second second second second second second second second second second second second second second second s	September 30, 2021 11:53 PM		(i)

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.

Select Site					
San Fr	ancisco 🗸				
≛ 0	ownload (0 Bytes / 1 GB)			Search Device Logs	Q
	Name	Last Modified	Size		
	init.log	September 20, 2019 11:10 AM	2.76 MB		
	SDWAN_filetransfer.log	September 20, 2019 11:10 AM	1.66 MB		
	SDWAN_ip_learned.log	September 20, 2019 11:10 AM	1.21 MB		
	SDWAN_snmp_poll.log	September 20, 2019 11:10 AM	1.66 MB		
	SDWAN_config_update.old.log	September 20, 2019 11:10 AM	1.91 MB		
	SDWAN_snmp_poll.old.log	September 20, 2019 11:10 AM	1.91 MB		
	SDWAN_dynamic_virtual_path.old.log	September 20, 2019 11:10 AM	7.63 MB		
	SDWAN_management.log	September 20, 2019 11:10 AM	1.51 MB		
	SDWAN_filetransfer.old.log	September 20, 2019 11:10 AM	1.91 MB		
	SDWAN_common.old.log	September 20, 2019 11:10 AM	3.81 MB		
	SDWAN_dynamic_virtual_path.log	September 20, 2019 11:10 AM	1.66 MB		
	SDWAN_igmp_proxy.old.log	September 20, 2019 11:10 AM	1.91 MB		
	SDWAN_security.old.log	September 20, 2019 11:10 AM	1.91 MB		
	dynamic_routing.log	September 20, 2019 11:10 AM	123.47 KB		

Security Logs

In the Citrix SD-WAN appliance, the Edge Security events are logged in the *SDWAN_advanced_firewall.log* file. The log file is periodically rotated based on the size, with up to 23 archives or a day's worth of logs remaining, whichever is less. For example, consider the following two use cases:

- If the log file fills up at a rate of 1 GB per 20 transactions (log entries), logs for approximately 8 hours is available, in the appliance, at any given time.
- If the log file fills up at a rate of 1 GB per hour or slower, logs for exactly a day are available in the appliance.

Note

- The size threshold for log rotation depends on the appliance. For the Citrix SD-WAN 1100 appliance the log rotation size threshold is 1 GB.
- The log file SDWAN_advanced_firewall.log is available for Citrix SD-WAN 1100 appliance only. It is not available on Citrix SD-WAN 210 SE and Citrix SD-WAN 210 SE LTE appliances.

To receive the security logs from the Citrix SD-WAN appliance, in the appliance UI, navigate to **Configuration** > **Appliance Settings** > **Logging/Monitoring** > **Syslog Server** and ensure that the **Firewall Logs to Syslog** option is enabled.

Retrieval from Citrix SD-WAN Orchestrator service

Similar to other appliance log files, you can retrieve the Edge Security firewall logs from the Citrix SD-WAN Orchestrator service. At the network level, navigate to **Troubleshooting** > **Device Logs**, select a site with Edge Security enabled, select the Advanced Firewall logs you want to download and click **Download**.

Dashboard		Network TroubleShooting : Device Logs		
Lill Reports	>	Select Site		
Configuration	>	myorance ✓ ▲ Download (122.8 MB / 1 GB)		
Troubleshooting Audit Logs Device Logs	~	Name SDWAN_advanced_firewall-2020-05-26T12-20-54.284.log.gz SDWAN_advanced_firewall.log	Last Modified May 26, 2020 3:20 PM May 27, 2020 12:06 AM	Size 4.87 MB 58.96 MB
Diagnostics	>			

Exporting to external syslog server

If an external syslog server is configured on the appliance UI (**Appliance Settings** > **Logging/Moni-toring** > **Syslog server**) Edge Security logs are generated and offloaded to this server.

Log entries

Edge Security log entries follow the Common Event Format (CEF). CEF is a standard that defines the syntax of log messages and therefore allows the interoperability of multiple devices generating log messages in a solution.

CEF consists of a standard header and a variable extension. The header format is as follows:

```
1 Timestamp host CEF:Version|Device Vendor|Device Product|Device Version|
    Device Event Class ID|Name|Severity|[Extension]
```

Example:

```
1 Jan 18 11:07:53 sd-wan CEF:0|Citrix|SD-WAN|11.2.2.7|EdgeSec|Name|
Severity|Extension
```

The following fields are common to all edge security logs generated by SD-WAN:

• Timestamp: The time when the log message is generated.

Note

This time can be different from the time of the event the message corresponds to.

- Host: The name of the host that generates the log file. For example, mybranch.
- **CEF**: A fixed string, indicating that the remainder of the message follows the CEF format.

Note

No other format is supported.

- Version: Identifies the version of the CEF format. The current CEF version is 0.
- **Device Vendor**: The vendor of the instance or appliance generating the CEF message. The field is always **Citrix**.
- Device Product: The product, SD-WAN.
- **Device Version**: The software version of the SD-WAN appliance in **major.minor.patch.buildnumber** format. For example, 11.2.0.88.
- Device Event Class ID: A unique identifier for every event-type. For Edge security logs, it is always EdgeSec.
- **Name**: A human-readable description of the Edge Security event-type. For example, HTTP, FTP, and so on.
- **Severity**: Reflects the security criticality of the event. The severity levels defined in the CEF standard are as follows:
 - **0-3**=Low
 - **4-6**=Medium
 - **7-8**=High
 - 9-10=Very-High

For Citrix SD-WAN Edge Security events, the following criteria are used to determine the severity level:

Severity level	Description
0	All SESSION events and all allowed HTTP Web filtering events
3	All clean (allowed) FTP, SMTP, and HTTP Anti-Malware events Logged IPS events
6	Blocked HTTP Web filtering events
7	Blocked IPS events
8	Blocked (infected) FTP, SMTP, and HTTP Anti-Malware events

• **Extensions**: A collection of key-value pairs that provide more details on the event. For example, "rt=Aug 13 2020 11:46:55", where "rt"is the key for the event timestamp and "Aug 13 2020 11:46:55" is the value. The key-value pairs used depend on the event type the CEF message corresponds to. The detailed descriptions of the event types are provided in the following sections.

HTTP(S) HTTP(S) log entries capture events related to HTTP or HTTPS traffic. Such events can be generated by either the web-filtering component, which performs URL categorization on HTTP(S) requests, or the Anti-Malware component, which scans HTTP responses for malware infections. The following table describes the various extensions in an HTTP log entry:

Field	Description
rt	The time of the event, without time zone. The time is expressed in UTC.
cn1	The session identifier, allows correlation with session events
cn1Label	Descriptive text for the cn1 field. The value is session_Id .
cs1	The configured security policy
cs1Label	Descriptive text for the cs1 field. The value is Security profile .
src	The source IP address (client-side)
spt	The source port (client-side)
dst	The destination IP address (server-side)
dpt	The destination port address (server-side)
requestMethod	The HTTP request (for example, GET, POST)
request	The HTTP URL
dhost	The HTTP host name
act	The action for the HTTP event. For an allowed HTTP event, the value is allowed and for a blocked HTTP event, the value is blocked .
reason	The component that generated the event. Valid values are web_filter and anti_malware .
cs2	The category name of the URL category matched
cs2Label	Descriptive text for the cs2 field. The value is
2	
CS3	I he name of the malware identified in the
cs3Lahel	payloau (II ally) Descriptive text for the cs3 field. The value is
	Malware name.

HTTP events can be generated by either the web-filtering or Anti-Malware components. For web-

filtering events, the value for cs3 key is blank, whereas for Anti-Malware events, the value for cs2 key is blank.

A typical log entry for an allowed HTTP web-filtering event is as follows:

```
1 Oct 8 2020 09:51:01 mybranch CEF:0|Citrix|SD-WAN|11.2.2.2|EdgeSec|HTTP
|0|rt=Oct 8 2020 09:51:01 cn1=104946811893306 cn1Label=session_id
cs1=Test_Prof1 cs1Label=Security profile src=192.168.0.2 spt=54749
dst=192.168.1.2 dpt=80 requestMethod=GET request=http://192.168.1.2/
eicar.exe dhost=192.168.1.2 act=allowed reason=web_filter cs2=
Uncategorized cs2Label=URL Category cs3= cs3Label=Malware name
```

A typical log entry for a Blocked HTTP web-filtering event is as follows:



A typical log entry for an allowed HTTP Anti-Malware event is as follows:

1 Oct 8 2020 11:49:09 mybranch CEF:0|Citrix|SD-WAN|11.2.2.2|EdgeSec|HTTP |3|rt=0ct 8 2020 11:49:08 cn1=104946811893527 cn1Label=session_id cs1=Test_Prof1 cs1Label=Security profile src=192.168.0.2 spt=34143 dst=192.168.1.2 dpt=80 requestMethod=GET request=http://192.168.1.2/ harmless.exe dhost=192.168.1.2 act=allowed reason=anti_malware cs2= cs2Label=URL Category cs3= cs3Label=Malware name

A typical log entry for a blocked HTTP Anti-Malware event is as follows:

```
1 Oct 8 2020 11:45:43 mybranch CEF:0|Citrix|SD-WAN|11.2.2.2|EdgeSec|HTTP
|8|rt=Oct 8 2020 11:45:43 cn1=104946811893520 cn1Label=session_id
cs1=Test_Prof1 cs1Label=Security profile src=192.168.0.2 spt=37702
dst=192.168.1.2 dpt=80 requestMethod=GET request=http://192.168.1.2/
eicar.exe dhost=192.168.1.2 act=blocked reason=anti_malware cs2=
cs2Label=URL Category cs3=EICAR-Test-File cs3Label=Malware name
```

FTP events The FTP log entries capture user activity related to FTP requests. The following table describes the various fields in an FTP log entry:

Field	Description
rt	The time of the event, without Time Zone
cn1	The session identifier, allows correlation with session events

Field	Description
cn1Label	Descriptive text for the cn1 field. The value is session_Id .
cs1	The configured security policy
cs1Label	Descriptive text for the cs1 field. The value is Security profile .
src	The source IP address (client-side)
dst	The destination IP address (server-side)
request	The FTP URI
act	The action for the FTP event. For an allowed FTP event, the value is allowed and for a blocked FTP event, the value is blocked .
reason	The component that generated the event. The only component generating FTP events are currently anti_malware .
cs3	The name of the malware identified in the payload (if any)
cs3Label	Descriptive text for the cs3 field. The value is
	Malware name.

A typical log entry for an allowed FTP Anti-Malware event is as follows:

```
1 Oct 8 2020 09:49:56 mybranch CEF:0|Citrix|SD-WAN|11.2.2.2|EdgeSec|FTP
|3|rt=Oct 8 2020 09:49:56 cn1=104946811893256 cn1Label=session_id
cs1=Test_Prof1 cs1Label=Security profile src=192.168.0.2 dst
=192.168.1.2 request=harmless.exe act=allowed reason=anti_malware
cs3= cs3Label=Malware name
```

A typical log entry for a blocked FTP Anti-Malware event is as follows:

```
1 Oct 8 2020 09:50:06 mybranch CEF:0|Citrix|SD-WAN|11.2.2.2|EdgeSec|FTP
|8|rt=Oct 8 2020 09:50:06 cn1=104946811893276 cn1Label=session_id
cs1=Test_Prof1 cs1Label=Security profile src=192.168.0.2 dst
=192.168.1.2 request=eicar.exe act=blocked reason=anti_malware cs3=
EICAR-Test-File cs3Label=Malware name
```

SMTP events The SMTP log entries capture user activity related to unencrypted email, sent using the SMTP protocol. The following table describes the various fields in an SMTP log entry:

Field	Description
rt	The time of the event, without Time Zone
cn1	The session identifier, allows correlation with session events
cn1Label	Descriptive text for the cn1 field. The value is session_Id .
cs1	The configured security policy
cs1Label	Descriptive text for the cs1 field. The value is Security profile .
SrC	The source IP address (client-side)
spt	The source port (client-side)
dst	The destination IP address (server-side)
dpt	The destination port address (server-side)
cn2	The message identifier
cn2Label	Descriptive text for the cn2 field. The value is Message identifier .
cs4	The email subject
cs4Label	Descriptive text for the cs4 field. The value is Message subject .
suser	The address of the sender
duser	The address of the receiver
act	The action for the SMTP event. The value is allowed , for an allowed SMTP email message, blocked , for a blocked SMTP email message, and remove for an SMTP email message that was allowed after a malware payload was removed.
reason	The reason for the action. The value is anti_malware .
cs3	The name of the malware identified in the payload (if any)
cs3Label	Descriptive text for the cs3 field. The value is Malware name .

A typical log entry for an SMTP event with virus is as follows:

A typical log entry for an SMTP event without virus is as follows:

1 Oct 8 2020 11:50:50 mybranch CEF:0|Citrix|SD-WAN|11.2.2.2|EdgeSec|SMTP |3|rt=Oct 8 2020 11:50:50 cn1=104946811893573 cn1Label=session_id cs1=Test_Prof1 cs1Label=Security profile src=192.168.0.2 spt=52737 dst=192.168.1.2 dpt=25 cn2=104946811893537 cn2Label=message identifier cs4=Test email cs4Label=subject suser=sender@sender.com suserLabel=sender duser=receiver@receiver.com duserLabel=receiver act=allowed reason=anti_malware cs3= cs3Label=Malware name

IPS/IDS

Field	Description
rt	The time of the event, without Time Zone
cn3	The IPS/IDS signature identifier that triggered the event
cn3Label	Descriptive text for cn3. The value is signature_id.
src	The source IP address of the packet
spt	The source port of the packet (if applicable)
dst	The destination IP address of the packet
dpt	The destination port of the packet (if applicable)
proto	The protocol of the packet (TCP, UDP)
act	The action for the IPS/IDS event. For an allowed IPS/IDS event the value is logged , whereas for a blocked IPS/IDS event, the value is blocked .
cs5	The class-type of the IPS/IDS signature that triggered the event
cs5Label	Descriptive text for cs5. The value is class-type
msg	The IPS message associated with the event

A typical log entry for a blocked IPS event is as follows:

```
1 Aug 14 2020 14:58:59 mybranch CEF:0|Citrix|SD-WAN|11.2.2.53|EdgeSec|
HTTP|7|rt=Aug 14 2020 14:58:59 cn3=2210051 cn3Label=signature_id src
=192.168.0.2 spt=1944 dst=192.168.1.2 dpt=22 proto=TCP act=blocked
cs5=protocol-command-decode cs5Label=class-type msg=SURICATA STREAM
Packet with broken ack
```

A typical log entry for a logged IPS event is as follows:

Session Events The Session log entries capture user activity at the TCP layer. They complement HTTP, FTP, and SMTP events by providing insight about TCP session duration, and start and stop time-stamps. Session log entries can refer to session start, session end, or update events.

Field	Description
rt cn1	The time of the event, without Time Zone. For session start events, the timestamp is when the session was established. The session identifier
cn1Label cs1	Descriptive text for the cn1 field. The value is session_Id . The configured security policy
cs1Label	Descriptive text for the cs1 field. The value is Security profile .
src	The source IP address (client-side)
spt	The source port (client-side)
dst	The destination IP address (server-side)
dpt	The destination port address (server-side)
act	The type of the session event. It can be new_session for events referring to a newly established session, session_update , for events referring to existing long-lived sessions, and session_closed , for events referring to sessions closing.

Field

Description

end

scription

The time the session closed without time zone. The field is only applicable to **session_closed** events.

A typical log entry for a session start event is as follows:

```
1 Oct 7 2020 23:46:44 mybranch CEF:0|Citrix|SD-WAN|11.2.2.2|EdgeSec|
Session|0|rt=Oct 7 2020 23:46:44 cn1=104946811892916 cn1Label=
session_id cs1=Test_Prof1 cs1Label=Security profile src=192.168.0.2
spt=43838 dst=10.78.242.11 dpt=53 act=new_session
```

A typical log entry for a session end event is as follows:

```
1 Oct 7 2020 23:46:46 mybranch CEF:0|Citrix|SD-WAN|11.2.2.2|EdgeSec|
Session|0|rt=Oct 7 2020 23:46:45 cn1=104946811892917 cn1Label=
session_id cs1=1 cs1Label=Security profile end=1602114405989 src
=192.168.0.2 spt=42253 dst=10.78.242.11 dpt=53 act=session_closed
```

Session Updates The Session updates log entries capture user activity at the TCP layer for longrunning sessions on a per-minute basis. Session updates help identify existing log entries (HTTP, SMTP, FTP, and session events) that correspond to still open sessions. The corresponding events can either be ignored, or treated as **tentative**, since session closure might update certain attributes (that is, session end time). Contrary to session_start and session_closed events, the session_update events only have a limited subset of the fields.

Field	Description
rt	The time of the event, without Time Zone
cn1	The session identifier
cn1Label	Descriptive text for the cn1 field. The value is
	session_ld.
act	The action for the IPS/IDS event. For a session
	update, the value is session_update .

A typical log entry for a session update event is as follows:

```
1 Oct 7 2020 23:47:00 mybranch CEF:0|Citrix|SD-WAN|11.2.2.2|EdgeSec|
    Session|0|rt=Oct 7 2020 23:47:00 cn1=104946811892912 cn1Label=
    session_id act=session_update
```

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.

Select a site for which to create or download the STS bundle. 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 an STS bundle, at the network level, navigate to **Troubleshooting > STS Bundle**, select a site, and click **Create New**.

STS Bundle								
Select Site								
CB210		\sim						
Create New							Search	Q,
Name	Last Up	dated At	File Size		STS Status		Action	
			No rows found					
				Sho	wing 1-0 of 0 items	Page 1	of 0 🔹 🕨	5 rows 🗸
* Packages are available	for 7 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 allowed length of the name is 32 characters. The user provided name is used as a prefix in the final name. To ensure that the file names are unique (timestamp) and to help recognize the device from the STS package (serial number), the service generates a full name. If no name is provided, a name is auto-generated while creating the bundle.

You can request for a new STS only when the device is online and no STS process is running on the appliance. You can download an already available STS from the Citrix SD-WAN Orchestrator service even if the device is offline.

Create Diagnost	ic Information Dum	q		
Create a diagnostic dum	ιp.			
f the filename is left	blank, Site Name will be	e used as the prefix.		
ilename Prefix				
sts-bundle-network				
			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. The request takes a few minutes to get processed. 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.

Once the STS process starts on the appliance, the progress is updated under the status column at regular intervals. For example, **Requested (Collecting log files)**.

The STS bundles and failure records are maintained for 7 days, post which they are auto-deleted.

Site troubleshooting

September 30, 2021

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.

🕹 D	ownload (0 Bytes / 1 GB)			Search Device Logs Q
	Name	Last Modified	Size	
	ps.1.log	February 25, 2020 10:12 AM	24.52 MB	
	init.log	February 25, 2020 10:12 AM	2.65 MB	
	SDWAN_filetransfer.log	February 25, 2020 10:12 AM	1.08 MB	
	SDWAN_ip_learned.log	February 25, 2020 10:12 AM	1.08 MB	
	SDWAN_snmp_poll.log	February 25, 2020 10:12 AM	1.07 MB	
	SDWAN_config_update.old.log	February 25, 2020 10:12 AM	1.91 MB	
	SDWAN_snmp_poll.old.log	February 25, 2020 10:12 AM	1.91 MB	
	SDWAN_dynamic_virtual_path.old.log	February 25, 2020 10:12 AM	7.63 MB	
	SDWAN_management.log	February 25, 2020 10:12 AM	32.42 KB	
	launch_proc.log	February 25, 2020 10:12 AM	38.02 KB	
	SDWAN_filetransfer.old.log	February 25, 2020 10:12 AM	1.91 MB	
	SDWAN_common.old.log	February 25, 2020 10:12 AM	3.81 MB	
	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 an STS bundle for a site appliance, at the site level, navigate to **Troubleshooting** > **STS bundle** and click **Create New**.

Active	\sim				
Create New				Search	(
ame	Last Updated At	File Size	Status	Action	
angalore_mcn-8dc156e	August 12, 2020 2:11 PM	16.04 MB	Available For Download	⊥ 🖻	
.ew_test-8dc156e9-af52	August 11, 2020 10:36 AM	16.34 MB	Available For Download	⊥ 🖻	

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 allowed length of the name is 32 characters. The user provided name is used as a prefix in the final name. To ensure that the file names are unique (timestamp) and to help recognize the device from the STS package (serial number), the service generates a full name. If no name is provided, a name is auto-generated while creating the bundle.

You can request for a new STS only when the device is online and no STS process is currently running on the appliance. You can download an already available STS from the Citrix SD-WAN Orchestrator service even if the device is offline.

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. The request
	takes a few minutes to get processed. You can
	choose to cancel the STS creation process, if
	necessary.

STS Status	Description
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
Failure	process. 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.

Once the STS process starts on the appliance, the progress is updated under the status column at regular intervals. For example, **Requested (Collecting log files)**.

The STS bundles and failure records are maintained for 7 days, post which they are auto-deleted.

AppFlow and IPFIX

November 6, 2021

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 or IPv6 collectors. The collectors aggregate the flow records and generate real-time or historical reports.

AppFlow

AppFlow exports flow level data for HDX / ICA connections only. You can enable either the TCP only for HDX dataset template or the HDX dataset template. The TCP only for HDX dataset provides multi-hop data. The HDX dataset provides HDX insight data.

Note

HDX template is available for Citrix SD-WAN PE edition and Two-box appliances only. It should be enabled on the Data Center appliance.

AppFlow Collectors like Splunk and Citrix ADM have dashboards to interpret and present these templates.

IPFIX

IPFIX is a collector export protocol used for exporting flow level data for all connections. For any connection, you can view information such as packet count, byte count, type of service, flow direction, routing domain, application name and so on. IPFIX flows are transmitted through the management interface. Most collectors can receive IPFIX flow records, but may need to build a custom dashboard to interpret IPFIX template.

The IPFIX template defines the order in which the data stream is to be interpreted. The collector receives a template record, followed by the data records. Citrix SD-WAN uses templates 611 and 613 to export IPv4 IPFIX flow data, 615 and 616 to export IPv6 IPFIX flow data along with Options template 612.

Application Flow Info (IPFIX) exports data sets as per templates 611 for IPv4 flows, 615 for IPv6 flows and 612 options Template with Application info.

Basic Properties (IPFIX) exports data sets as per templates 613 for IPv4 flows and 616 for IPv6 flows.

The following tables provide the detailed list of flow data associated with each IPFIX template.

Application Flow Info (IPFIX) - V10 templates

Template ID - 611

Info Element (IE)	IE name & ID	Type and len	Description
Observation point ID	observationPointId, 138	Unsigned32, 4	
Export process ID	exportingProcessId, 144	Unsigned32, 4	
Flow ID	flowid, 148	Unsigned64, 8	
Ipv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	
Ipv4 DST IP	destinationIpv4Addres, 12	Ipv4address, 4	
Ipversion	ipVersion, 60	Unsigned8, 1	Set to 4.

Info Element (IE)	IE name & ID	Type and len	Description
IP protocol number	protocoldentifier,4	Unsigned8, 1	
Padding	N/A	Unsigned16, 2	
SRC Port	sourceTransportPort, 7	Unsigned16, 2	
DST Port	destinationTransportPor	rt,Utsigned16, 2	
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Byte Count	octetDeltaCount, 1	Unsigned64, 8	
Time for first pkt in microseconds Time for lastpkt in microseconds IP ToS	flowStartMicroseconds, 154 flowEndMicroseconds, 155 ipClassOfService, 5	dateTimeMicroseconds, 8 dateTimeMicroseconds, 8 Unsigned8, 1	
Flow Flags	tcpControlBits, 6	Unsigned8, 2	Currently set to 0.
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN flows are a possibility in SDWAN
Input Interface	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Output Interface	egressInterface, 14	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Input Vlan ID	vlanId, 58	Unsigned16, 2	
Output Vlan ID	postVlanId, 59	Unsigned16, 2	

Info Element (IE)	IE name & ID	Type and len	Description
VRF ID	ingressVRFID, 234	Unsigned32, 4	
Flow Key Indicator	flowKeyIndicator, 173	Unsigned64, 8	Set to 0x1E037F.
Application ID	applicationId, 95	octetArray, variable	The Application ID is same as the ID of the applications classified by the DPI engine. The application IDs remain constant. The application IDs for Custom domain name based applications change with every configuration update.

Template ID –615 (IPv6 flows)

Info Element (IE)	IE name & ID	Type and len	Comment
Observation point ID	observationPointId, 138	Unsigned32, 4	
Export process ID	exportingProcessId, 144	Unsigned32, 4	
Flow ID	flowId, 148	Unsigned64, 8	
Ipv6 SRC IP	sourceIPv6Address, 27	Ipv6address, 16	
lpv6 DST IP	destinationIpv6Add 28	r tps y6address, 16	
Ipversion	ipVersion, 60	Unsigned8, 1	Set to 6
IP protocol number	protocoldentifier, 4	Unsigned8, 1	
Padding	N/A	Unsigned16, 2	
SRC Port	sourceTransportPor 7	tŲnsigned16, 2	
DST Port	destinationTranspo 11	r tProsit gned16, 2	

Info Element (IE)	IE name & ID	Type and len	Comment
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Byte Count	octetDeltaCount, 1	Unsigned64, 8	
Time for first pkt	flowStartMicroseco	n da țe Time Microsec	onds,
in microseconds	154	8	
Time for lastpkt	flowEndMicrosecon	ddsate Time Microsec	onds,
in microseconds	155	8	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Flow Flags	tcpControlBits, 6	Unsigned8, 2	Currently set to 0.
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN flows are a possibility in
Input Interface	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.

Info Element (IE)	IE name & ID	Type and len	Comment
Output Interface	egressInterface, 14	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface
Input Vlan ID	vlanId, 58	Unsigned16, 2	combinations.
Output Vlan ID	postVlanId, 59	Unsigned16, 2	
VRF ID	ingressVRFID, 234	Unsigned32, 4	
Flow Key Indicator	flowKeyIndicator, 173	Unsigned64, 8	Set to 0x1E037F.
Application ID	applicationId, 95	octetArray, variable	The Application ID is same as the ID of the applications classified by the DPI engine. The application IDs remain constant. The application IDs for Custom domain name based applications change with every configuration

Template 612 (Options Template)

Info Element (IE)	IE name & ID	Туре	Comment
Application ID	applicationId, 95	octetArray	The Application ID is same as the ID of the applications classified by the DPI engine. The application IDs remain constant. The application IDs for Custom domain name based applications change with every configuration update.
Application Name	applicationName, 96	string	Specifies the name of the Citrix SDWAN specific proprietary application.
Application Description	applicationDescription, 94	string	Specifies the description of the application.

Basic Properties (IPFIX) – V9 compliant template - Template 613 (IPv4 flows)

Info Element (IE)	IE name & ID	Type and len	Comment
Ipv4 SRC IP	sourceIPv4Address, 8	Ipv4address, 4	
Ipv4 DST IP	destinationIpv4Addres, 12	Ipv4address, 4	
Ipversion	ipVersion, 60	Unsigned8, 1	
IP protocol number	protocoldentifier, 4	Unsigned8, 1	
IP ToS	ipClassOfService, 5	Unsigned8, 1	
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN flows are a possibility in SDWAN
SRC Port	sourceTransportPort, 7	Unsigned16, 2	
DST Port	destinationTransportPort 11	t,Unsigned16, 2	

Info Element (IE)	IE name & ID	Type and len	Comment
Pkt Count	packetDeltaCount, 2	Unsigned64, 8	
Byte Count	octetDeltaCount, 1	Unsigned64, 8	
Input Interface	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Output intenace	egressintenace, 14	Unsigned 32, 4	balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.
Input Vlan ID	vlanId, 58	Unsigned16, 2	
Output Vlan ID	postVlanId, 59	Unsigned16, 2	

Template ID –616 (IPv6 flows)

Info Element (IE)	IE name & ID	Type and len	Comment
Ipv6 SRC IP	sourceIPv6Address, 27	Ipv6address, 16	
lpv6 DST IP	destinationIpv6Add 28	r ŧps y6address, 16	
Ipversion	ipVersion, 60	Unsigned8, 1	Set to 6
IP protocol number	protocoldentifier,4	Unsigned8, 1	
IP ToS	ipClassOfService, 5	Unsigned8, 1	

Info Element (IE)	IE name & ID	Type and len	Comment	
Flow Direction	flowDirection, 61	Unsigned8, 1	0x00: ingress flow0x01: egress flowWAN-WAN and LAN-LAN flows are a possibility in SDWAN	
SRC Port	sourceTransportPo 7	rtUnsigned16, 2		
DST Port	destinationTranspo 11	r tPosi gned16, 2		
Pkt Count	packetDeltaCount, 2	Unsigned64, 8		
Byte Count	octetDeltaCount, 1	Unsigned64, 8		
Input Interface	ingressInterface, 10	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.	
Output Interface	egressInterface, 14	Unsigned32, 4	Citrix SD-WAN load balances data flows through multiple member paths, hence a single data flow can have multiple input/output interface combinations.	
Input Vlan ID	vlanId, 58	Unsigned16, 2		

Info Element (IE)	IE name & ID	Type and len	Comment
Output Vlan ID	postVlanId, 59	Unsigned16, 2	

Limitations

- AppFlow does not support IPv6 collector and flow records.
- The export interval for Net Flow is increased from 15 seconds to 60 seconds.
- AppFlow/IPFIX flows are transmitted over UDP, on connection loss not all data is retransmitted. If the export interval is set to X minutes, the appliance stores X minutes of data only. Which is retransmitted after X minutes of connection loss.
- In Citrix SD-WAN, release 10 version 2 the **AppFlow** settings are made local to every appliance, while in the previous releases it was a global setting. If the SD-WAN software release is down-graded to any of the previous releases and if AppFlow is configured on any one of the appliances, it will be applied globally to all alliances.

Configuring AppFlow/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: O TO	CP only for HDX O HDX
AppFlow / IPFIX Collector	Port
10.102.76.35	4730
Data Set: Appflow	Application Flow Info (IPFIX) Basic Properties (IPFIX)
Citrix ADM	Citrix ADM user' Password'
AppFlow / IPFIX Collector	Port
10.102.36.89	4736
Data Set: Appflow	Application Flow Info (IPFIX) Basic Properties (IPFIX)
Citrix ADM	Citrix ADM Password
	admin
AppFlow / IPFIX Collector	r 3 Port
10.29.30.45	4735
Data Set: 🖌 Appflow	Application Flow Info (IPFIX) Basic Properties (IPFIX)
Citrix ADM	Citrix ADM Password
AppFlow / IPFIX Collector	r 4
IP Address	Port
10.102.89.46	4732
Data Set: Appflow	Application Flow Info (IPFIX) 🗸 Basic Properties (IPFIX)
Citrix ADM	Citrix ADM Password
Savo	
Save	

Log files

For troubleshooting issues related to AppFlow / IPFIX export protocols, you can view and download the SDWAN_export.log files from Site logs

Adaptive bandwidth detection

November 11, 2021

Adaptive bandwidth detection is applicable to networks with VSAT, LOS, Microwave, 3G/4G/LTE WAN Links, where the available bandwidth varies based on weather, atmosphere conditions, location, and line of site obstructions.

You can adjust the bandwidth rate on the WAN Link dynamically based on a defined bandwidth range (minimum and maximum WAN link rate) to use the maximum amount of available bandwidth without marking the paths BAD.

- Greater bandwidth reliability (Over VSAT, Microwave, 3G/4G, and LTE)
- Greater predictability of adaptive bandwidth over user configured settings



This feature needs the Bad loss sensitivity option to be enabled (default/custom) as a prerequisite. You can enable the Bad Loss Sensitivity option under Path or Autopath group.

To enable adaptive bandwidth detection, while configuring sites, navigate to **Configuration** > **Site Configuration** > **WAN Links** > **Advanced WAN Options**. Select **Adaptive Bandwidth Detection** and enter a value in the **Minimum Acceptable Bandwidth** field.

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%.

Advanced WAN Options		^
Enable Metering Ad	laptive Bandwidth Detection	
30 Congestion Threshold (µs)	Provider ID	Frame Cost (Bytes)
20000		1
Standby Mode	MTU (Bytes)	
Disabled ~	1350	

Provider reports

April 23, 2021

The **Provider Reports** provide visibility into alerts, usage trends, and inventory aggregated across all the customers managed by a Provider.

In the Citrix SD-WAN Orchestrator service provider level UI, navigate to **Reports**.

Alerts

The provider can review all the events and alerts generated across all the customer networks.

The **Summary** view displays the number of high, medium, and low alerts for each customer.

Dashboard		Provider Report : Alerts					
Ltd Reports	~	Summary Details					
Alerts							
Usage						Search	Q,
Inventory		Customer Name	High	Medium	Low		
		Citrix Demo Center	0	0	0		
Configuration	>	ABC Systems	0	0	0		
•		Winstorm Motors	0	0	0		
F Troubleshooting	>	Creative Enterprises	0	0	0		
		Gremona Textiles	0	0	0		
Ω Administration	>	AMS_Demo	0	0	0		
		Demo1	0	0	0		
		Test	0	0	0		
		Test-Customer-t123	0	0	0		
		Rehab_Test	0	0	0		
		Support_Training	59	10	11		
		Abycare Hospitals	0	76	480		
				Page 5	ize: 25 V Showing 1 - 12 of 12 items	Page 1 of 1	Þ.

You can also view the severity, site at which the alert originated, alert message, time, and other information under **Details**.

Provider Report : Alerts

Summary De	tails				
Delete Alerts				Search Q 54	4 8 42 ■ HIGH ■ MEDIUM ■ LOW
Severity	Customer Name	Site	Source	Message	Time
Low	Abycare Hospitals	San Francisco	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1- San_Francisco-Broadband-AMIS-2 state has changed from BAD to GOOD.	Jun 21st 2020, 5:40 am
Low	Abycare Hospitals	San Francisco	APPLIANCE	The state of Virtual Path San_Francisco-Madrid has changed from BAD to GOOD	Jun 21st 2020, 5:40 am
Low	Abycare Hospitals	Madrid	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1- >San_Francisco-Broadband-AMIS-2 state has changed from BAD to GOOD because notified by peer.	Jun 21st 2020, 5:40 am
Low	Abycare Hospitals	Madrid	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1- >San_Francisco-Broadband-AMIS-2 state has changed from GOOD to BAD because notified by peer.	Jun 21st 2020, 5:40 am
Low	Abycare Hospitals	San Francisco	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1- >San_Francisco-Broadband-AMIS-2 state has changed from GOOD to BAD because silence time exceeds threshold.	Jun 21st 2020, 5:40 am
Medium	Abycare Hospitals	San Francisco	APPLIANCE	The state of Virtual Path San_Francisco-Madrid has changed from GOOD to BAD	Jun 21st 2020, 5:40 am
Low	Abycare Hospitals	Madrid	APPLIANCE	WAN Link Madrid-DSL-ono-1 is now up.	Jun 19th 2020, 12:29 pm
Low	Abycare Hospitals	London	APPLIANCE	Ethernet link on device 2 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jun 19th 2020, 12:29 pm
Medium	Abycare	London	APPLIANCE	The Citrix SD-WAN service has restarted.	Jun 19th 2020, 12:29 pm
Low	Abycare	London	APPLIANCE	Ethernet link on device 1 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jun 19th 2020, 12:29 pm
Low	Abycare Hospitals	San Francisco	APPLIANCE	Virtual Path San_Francisco-Madrid Path Madrid-DSL-ono-1- >San_Francisco-Broadband-AMIS-2 state has changed from DEAD to BAD because packet loss exceeds threshold.	Jun 19th 2020, 12:29 pm
High	Abycare Hospitals	San Francisco	APPLIANCE	The Virtual Path San_Francisco-Madrid is no longer DEAD	Jun 19th 2020, 12:29 pm

Suitable filtering options can be used as needed for example: Look for the high severity alerts across all the customers, or the alerts for a given customer and so on.

You can also select and delete alerts.

Usage

The provider can review cross-customer usage trends such as **Top Applications**, **Top Application Categories**, **Application Bandwidth**, and **Top Sites**.

Top application and application categories

The **Top Applications** and **Top Application Categories** chart shows the applications and application families that are widely used across all customer networks. This allows you to analyze the data consumption pattern and reassign the bandwidth limit for each class of data, if necessary.

nuer	nepont. Usage					Relative Tim	e 🗸 Interval:	Last 1 Hou
App	plication Usage Net	work Usage						
aport Typ	De	Apps						
Тор А	Apps ~	All	~					
				Top Applications				
mi d	crosoft (36%) 📕 lync_c	online (27%) 📕 window	slive (27%) 🔳 windows	s_update (9%) Unkn	own (0%)			
mic	crosoft (36%) <mark> Internations Descriptions Internations In</mark>	online (27%) 🛑 window	slive (27%) 🔳 windows	s_update (9%) Unkn	own (0%)		Search	٩
Top	crosoft (36%) I ync_c D Applications	online (27%) 💻 window Total Data	slive (27%) 🔳 windows	s_update (9%) Unkn	own (0%) Total Bandwidth	Upload Bandwidtl	Search h Downloa	Q ad Bandwidth
Top No 1	crosoft (36%) IVnc_c DApplications Applications microsoft	Total Data 36.25 KB	Slive (27%) windows	Download Data 24.5 KB	own (0%) Total Bandwidth 0.08 Kbps	Upload Bandwidti 0.03 Kbps	Search h Downloo 0.05 Kl	Q ad Bandwidth bbps
Top No 1 2	crosoft (36%) Inc.co	Total Data 36.25 KB 32.72 KB	Upload Data 11.75 KB 8.96 KB	Download Data 24.5 KB 23.76 KB	own (0%) Total Bandwidth 0.08 Kbps 0.73 Kbps 3.48 Kbps	Upload Bandwidtl 0.03 Kbps 0.2 Kbps	Search Downlow 0.05 Kl 0.53 Kl 2.64 Kl	Q ad Bandwidth bps bps bps
Top No 1 2 3 4	crosoft (36%) Ivnc_co Applications Applications microsoft lync_online windowslive windows update	Total Data 36.25 KB 32.72 KB 26.11 KB 7.28 KB	Slive (27%) windows Upload Data 11.75 KB 8.96 KB 6.57 KB 1.75 KB	Download Data 24.5 KB 23.76 KB 19.54 KB 5.53 KB	own (0%) Total Bandwidth 0.08 Kbps 0.73 Kbps 3.48 Kbps 0.32 Kbps	Upload Bandwidtl 0.03 Kbps 0.2 Kbps 0.88 Kbps 0.08 Kbps	Search Downlow 0.05 Kl 0.53 Kl 2.61 Kl 0.25 Kl	Q ad Bandwidth bps bps bps bps

						Relative Time ~	Interval:	Last 1 Hour
App	olication Usage Net	work Usage						
port Typ	e	App Categories						
Тор А	pp Categories V	All	~					
			Тор	Application Categories	3			
We	b (91%) 📕 Application	n Service (9%) 📕 None I	(0%)					
■ We	b (91%) Application	n Service (9%) 🔳 None i Pegories	(0%)			Se	arch	Q
Top	b (91%) Application	n Service (9%) None i egories Total Data	(0%) Upload Data	Download Data	Total Bandwidth	Se Uploed Bandwidth	arch Downlog	Q. ad Bandwidth
Top No 1	Application Category None	n Service (9%) None of Operation Service (9%) Service (9%) None of Operation Service (9%) Service (9%) None of Operation Service (9%) Service (9\%) S	(0%) Upload Data 0 KB	Download Data 0 KB	Total Bandwidth 0 Kbps	Se Upload Bandwidth 0 Kbps	arch Downloc 0 Kbps	Q. ad Bandwidth
Ve Top No 1 2	b (91%) Application Application Category None Application Service	n Service (9%) None i Pegories Total Data 0 KB 8.62 KB	Upload Data 0 KB 2.54 KB	Download Data 0 KB 6.07 KB	Total Bandwidth 0 Kbps 1.15 Kbps	Se Upload Bandwidth 0 Kbps 0.34 Kbps	Downloa 0 Kbps 0.81 KJ	Q ad Bandwidth S bpps

You can 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 from the list.

• **Metric:** Select the bandwidth metric (such as Total Data, Incoming Data, Total Bandwidth) from the list.

Network usage

The network usage chart depicts the top 10 sites across all the customers that have the highest bandwidth usage. You can view the Sites by Utilization (%) or Data Volume (MB).



Inventory

The provider can view the entire device inventory across all the customers. 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 customer networks.



Suitable filtering options can be used as needed for example: Look for all appliances belonging to a specific customer, 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. Choose a customer from the **Select Customer** drop-down list. You can view the site name, device role, device model, device serial number, current software, and device management IP address.

Select Customer : Abycare Site Name C San Francisco M	e Hospitals		Search	Q. DEPLOYED	UNDEPLOYED
Site Name	Device Dela				
San Francisco	Device Role	Device Model	Serial Number	Current Software	Management IP
	MCN	CBVPX	4ffa8122-3baa-5d43-315	11.2.0.88.861012	10.106.112.17
San Francisco	MCN	CBVPX	691852ab-fcc0-3d18-b4	11.2.0.88.861012	10.106.112.72
Madrid E	Branch	CBVPX	4343796c-53f6-4ce2-631	11.2.0.88.861012	10.106.112.71
Belgium F	Branch	CBVPX	e5a3bc15-e874-4803-db	10.2.6.1012.846463	10.106.112.18
London F	Branch	CBVPX	3fc0e3c3-1a16-7356-710	11.2.0.88.861012	10.106.112.70
NewYork E	Branch	CBVPX	c460fa20-aee7-0b54-4cc	11.2.0.88.861012	10.106.112.23
			Page Size: 25 ∨	Showing 1 - 6 of 6 items	Page 1 of 1

Customer/Network reports

May 26, 2022

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.

To view the reports, navigate to **Partner > Provider > Customer > Reports**.

Alerts

The customer can review a detailed report of all the events and alerts generated across all the sites in the network.

It includes the severity, site at which the alert originated, alert message, time, and other details.

Netwo	rk Reports: /	Alerts				Sit	: Group: All ~
D	elete Alerts					Search Q. 678	79 256 343 HIGH MEDIUM LOW
	Councity	Cito	Source	Object Name	Object Turne	Marcono	Export as CSV Export as PDF
	Severity	Jite	Source	object wante	object type	wesselfe	Time
	🔴 High	Boston	orchestrator	Connectivi	connectio	Site: Boston with device serial number: 63BEBF3C-F0FD-B980-F913-E9E0A2A94F33 lost Orchestrator	Jul 23rd 2021, 10:54 pm
	🔴 High	Boston	orchestrator	Connectivi	connectio	Site: Boston with device serial number: 63BEBF3C-F0FD-B980-F913-E9E0A2A94F33 lost Orchestrator	Jul 20th 2021, 12:03 am
	Low	Kansas	orchestrator	Connectivi	connectio	Site: Kansas with device serial number: AC75F331-7094-52F8-727F-DEB804A4B5F5 is now online and	Jul 20th 2021, 12:06 am
	Low	SantaClara	orchestrator	Connectivi	connectio	Site: SantaClara with device serial number: 1C64F43E-E4DC-8E48-34C9-DD524FE23121 is now online	Jul 20th 2021, 12:06 am
	🔴 High	SantaClara	orchestrator	Connectivi	connectio	Site: SantaClara with device serial number: 1C64F43E-E4DC-8E48-34C9-DD524FE23121 lost Orchestra	Jul 20th 2021, 12:03 am
	🔴 High	SantaClara	orchestrator	Connectivi	connectio	Site: SantaClara with device serial number: 1C64F43E-E4DC-8E48-34C9-DD524FE23121 lost Orchestra	Jul 27th 2021, 2:57 pm
	Low	SantaClara	orchestrator	Connectivi	connectio	Site: SantaClara with device serial number: 1C64F43E-E4DC-8E48-34C9-DD524FE23121 is now online	Jul 27th 2021, 2:57 pm
	🔴 High	myLTE	orchestrator	Connectivi	connectio	Site: myLTE with device serial number: JDZXXCX45J lost Orchestrator connectivity	Jul 20th 2021, 12:03 am
	🔴 High	Kansas	orchestrator	Connectivi	connectio	Site: Kansas with device serial number: AC75F331-7094-52F8-727F-DEB804A4B5F5 lost Orchestrator	Jul 23rd 2021, 10:54 pm
	Low	Boston	orchestrator	Connectivi	connectio	Site: Boston with device serial number: 63BEBF3C-F0FD-B980-F913-E9E0A2A94F33 is now online and	Jul 23rd 2021, 11:11 pm
	Low	Boston	orchestrator	Connectivi	connectio	Site: Boston with device serial number: 63BEBF3C-F0FD-B980-F913-E9E0A2A94F33 is now online and	Jul 20th 2021, 12:06 am
	🔴 High	Dallas	orchestrator	Connectivi	connectio	Site: Dallas with device serial number: 4E945004-DE3D-6CD8-F33B-375CEBE686FA lost Orchestrator	Jul 23rd 2021, 10:54 pm
	Low	myLTE	orchestrator	Connectivi	connectio	Site: myLTE with device serial number: JDZXXCX45J is now online and connected to Orchestrator	Jul 23rd 2021, 10:56 pm
	🔴 High	Dallas	orchestrator	Connectivi	connectio	Site: Dallas with device serial number: 4E945004-DE3D-6CD8-F33B-375CEBE686FA lost Orchestrator	Jul 20th 2021, 12:03 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 export the filtered results in to a CSV or PDF file by using the **Export as CSV** and **Export as PDF** options. The CSV and PDF file name is prefixed with **Alerts List** followed by the date and time when the file is exported.

The maximum events that each page can contain is 100. For example, if 9 events are available on the table, all the 9 events are exported to PDF or CSV. However, if more than 100 events are available on the table, you will still be able to export only 100 events each time because of the page capacity.

You can also select and clear alerts.

Security alerts

Edge Security resource alerts A set amount of system resources such as CPU, Memory, and Hard disk is allocated to the Edge security subsystem. Whenever a resource usage exceeds the set amount, the respective alerts are generated every minute. The following are the Edge security resource alerts:

- Edge security subsystem exceeds typical CPU allotment
- Edge security subsystem exceeds typical Memory allotment
- Edge security subsystem exceeds typical Hard Disk allotment

If one of these alerts is encountered consider revising the **Intrusion Prevention** settings to exclude low-priority rules and free up resources.

Edge Security system alert The following Edge Security system alerts are generated:

• State changed to UP: When the Edge Security processing state is changed to UP.

- *State changed to DOWN*: When the Edge Security processing state is changed to DOWN.
- State changed to DISABLED: When the Edge Security is disabled.
- *Policies are configured but service is not initialized*: When the Edge Security is not initialized but INSPECT policies are configured.

Wi-Fi alerts

The customer can review a detailed report of all Wi-Fi events and alerts generated across all the sites in the network. It includes the severity, site at which the alert originated, alert message, time, and other details. To view the Wi-Fi alerts, at the network level, navigate to **Reports > Alerts** and search for **hostapd**.

The following Wi-Fi alerts are generated:

- hostapd monitor started: When the Wi-Fi service starts.
- hostapd monitor stopped: When the Wi-Fi service stops.
- Client with MAC:<MAC> failed to authenticate with RADIUS on SSID :<SSID>: When a client fails to get authenticated using WPA2 Enterprise security protocol.
- Client with MAC:<MAC> failed to authenticate on SSID:<SSID>: When a client fails to get authenticated using WPA2 Personal security protocol.
- Possibly lost connectivity with RADIUS <IP>:<Port> on SSID:<SSID> :When network connectivity with the RADIUS server is lost.
- RADIUS bad authenticators on SSID:<SSID>: When bad authenticators are received from a RADIUS server.
- RADIUS malformed packets on SSID:<SSID>: When malformed packets are received from a RADIUS server.

Network Reports: Alerts

D	elete Alerts				host	Q 1019	9 44 85 890 ● HIGH ● MEDIUM ● LOW
	Severity	Site	Source	Object Name	Object Type	Message	Time
	Low	asimakisl_home_11	APPLIANCE	hostapd	undefined	hostapd monitor started	Dec 10th 2020, 11:40 am
	Low	asimakisl_home_11	APPLIANCE	hostapd	undefined	hostapd monitor started	Dec 9th 2020, 6:47 pm
	Low	asimakisl_home_11	APPLIANCE	hostapd	undefined	hostapd monitor started	Dec 9th 2020, 6:47 pm
	Low	asimakisl_home_11	APPLIANCE	hostapd	undefined	hostapd monitor started	Dec 9th 2020, 6:44 pm
	Low	asimakisl_home_11	APPLIANCE	hostapd	undefined	hostapd monitor started	Dec 9th 2020, 6:35 pm
	Low	asimakisl_home_11	APPLIANCE	hostapd	undefined	hostapd monitor stopped	Dec 9th 2020, 6:33 pm
	🔴 High	branch_110_3	APPLIANCE	hostapd	undefined	Client with MAC:60:67:20:67:fa:f8 faile	Dec 8th 2020, 6:52 pm
	🔴 High	branch_110_3	APPLIANCE	hostapd	undefined	Client with MAC:dc:a6:32:cf:40:80 faile	Dec 1st 2020, 6:31 pm
	🔴 High	branch_110_3	APPLIANCE	hostapd	undefined	Client with MAC:dc:a6:32:cf:40:80 faile	Dec 1st 2020, 6:31 pm
	🔴 High	branch_110_3	APPLIANCE	hostapd	undefined	Possibly lost connectivity with RADIUS	Dec 2nd 2020, 4:24 pm
	🔴 High	branch_110_3	APPLIANCE	hostapd	undefined	Possibly lost connectivity with RADIUS	Dec 2nd 2020, 3:24 pm
	🔴 High	branch_110_3	APPLIANCE	hostapd	undefined	Possibly lost connectivity with RADIUS	Dec 2nd 2020, 3:23 pm
	🔴 High	branch_110_3	APPLIANCE	hostapd	undefined	Possibly lost connectivity with RADIUS	Dec 2nd 2020, 2:23 pm

Site Group: All

Wired 802.1X alerts

The customers can view a detailed report of all the unique wired 802.1X authentication attempts across all the sites in the network. In 90 seconds, a client can try as many authentications attempts as possible. All the attempts create the following alerts. The alerts include the severity, site at which the alert originated, alert message, time, and other details. To view the wired 802.1X alerts, at the network level, navigate to **Reports > Alerts** and search for **wired**.

- Wired client with MAC<mac address> authenticated: When the authentication attempt is successful.
- Wired client with MAC<mac address> failed to authenticate: When the authentication attempt has failed.

Netwo	ork Reports: Al	erts					Site Group:	All 🗸
I	Delete Alerts					wired Q	1748 18 TOTAL • H	30 310 1258 IIGH ● MEDIUM ● LOW
	Severity	Site	Source	Object Name	Object Type	Message	Time	
	Low	home_110	appliance	hostapd	8021x	Wired client with MAC:20:1a:06:c8:0d:f1 authenticated	Mar	22nd 2021, 8:03 pm
	🔴 High	home_110	appliance	hostapd	8021x	Wired client with MAC:20:1a:06:c8:0d:f1 failed to authenticate	Mar	22nd 2021, 8:00 pm
	🔴 High	home_110	appliance	hostapd	8021x	Wired client with MAC:20:1a:06:c8:0d:f1 failed to authenticate	Mar	22nd 2021, 7:59 pm
	Low	home_110	appliance	hostapd	8021x	Wired client with MAC:20:1a:06:c8:0d:f1 authenticated	Mar	22nd 2021, 7:32 pm
	Low	home_110	appliance	hostapd	8021x	Wired client with MAC:20:1a:06:c8:0d:f1 authenticated	Mar	22nd 2021, 6:02 pm
	Low	home_110	appliance	hostapd	8021x	Wired client with MAC:dc:a6:32:b0:45:65 authenticated	Mar	22nd 2021, 4:42 pm
	Low	home_110	appliance	hostapd	8021x	Wired client with MAC:20:1a:06:c8:0d:f1 authenticated	Mar	22nd 2021, 4:36 pm
	Low	home_110	appliance	hostapd	8021x	Wired client with MAC:dc:a6:32:b0:45:65 authenticated	Mar	19th 2021, 2:41 pm
	Low	home_110	appliance	hostapd	8021x	Wired client with MAC:dc:a6:32:b0:45:65 authenticated	Mar	19th 2021, 1:13 pm

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.

	Reports . Usage			Relative	Time V Interval:	Last 1 Hour \smallsetminus	Site Group:	All	
Ap	plication Usage Net	work Usage							
ort Typ	e	Apps							
Top A	Apps ~	All	~						
			To	op Applications					
m i	crosoft (42%) 📕 windo	wslive (25%) 📕 lync_o	nline (17%) 🔳 windows_n	marketplace (8%) 🖕 w	vindows_update (8%)	Others (0%)			
∎ mie	crosoft (42%) 🛑 windo O Applications	wslive (25%) 📕 lync_o	nline (17%) 🔳 windows_n	marketplace (8%) 🖕 w	vindows_update (8%)	Others (0%)	Search		Q
■ mia Top	crosoft (42%) windo O Applications Applications	wslive (25%) 📕 lync_o Total Data	nline (17%) 🖿 windows_n	marketplace (8%) v	vindows_update (8%) Total Bandwidth	Others (0%) Upload Bandwidt	Search	mload Bandwic	Q
Top No	crosoft (42%) windo Applications Applications microsoft	wslive (25%) 🛑 lync_o Total Data 51.54 KB	nline (17%) windows_n Upload Data 15.52 KB	marketplace (8%) w	Total Bandwidth 0.12 Kbps	Others (0%) Upload Bandwidtl 0.03 Kbps	Search Dow 0.00	mload Bandwic	Q
Top No 1	Applications microsoft windowslive	vslive (25%) Ivnc_o Total Data 51.54 KB 26.11 KB	Upload Data 15.52 KB 6.57 KB	Download Data 36.02 KB 19.54 KB	Total Bandwidth 0.12 Kbps 3.48 Kbps	 Others (0%) Upload Bandwidtl 0.03 Kbps 0.88 Kbps 	Search Dow 0.00 2.6	mioad Bandwic 3 Kbps 1 Kbps	Q.
■ min Top No 1 2 3	Applications microsoft windowslive Jync_online	Total Data 51.54 KB 26.11 KB 23.81 KB	Upload Data 1 15.52 KB 5 6.57 KB 7.04 KB 7	Download Data 36.02 KB 19.54 KB 16.77 KB	Total Bandwidth 0.12 Kbps 3.48 Kbps 0.79 Kbps	 Others (0%) Upload Bandwidti 0.03 Kbps 0.88 Kbps 0.24 Kbps 	Search Dow 0.0: 2.6 0.50	mload Bandwic 3 Kbps 1 Kbps 5 Kbps	Q. dth
■ mit Top No 1 2 3 4	Applications Mapplications microsoft windowslive lync_online windows_marketpl	Total Data 51.54 KB 26.11 KB 23.81 KB 8.62 KB	Upload Data I 15.52 KB 3 6.57 KB 7 7.04 KB 7 2.54 KB 0	Download Data 36.02 KB 19.54 KB 16.77 KB 6.07 KB	Total Bandwidth 0.12 Kbps 3.48 Kbps 0.79 Kbps 1.15 Kbps	 Others (0%) Upload Bandwidtt 0.03 Kbps 0.88 Kbps 0.24 Kbps 0.34 Kbps 	Search Dow 2.6 0.5 0.8	mload Bandwid 3 Kbps 1 Kbps 3 Kbps 1 Kbps	Q.
min Top No 1 2 3 4 5	Applications Applications microsoft Windowslive lync_online windows_marketpl windows_update	wslive (25%) ■ lync_o Total Data 51.54 KB 26.11 KB 23.81 KB 8.62 KB 6.25 KB	Upload Data 1 15.52 KB 3 6.57 KB 7 7.04 KB 7 2.54 KB 0 1.21 KB 3	Download Data 36.02 KB 19.54 KB 16.77 KB 6.07 KB 5.03 KB	Total Bandwidth (8%) 0.12 Kbps 3.48 Kbps 0.79 Kbps 1.15 Kbps 0.83 Kbps 0.50 Kbps	 Others (0%) Upload Bandwidt 0.03 Kbps 0.88 Kbps 0.24 Kbps 0.34 Kbps 0.36 Kbps 0.16 Kbps 	Search Dow 0.00 0.00 2.66 0.59 0.8 0.61	nload Bandwid 3 Kbps 1 Kbps 3 Kbps 1 Kbps 1 Kbps 7 Kbps	Q

	Reports : Usage	e C		Relative	Time V Interval:	Last 1 Hour \vee	Site Group: All
Ap	plication Usage Net	work Usage					
ort Typ	pe	App Categories					
Fop A	App Categories 🛛 🗸	All	~				
			Тори	Application Categories			
W	eb (88%) 📕 Application	i Service (13%) 📕 None	(0%)				
Тор	o Application Cate	egories				S	earch Q
No	Application Category	Total Data	Upload Data	Download Data	Total Bandwidth	Upload Bandwidth	Download Bandwidth
	None	0 KB	0 KB	0 KB	0 Kbps	0 Kbps	0 Kbps
1	Application Service	8.62 KB	2.54 KB	6.07 KB	1.15 Kbps	0.34 Kbps	0.81 Kbps
1 2							

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 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 Data Volume (MB).

Network Reports : Top Sites by	Utilization (%) Utilization (%) Data Volume : (MB	~ C	Utilization Lev	el Across Sites	Relative Time $$	Interval:	Last 1 Hour 🗸	Site Group:	All	~
		Capacity Utilization	< 80%	80-95X	> 95%					
		No of Sites	3/3	0/3	0/3					
Top Sites								Sea	rch	Q
NO SITE NAME				AVERAGE UTILIZATI	DN (%)					
1 Berlin				0.17						
2 Colombia				0.13						
3 Miami				0.12						

Wi-Fi

Citrix SD-WAN Orchestrator service allows you to view the Wi-Fi summary reports. It provides an overview of the number of devices connected to Wi-Fi networks and the Wi-Fi data used within your network.

\bigcirc	DASHBOARD			Reports /	WI-FI /	WI-FI						
				Wi-Fi								Last 1 Hour
ай !	REPORTS	~		Connected D	Devices					Conr	nected Devices (over Last 1 Hou	ır)
	Alerts			13	5	8			16			
	Usage			Devices	corporate	Home		Connected Devices				
	Wi-Fi			As of current dat	e, time				0	15:50 16:00	16:10 16:20	16:30 16:40
	Inventory											 corporate home
	Security	>										
	Secure Internet Service	9		Data Utilizati	ion				Da	ta Utilization (over Last 1 Hour)		
	HDX (preview)	>		28.7 KB	14.46 KB	14.23 KB			240			
	Quality			Data Utilized	Corporate	Home	lome					
	QoS			As of current dat	e. time			(MB)	0	15:50 16:00	16:10 16:20	16:30 16:40
	Historical Statistics											corporate
	Real Time	>										
	Cloud Direct			Usage								
	Application Quality											
	O365 Metrics			Sites Auth	entication Log I	ailures						
	CAS Analytics		•	Site Name		Number of SSIDs	Connected Devices	Devices with poor si	ional	Avo Wi-Fi Throughput	Max Wi-Fi Throughput	Total data transferred
<				myBranch		4	14	0	. <u>9</u> ui	2.02 Mbps	27.76 Mbps	212.46 MB

To view a Wi-Fi report, at the network level, navigate to **Reports** > **Wi-Fi**.

Connected devices

The **Connected devices** section displays the total number of devices, in your network, that are currently connected to Wi-Fi. You can also see the number of appliances connected to the corporate network or home network based on the SSID it is connected to.

Connected Devices



You can also select the timeline to view a graphical representation of the historic data. The graph shows the number of corporate and home devices connected over the selected period. Hover the mouse over a bar to view the exact number of devices connected to corporate and home networks at specific time.



Data utilization

The **Data utilization** section displays the total amount of Wi-Fi data used by the connected appliances at the current moment. You can also view the data used by devices connected to the corporate or home network.

Data Utilization

39.06 KB Data Utilized 18.29 KB Corporate

20.77 KB Home

As of current date, time

You can also select the timeline to view a graphical representation of the historic data. The graph shows the amount of data used by the corporate and home devices over the selected period. Hover the mouse over a bar to view the exact data utilization of the corporate and home network users at specific time.



Usage

The usage table is a leaderboard that lists the top five Wi-Fi sites and Wi-Fi authentication failure logs in your network.

Sites The Sites table lists the top five Wi-Fi sites in your network based on the parameters such as average Wi-Fi throughput, maximum Wi-Fi throughput, total data transferred, and devices with poor signal. Click the parameter header to sort the column in descending order.

The network administrator can use this information to identify and troubleshoot issues in the network. For example, you can identify the sites with the most number of devices with poor signal and try to resolve the issue on the SD-WAN appliance at that site.

U	S	а	q	e
			~	

Authentication Log Failures									
Site Name	Number of SSIDs	Connected Devices	Devices with poor signal	Avg Wi-Fi Throughput	Max Wi-Fi Throughput	Total data transferred			
myBranch	4	14	0	2.02 Mbps	27.76 Mbps	212.46 MB			

Click **View more** to view the Wi-Fi details for all the sites in the network. You can select the period or search the list by site name.

Wi-Fi	/i-Fi							
Sites Authentication Log Failures								
myB								
туч								
Site Name	Number of SSIDs	Connected Devices	Devices with poor signal	Avg Wi-Fi Throughput	Max Wi-Fi Throughput	Total data transferred		
myBranch	4	20	0	6.26 Mbps	56.65 Mbps	938.5 MB		

Click a site name to view site level Wi-Fi reports. For more information, see Site Wi-Fi reports.

Authentication failure logs The authentication failure logs table displays the recent five authentication failures to the Wi-Fi network. You can view the site name, MAC address and IP address of the clients that are trying to connect to specific SSID along with authentication failure time.

Usage						
Sites Authentication Log Fa	ilures					
						Last Authentication Failure
User ID/MAC ID	Site Name	Authentication Type	SSID Name	IP Address	Authentication Failures(s)	Time
Alice	asimakisl_home_110_wifi	WPA2-Enterprise	ssid1	192.168.102.50	3	24th Nov 2020, 14:27
						View more

Click **View more** to view all the authentication failure logs. You can select the period or search the list by site name.

Wi-Fi	Last							
Sites Authentication Log Fai	lures							
User ID/MAC ID	Site Name	Authentication Type	SSID Name	IP Address	Authentication Failures(s)	Last Authentication Failure Time		
Alice	asimakisl_home_110_wifi	WPA2-Enterprise	ssid1	192.168.102.50	3	24th Nov 2020, 14:27		
Bob	asimakisl_home_110_wifi	WPA2-Enterprise	ssid1	192.168.102.51	4	24th Nov 2020, 14:34		

Click a site name to view site level authentication failure logs. For more information, see Site Wi-Fi reports.

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				Site Gro	oup: All 🗸
Summary	tails					
			Sea	rch Q	DEPLOYED	UNDEPLOYED
Site Name	Device Role	Device Model		Serial Number	Current Software	Management IP
San Francisco	MCN	CBVPX		4ffa8122-3baa-5d4	11.2.0.88.861012	10.106.112.17
San Francisco	MCN	CBVPX		691852ab-fcc0-3d1	11.2.0.88.861012	10.106.112.72
Madrid	Branch	CBVPX		4343796c-53f6-4ce	11.2.0.88.861012	10.106.112.71
Belgium	Branch	CBVPX		e5a3bc15-e874-48	10.2.6.1012.846463	10.106.112.18
London	Branch	CBVPX		3fc0e3c3-1a16-735	11.2.0.88.861012	10.106.112.70
NewYork	Branch	CBVPX		c460fa20-aee7-0b5	11.2.0.88.861012	10.106.112.23
			Page Siz	ze: 25 🗸 Showing	g 1 - 6 of 6 items Pag	ge 1 of 1

Security reports

Citrix SD-WAN Orchestrator service allows you to view summary reports for the Web filtering, Anti-Malware, and Intrusion Prevention security features. You can view the reports for the last 5 mins, 10 mins, 30 mins, 1 hr., 3 hr., day, week, or month.

Web filtering

To view the web filtering report, at the network level navigate to **Reports** > **Security** > **Web Filtering** and select the timeline for which you want to view the report.

The **Web Filtering Distribution** section displays the following information:

- Total number of web requests.
- Percentage of web requests allowed.
- Percentage of web requests that were flagged but not blocked.
- Percentage of web requests blocked.

Dashboard	Reports > Security > Web Filtering						
	Web Filtering						
III Reports							
Alerts	Web Filtering Distribution		Web Filtering (over Last 1 Month)				
Usage	14.08M 24 % 0 % 76 %	100 80					
Inventory	The referre that to a sector	Requests 20					
Security 🗸		0 21. May	22. May 23. May 24. May 25. May 26. May 27. May 28.	May 29. May 30. May 31. May			
Web Filtering				Allowed • Flagged • Elocked			
Anti Malware							
Intrusion Prevention	Top Web Events						
Quality	Sites Security Profiles						
0.05	Site Name Tr	Total Requests	Allowed Flagged	blocked			
LEsteries Otatistics	cb1100_2_branch 1-	4082997	3385478 0	10697519			
Historical Statistics				View more affected Sites			
Real time >							

You can also view a graphical representation of the percentage of web requests allowed, flagged, and blocked over the selected time frame.

Top web events The Top Web Events table provides web filtering details of the top 5 network sites and security profiles.

Sites:

It displays the total number of requests, the number of requests allowed, the number of requests flagged, and the number of requests blocked at the top 5 sites.

Top Web Events				
Sites Security Profiles				
Site Name	Total Requests	Allowed	Flagged	blocked
cb1100_2_branch	16547	15783	0	764
				View more affected Sites

Click **View more affected Sites**, to view the web filtering details of all the affected sites in the network.

W	/eb Filtering Last1 Hour Y								
	Sites Security Profiles								
	Search Q								
	Site Name	Total Requests	Allowed	Flagged	blocked				
	cb1100_2_branch	17946	17132	0	814				

Click an individual site name to view a graphical representation of the web filter details at the site. The **Web Filtering** of the chosen site also provides the real-time report of the last 1000 web (HTTP, HTTPS) events from the total number of the web requests (for the selected timeline).

Web Filtering	Last 1 Hour 🗡					
RemoteOffice Name	16 Web Requests	100 % 0 % Allowed Flagged	0 % Blocked			
Web Events			16 Web Requests	 16 Allowed 0 Flagged 0 Blocked 		
Time Stamp	Client	Server	Server Port	Domain Name	URI	Action
2020-07-30T04:49:02	172.16.14.11	52.229.168.53	80	array704.prod.do.dsp	/	Allowed
2020-07-30T04:43:40	172.16.14.11	52.139.168.125	80	settings-win.data.mic	/	Allowed
2020-07-30T04:43:39	172.16.14.11	40.90.137.127	80	login.live.com	/	Allowed
2020-07-30T04:38:09	172.16.14.11	52.229.168.53	80	array704.prod.do.dsp	/	Allowed
2020-07-30T04:36:42	172.16.14.11	52.139.153.205	80	settings-win.data.mic	/	Allowed
2020-07-30T04:36:14	172.16.14.11	52.114.132.73	80	v10.events.data.micro	/	Allowed
2020-07-30T04:31:46	172.16.14.11	52.229.168.53	80	array704.prod.do.dsp	/	Allowed
2020-07-30T04:21:42	172.16.14.11	52.139.153.205	80	settings-win.data.mic	/	Allowed
2020-07-30T04:20:50	172.16.14.11	23.49.60.152	80	ctldl.windowsupdate	/msdownload/updat	Allowed
2020-07-30T04:20:50	172.16.14.11	23.49.60.152	80	ctldl.windowsupdate	/msdownload/updat	Allowed
2020-07-30T04:19:50						
	172.16.14.11	52.139.153.205	80	settings-win.data.mic	/	Allowed

You can click the individual slices of the pie chart (demarcated by the color) or the legends beside the pie chart to view the top-10 allowed, flagged, and blocked web request details for clients, URLs, and categories.



Security profiles:

It displays the total number of requests, the number of requests allowed, the number of requests flagged, and the number of requests blocked by the top 5 Security profiles.

Top Web Events Sites Security Profiles				
Security Profile	Total Requests	Allowed	Flagged	blocked
	1787790	114894	0	1672896
	1787354	114532	0	1672822
	1788474	115755	0	1672719
	1786874	114376	0	1672498
	1795435	227450	0	1567985
				View more affected Security Profiles

Click **View more affected Security Profiles**, to view the web filtering details of all the security profiles.

Neb Filtering Last 1 Month ~							
Sites Security Profiles							
Search Q							
Security Profile	Total Requests	Allowed	Flagged	blocked			
	1787790	114894	0	1672896			
	1787354	114532	0	1672822			
	1788474	115755	0	1672719			
	1786874	114376	0	1672498			
	1795435	227450	0	1567985			

Click an individual Security profile name to view a graphical representation of its web filter details.

Web Filtering	Last 1 Month 💙					
Name	1.79M 6.4 % Web Requests Allowed	0 % Flagged	93.6 % Blocked			
				1.79M Web Requests	 114894 Allowed 0 Flagged 1672896 Blocked 	

Anti-malware

To view Anti-Malware reports, at the network level navigate to **Reports** > **Security** > **Anti-Malware** and select the timeline for which you want to view the reports.

The **Event Distribution** section displays the following information:

- Total number of files scanned.
- Percentage of files that were clean.
- Percentage of files that were infected.

Anti Malware Last 1 Month V		Scanned Events (over Last 1 M	(onth)
7686 81 % 19 % Cean Infected	Scanned 80 Requests (%) 20 21. May 22. May 23. May	24. May 25. May 26. May 27.	May 28. May 29. May 30. May 31. May • Clean • Infected
Top Scanned Events Sites Security Profiles			
Site Name	Scanned	Clean	Infected
cb1100_2_branch	7686	6224	1462
			View more affected Sites

You can also view a graphical representation of the percentage of files that were clean or infected over the selected time frame.

Top scanned events The **Top Scanned Events** table provides the Anti-Malware scan details at the top 5 sites and security profiles.

Sites:

It displays the total number of scanned files, the number of clean files, and the number of infected files at the top 5 sites.

Top Scanned Events			
Sites Security Profiles			
Site Name	Scanned	Clean	Infected
cb1100_2_branch	7685	6223	1462

View more affected Sites

Click **View more affected Sites**, to view the Anti-Malware scan details of all the affected sites in the network.

Anti Malware Last 1 Month ~						
Sites Security Profiles						
Search Q						
Site Name	Scanned	Clean	Infected			
cb1100_2_branch	7686	6224	1462			

Click an individual site name to view a graphical representation of the Anti-Malware scan details at the site. The **Anti-Malware** of the chosen site also provides the real-time report of the last 1000 Anti-Malware events from the total number of the files scanned (for the selected timeline).



You can click the individual slices of the pie chart (demarcated by the color) or the legends beside the pie chart to view the top-10 clean and infected event details for Web, FTP, and Email. You can further drilldown to verify the top-10 visited websites / FTP sites / email from, clients, virus.

RemoteOffice 3 Name Scanne	ed Clean Infected	
	3 Scanned Events	• 3 Clean • 0 Infected
Top 10 Clean Events		
Top 10 Clean Events Web FTP Email Visited Websites Clien	nts Virus	
Top 10 Clean Events Web FTP Email Visited Websites Clien Web Clien	nts Virus Scanned	Clean
Top 10 Clean Events Web FTP Email Visited Websites Clien Web 2.tlu.dl.delivery.mp.microsoft.com	nts Virus Scanned 681	Clean 681
Top 10 Clean Events Web FTP Email Visited Websites Clien Web 2.tlu.dl.delivery.mp.microsoft.com ctldl.windowsupdate.com	nts Virus Scanned 681 52	Clean 681 52
Top 10 Clean Events Web FTP Email Visited Websites Clien Web 2.tlu.dl.delivery.mp.microsoft.com ctldl.windowsupdate.com download.windowsupdate.com	nts Virus Scanned 681 52 48	Clean 681 52 48
Top 10 Clean Events Web FTP Email Visited Websites Clien Web 2.tlu.dl.delivery.mp.microsoft.com ctldl.windowsupdate.com download.windowsupdate.com 11.tlu.dl.delivery.mp.microsoft.com	nts Virus Scanned 681 52 48 33	Clean 681 52 48 33
Top 10 Clean Events Web FTP Email Visited Websites Clien Web 2.tlu.dl.delivery.mp.microsoft.com ctldl.windowsupdate.com download.windowsupdate.com 11.tlu.dl.delivery.mp.microsoft.com msedge.b.tlu.dl.delivery.mp.microsoft.com	Virus Scanned 681 52 48 33 m 13	Clean 681 52 48 33 13
Top 10 Clean Events Web FTP Email Visited Websites Clien Web 2.tlu.dl.delivery.mp.microsoft.com ctldl.windowsupdate.com download.windowsupdate.com 11.tlu.dl.delivery.mp.microsoft.com msedge.b.tlu.dl.delivery.mp.microsoft.com r4sn-h5576n7k.gvt1.com	nts Virus Scanned 681 52 48 33 m 13 11	Clean 681 52 48 33 13 11
Top 10 Clean Events Web FTP Email Visited Websites Clien Web 2.tlu.dl.delivery.mp.microsoft.com cttldl.windowsupdate.com download.windowsupdate.com 11.tlu.dl.delivery.mp.microsoft.com msedge.b.tlu.dl.delivery.mp.microsoft.com r4sn-h5576n7k.gvt1.com r5sn-h5576n7k.gvt1.com	Virus Scanned 681 52 48 33 m 13 11 10	Clean 681 52 48 33 13 11 10
Top 10 Clean Events Web FTP Email Visited Websites Clien Web 2.tlu.dl.delivery.mp.microsoft.com ctldl.windowsupdate.com download.windowsupdate.com 11.tlu.dl.delivery.mp.microsoft.com msedge.b.tlu.dl.delivery.mp.microsoft.com r4sn-h5576n7k.gvt1.com dl.delivery.mp.microsoft.com	Virus Scanned 681 52 48 33 m 13 11 10 8	Clean 681 52 48 33 13 11 10 8
Top 10 Clean Events Web FTP Email Visited Websites Clien Web 2.tlu.dl.delivery.mp.microsoft.com cttldl.windowsupdate.com download.windowsupdate.com 11.tlu.dl.delivery.mp.microsoft.com r4sn-h5576n7k.gvt1.com r5sn-h5576n7k.gvt1.com dl.delivery.mp.microsoft.com r5sn-h5576n7k.gvt1.com	Virus Scanned 681 52 48 33 m 13 11 10 8 6	Clean 681 52 48 33 13 11 10 8 6

Security profiles:

It displays the total number of scanned files, the number of clean files, and the number of infected files scanned by the top 5 security profiles.

Top Scanned Events						
Sites Security Profiles						
Security Profile	Scanned	Clean	Infected			
	776	122	654			
	3229	2716	513			
	1857	1818	39			
	120	94	26			
	128	104	24			

View more affected Security Profiles

Click **View more affected Security Profiles**, to view the Anti-Malware scan details of all the security profiles.

Security Profile Scanned	Clean	Infected	
776	122	654	
3229	2716	513	
1857	1818	39	
120	94	26	
128	104	24	

Click an individual Security Profile name to view a graphical representation of its Anti-Malware scan details.

Anti Malware	Last 1 Month \vee			
Name	3229 Scanned	84.1 % Clean	15.9 %	
				• 2716 Clean
				3229 Scanned Events

Intrusion Prevention

To view the Intrusion Prevention report, at the network level navigate to **Reports** > **Security** > **Intrusion Prevention** and select the timeline for which you want to view the report.

The Intrusion Distribution section displays the following information:

- Total number of intrusion events
- Percentage of intrusion events logged
- Percentage of intrusion events blocked

ntrusion Prevention Last 1 Hour ~									
Intrusion Distribution					Intrusion E	vents (over Last 1 Hour)		
15211 23.2 % 76.8 % Intrusion Events Logged Blocked	Intrusion Events	100 80 60 40 20 0	12:40	12:50	13:00	13:10	13 [:] 20	13:30	13:40
Top Intrusion Events								Logged	Blocked
Site Name	Intrusion Events				Logged		Blocked		
cb1100_2_branch	15211				3530		11681		
								View more affe	ected Sites

You can also view a graphical representation of the percentage of intrusion events logged or blocked over the selected time frame.

Top intrusion events The **Top Intrusion Events** table provides the intrusion prevention details at the top 5 sites. It displays the total number of intrusion events, the number of intrusion events logged, and the number of intrusion events blocked at the top 5 sites.

Top Intrusion Events			
Sites			
Site Name	Intrusion Events	Logged	Blocked
cb1100_2_branch	15634	3928	11706
			View more affected Sites

Click **View more affected Sites**, to view the Intrusion Prevention details of all the affected sites in the network.

Intrusion Prevention 🕛 Last 1 Hour 👻			
Sites			
Search Q			
Site Name	Intrusion Events	Logged	Blocked
cb1100_2_branch	15672	3941	11731

Click an individual site name to view a graphical representation of the Intrusion Prevention details at the site. The **Intrusion Prevention** of the chosen site also provides the real-time report of the last 1000 logged and blocked intrusion prevention system events from the total number of intrusion events (for the selected timeline).

		Lust a rioui						
RemoteOffic	e 11	100	% 0 %					
Name	Intrus	sion Events Elogged	Blocked					
				11 Intrusion Events	• 11 Logg • 0 Block	ied ked		
Intrusion Events Time Stamp	Source IP	Source Port	Destination IP	Destination Port	Protocol	Category	Class Type	Message
Intrusion Events Time Stamp 2020-07-30T04:	Source IP 172.16.14.11	Source Port	Destination IP 204.79.197.200	Destination Port	Protocol 1	Category icmp-info	Class Type misc-activity	Message GPL ICMP_INF
Intrusion Events Time Stamp 2020-07-30T04: 2020-07-30T04:	Source IP 172.16.14.11 172.16.14.11	Source Port 3 3	Destination IP 204.79.197.200 204.79.197.200	Destination Port	Protocol 1	Category icmp-info icmp-info	Class Type misc-activity misc-activity	Message GPLICMP_INF GPLICMP_INF
Intrusion Events Time Stamp 2020-07-30T04: 2020-07-30T04: 2020-07-30T04:	Source IP 172.16.14.11 172.16.14.11 172.16.14.11	Source Port 3 3 3	Destination IP 204.79.197.200 204.79.197.200 204.79.197.200	Destination Port 1 1 1 1	Protocol 1 1	Category icmp-info icmp-info icmp-info	Class Type misc-activity misc-activity misc-activity	Message GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF
Intrusion Events Time Stamp 2020-07-30T04: 2020-07-30T04: 2020-07-30T04: 2020-07-30T04:	Source IP 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11	Source Port 3 3 3 3 3	Destination IP 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200	Destination Port 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Protocol 1 1 1 1	Category icmp-info icmp-info icmp-info icmp-info	Class Type misc-activity misc-activity misc-activity misc-activity	Message GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF
Intrusion Events Time Stamp 2020-07-30T04: 2020-07-30T04: 2020-07-30T04: 2020-07-30T04: 2020-07-30T04:	Source IP 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11	Source Port 3 3 3 3 3 3 3 3	Destination IP 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200	Destination Port 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Protocol 1 1 1 1 1 1	Category icmp-info icmp-info icmp-info icmp-info	Class Type misc-activity misc-activity misc-activity misc-activity	Message GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF
Intrusion Events Time Stamp 2020-07-30T04: 2020-07-30T04: 2020-07-30T04: 2020-07-30T04: 2020-07-30T04:	Source IP 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11	Source Port 3 3 3 3 3 3 3 3 3 3 3 3	Destination IP 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200	Destination Port 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Protocol 1 1 1 1 1 1 1	Category icmp-info icmp-info icmp-info icmp-info icmp-info	Class Type misc-activity misc-activity misc-activity misc-activity misc-activity	Message GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF
Intrusion Events Time Stamp 2020-07-30T04: 2020-07-30T04: 2020-07-30T04: 2020-07-30T04: 2020-07-30T04: 2020-07-30T04:	Source IP 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11	Source Port 3 3 3 3 3 3 3 3 3 3 3 3 3 3	Destination IP 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200	Destination Port 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Protocol 1 1 1 1 1 1 1 1 1 1 1	Category icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info	Class Type misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity	Message GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF
Intrusion Events Time Stamp 2020-07-30T04:	Source IP 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11	Source Port 3	Destination IP 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200	Destination Port 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Protocol 1 1 1 1 1 1 1 1 1 1 1 1 1	Category icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info	Class Type misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity	Message GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF
Intrusion Events Time Stamp 2020-07-30T04:	Source IP 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11	Source Port 3	Destination IP 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200	Destination Port 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Protocol 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Category icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info	Class Type misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity	Message GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF
Intrusion Events Time Stamp 2020-07-30T04:	Source IP 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11	Source Port 3	Destination IP 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200	Destination Port 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Protocol 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Category icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info	Class Type misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity	Message GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF
Intrusion Events Time Stamp 2020-07-30T04:	Source IP 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11	Source Port 3	Destination IP 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200 204.79.197.200	Destination Port 1	Protocol 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Category icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info	Class Type misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity	Message GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF
Intrusion Events Time Stamp 2020-07-30T04: 2020-07-30T04:	Source IP 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11	Source Port 3	Destination IP 204.79.197.200	Destination Port 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Protocol 1	Category icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info icmp-info	Class Type misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity unknown	Message GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF ET POLICY Net8
Intrusion Events Time Stamp 2020-07-30T04: 2020-07-30T03:	Source IP 172216.14.11 1722.16.14.11 1722.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11 172.16.14.11	Source Port 3	Destination IP 204.79.197.200	Destination Port 1	Protocol 1	Category Icmp-info Icmp-info Icmp-info Icmp-info Icmp-info Icmp-info Icmp-info Icmp-info Icmp-info Icmp-info Icmp-info Icmp-info Icmp-info Icmp-info	Class Type misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity misc-activity unknown unknown	Message GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF GPL ICMP_INF ET POLICY Net8

You can click the individual slices of the pie chart (demarcated by the color) or the legends beside the pie chart to view the top-10 logged and blocked event details for class types, categories, source/destination IPs and ports, and Protocols along with the timestamp.

Intrusio	n Preven	tion	ast 1 Hour 💙		
RemoteC Name	Office	11 Intrusion Ev	ents Logged	0 % Blocked	
				11 Intrusion Events	
Top 10 Logo	ged Events Class Types	Source IPs	Source Ports	estination IPs Destination Ports Protocols	
Top 10 Logo	ged Events Class Types	Source IPs	Source Ports	estination IPs Destination Ports Protocols usion Events Log	ıgged
Top 10 Logg Categories Category icmp-info	ged Events Class Types	Source IPs	Source Ports	estination IPs Destination Ports Protocols usion Events Log 945	igged 5
Top 10 Logg Categories Category icmp-info policy	ged Events Class Types	Source IPs	Source Ports	estination IPs Destination Ports Protocols usion Events Log 945 30	igged 5
Top 10 Logg Categories Category icmp-info policy events	ged Events Class Types	Source IPs	Source Ports	estination IPs Destination Ports Protocols usion Events Log 945 30 11	agged 5
Top 10 Logs Categories Category icmp-info policy events misc	ged Events Class Types	Source IPs	Source Ports	estination IPs Destination Ports Protocols usion Events Log 30 11 11	igged 5

SSL inspection

To view the SSL inspection report, at the network level navigate to **Reports > Security > SSL Inspec-tion** and select the timeline for which you want to view the report.

The **SSL Inspection** section displays the following information:

- Total number of SSL inspection events
- Percentage of SSL inspection events inspected
- Percentage of SSL inspection events bypassed

Event Distribution				:	Scanned Even	ts (over Last 1	Hour)		
11 0 % Scanned Inspected	100 % Bypassed	Scanned Requests (%)	100 80 40 20						
			13:00	13:10	13:20	13:30	13:40	13:50	14:0
							Inspo	ected 🔴 By	ypassed
Top Scanned Events							• Insp	ected 🔴 By	ypassed
Top Scanned Events Sites Security Profiles						Durante	• Inspa	ected • By	ypassed

You can also view a graphical representation of the percentage of SSL inspection events inspected or bypassed over the selected time frame.

Top scanned events The **Top Scanned Events** table provides the SSL inspection details at the top 5 sites. It displays the total number of SSL inspection events, the number of events scanned, and the number of events bypassed at the top 5 sites.

Top Scanned Events			
Sites Security Profiles			
Site Name	Scanned	Inspected	Bypassed
mybranch	11	0	11
			View more affected Sil

Click **View more affected Sites**, to view the SSL inspection details of all the affected sites in the network.

Security SSL Inspection		Last 1 Hour	~	
-------------------------	--	-------------	---	--

Security Profiles				
Search	Q			
Site Name	Scanned	Inspected	Bypassed	
mybranch	11	0	11	

Click an individual site name to view a graphical representation of the SSL inspection details at the site. The **SSL Inspection** of the chosen site also provides the real-time report of the last 1000 scanned and bypassed SSL inspection events from the total number of SSL inspection events (for the selected timeline).

Security SSL I	nspection	Last 1 Hour 🗡				
nybranch	11 Scanned	0% 100 Inspected Bypas) % ssed			
			11 Scanned Events	• 0 Inspected • 11 Bypassed		
canned Events	Source Address	Source Port	Dest Address	Dest Port	Domain	Status
2020-11-26T13:00:01	192.168.0.2	41800	52.42.72.107	443	shavar.services.mozill	IGNORED
2020-11-26T13:15:00	192,168,0,2	45662	64 39 104 113	443	gaopublic og3 apps g	IGNORED
2020-11-26T13:15:01	192.168.0.2	45668	64.39.104.113	443	qaqpublic.qq3.apps.q	IGNORED
2020-11-26T13:16:03	192.168.0.2	45810	64.39.104.113	443	gagpublic.gg3.apps.g	IGNORED
2020-11-26T13:17:04	192 168 0 2	45944	64 39 104 113	443	qaqpublic qq3 apps q	IGNORED
2020-11-26T13:18:29	19216802	59986	151 101 128 223	443	pypi org	IGNORED
2020-11-26T13:28:14	192 168 0 2	38346	34 249 145 219	443	motdubuntu.com	IGNORED
2020-11-26713-28-14	19216802	35364	172 217 20 7/	443	safebrowsing google	IGNORED
2020-11-26T13-45-04	19216802	49548	64 39 104 113	443	agapublic and apps a	IGNORED
2020-11-26112:45:04	10216902	47340	64 20 104 112	442	agenublic and apps a	IGNORED
2020-11-20113:45:06	102160.0.2	49552	64.39.104.113	443		
2020-11-26113:46:07	192.168.0.2	49684	64.39.104.113	443	qaypublic.qg3.apps.q	
2020-11-26113:58:22	192.168.0.2	39128	1/2.217.20.74	443	satebrowsing.google	IGNORED
2020-11-26T14:02:32	192.168.0.2	52056	13.227.219.45	443	nretox.settings.servic	IGNORED
2020-11-26T14:02:33	192.168.0.2	41200	13.227.219.5	443	content-signature-2.c	IGNORED
2020-11-26T14:15:07	192.168.0.2	53424	64.39.104.113	443	qagpublic.qg3.apps.q	IGNORED
2020-11-26T14:15:09	192.168.0.2	53428	64.39.104.113	443	qagpublic.qg3.apps.q	IGNORED
2020-11-26T14:16:11	192.168.0.2	53564	64.39.104.113	443	qagpublic.qg3.apps.q	IGNORED
		52606	64 20 10 4 11 2			

You can click the individual slices of the pie chart (demarcated by the color) or the legends beside the pie chart to view the top-10 scanned, inspected, and bypassed event details for timestamp, source/destination IPs and ports, domain, and status.

Security profiles:

It displays the total number of scanned files, the number of inspected files, and the number of bypassed files scanned by the top 5 security profiles.

Top Scanned Events			
Sites Security Profiles			_
Security Profile	Scanned	Inspected	Bypassed
prof_0_2	12	0	12
prof_default	0	0	0
			View more affected Security Profiles

Click **View more affected Security Profiles**, to view the SSL inspection scan details of all the security profiles.

Security SSL	Inspection		Last 1 Hour	\sim
--------------	------------	--	-------------	--------

Sites Security Profiles				
Search	Q			
Security Profile	Scanned	Inspected	Bypassed	
prof_0_2	12	0	12	
prof_default	0	0	0	

Click an individual Security Profile name to view a graphical representation of its SSL inspection scan details.



Citrix Secure Internet Access report

You can see the CSIA dashboard under the **Reports > Secure Internet Service** page in Citrix SD-WAN Orchestrator. In this page you can see the status of the tunnels whether the tunnel is active or not including the total number of sites in your SD-WAN deployment, number of connected sites using the tunnel direction method, and the total number of tunnels. If host machines are actively connected and access internet resources, the outbound and inbound throughput will be measure.

		Total Sites		Sites	Connected		Total Tu	Innels
		3			1		1	
Status	Tunnel Type	Site Name	Local IP	VPN IP	Throughput (Outbound)	Throughput (Inbound)	Packets Dropped	Packets Fragmented
•	IPSEC	Home110LTE	172.17.30.158, 0	100.000.054.00	1.03 Kbps	3.19 Kbps	0	NA

Throughput usage for the tunnels can also be retrieved from the site-level **Reports > Real Time > IPsec Tunnel**.

ARP Routes	Virtual Path Services	Classes Interface	s Observed Pro	otocols Wan Path	Application Q	OS IPsec Tuni	nel 🗡	
Home110LTE	~	Retrieve latest o	lata					Search Q
Name	State	Service Type	Packets Received	Kbps Received	Packets Sent	Kbps Sent	Packets Dropped	Bytes Droppe
citrixSASService_1	GOOD	Intranet	2813	2.91	2643	1.07	0	0
¢								>

The site-level Routes table can also confirm that the routes to the CSIA service are being used by incrementing Hit Count. Contending default routes (0.0.0.0/0) have higher cost.

Jetwork Reports: Real Time Statistics										``				
ARP	Routes Virt	ual Path Servic	es Classes In	terfaces Observed Pro	tocols Wa	n Path Applic	ation QOS Ot	her Stats 🐱						
Home11	IOLTE		~	Retrieve latest data									0.0.0.0	Q
Num	Network Address	Gateway	Service	Firewall Zone	Reachable	Site	Туре	Protocol	Neighbor Direct	Cost	Hit Count	Eligible	Eligibility Type	Elig
25	0.0.0.0/0		citrixSASService_1	Default_LAN_Zone	YES	Home110LTE	Static		1.0	45	2632	YES	Tunnel	citri
26	0.0.0.0/0		Internet	Untrusted_Internet_Zo	YES	Home110LTE	Static		1.0	46	0	YES	N/A	N/A
27	0.0.0.0/0	•	DC-Home110LTE	Internet_Zone	YES	DC	Dynamic	Virtual WAN	YES	51	0	YES	N/A	N/A
29	0.0.0.0/0		Passthrough	Any	YES		Static			65535	0	YES	N/A	N/A
	00000		Discard	Δαν	VES		Centie			65535	0	VES	N/A	NI/A
31	0.0.0.0.0		Children		16.0		JUNC			47777		16.0	1976	199.0

Extra tunnel information can be obtained from the CSIA portal, which was formed during the creation of the CSIA service on SD-WAN. Navigate to **Connect Devices to Cloud > Tunnels > IPSec Tunnels**.

Coud Connectors Agent Politice							
Psec Tunnels							
Actions *							
sec Settings							
Sec Settings							
Pisec Mode Pisec Reserved IP Range Pisec Local IP Roured II 050.0.016 II 050.0.1 Pisec Tunnel Secret VPN Excluded Subnets IKE Lifetime (minutes) b4a28d330ff57/d9 Rekey Margin (minutes) Rekey Attempts 43000 3 1							
IPsec Mode IPsec Reserved IP Range IPsec Local IP Routed 10.50.0.016 10.50.0.1 Pice Tunnel Secret VPN Excluded Subnets IKE Lifetime (minutes) b4a28d330ff5f7d9 Rekey Margin (minutes) Rekey Attempts 43800 3 1							
Psec Mode IPsec Reserved IP Range IPsec Local IP Round ID 500.01/6 ID 500.1 Psec Tunel Secret VPN Excluded Subnets IEC Lifetime (minutes) Ld2283301757/30 Rekey Margin (minutes) 3000 Round 3 1							
Roured 10.50.0.016 10.50.0.1 Pace Tunel Secret VPN Excluded Subnets IRE Lifetime (minutes) 43800 43800 43800 sey Life (minutes) Rekey Margin (minutes) Rekey Attempts 1 3 1							
Psec Tunnel Secret VPN Excluded Subnets REC Lifetime (minutes) b42284330157709 43000 key Life (minutes) Rekey Margin (minutes) a300 3	10.50.0.1						
b4a28d330rf577d9 43800 tey Life (minutes) Rekey Margin (minutes) a3800 3 a1 anable Mobile User VPN							
Key Life (minutes) Rekey Margin (minutes) Rekey Attempts 43000 3 1	ł						
43800 g 3 g 1							
inable Mobile User VPN	ł						
fer som							
ingured insectionnels							
Add IPsec Tunnel 2 Refresh Filter							

Also, local subnets are automatically defined on the CSIA portal. Navigate to **Network > Local Subnets**. This is the subnet range that is expected from LAN devices connected behind the SD-WAN site and expected to use the tunnel for redirection.

citr	ſİŻ.	Citrix Demo 1 -	Account 14	1375 (Delegated Adr	nin) 👻							_	_			Q, onbos	Welcome, irdsdcustomei
C Loss	\mathcal{Q}	Bandwidth Optimization	ណ៍	Reporting & Analytics	Proxy & Caching	*	onnect Device Cloud	Use & D	rs, Groups evices	Custor	nizations	× ™ 🗗	Network	grations			
не Вура	ess IP Range	🔀 Local Sub	nets	SNMP	Admin SSL Certificates	🖗 Bandwi	dth Tracking	🖷 Internal	Gateways	YLAN	Network /	Advanced Settings					
Loca	al Subne	ets/IP Rar	nges														
Local	Subnets																
Actio	ons • + New	Local Subnet/IP I	Range 🛓	Export Subnets to C	SV @ Quick Edit Local	Subnets									Filter		
~ 1	Priority	Type F N	iltering fethod	Default Policy	Login Group	A thentic N thod	Bandwidth Accounting	Subnet Reporting Group (#)	SSL.	Lock Policy for Non- Authentic Users	Lock Subnet	IP Address & Subnet/Range	Network Tunnel (Type)	ypass roxy Auth	Injected VLAN ID	Note	Actions
	1 :	Subnet IF	Address	1. Default	1. Default	Fed	× Disabled	× Disabled	× Disabled	× Disabled	None	172.17.35.0/255.2	Home110130 (IPS	Disabled	× Disabled		QÊ

Note

The previsioning of the CSIA service automatically associates the **Local Subnet** with the Default security group. Use this security group to configure desired security policies on CSIA.

HDX dashboard and reports

For details on HDX dashboard and reports, see HDX dashboard and reports.

Network Quality

The **Network Quality** report enables a network-level comparison between the virtual overlay and the physical underlay paths in terms of availability and loss, latency, and jitter. This helps to effectively monitor how the overlay is faring relative to the underlay network, and also aids troubleshooting. For Latency and Jitter, only the details of the underlay member paths are displayed.

Quality	ý	Last1Hour ~
Availability	Loss Latency Jitter	Customize Threshold Restore Default Threshold
	Overlay (Virtual Paths across Network)	Underlay (Member Paths across Network)
	17 Overlay Paths 17 Overlay Paths 17 Overlay Paths 10 S Uptime	72 Underlay Paths • 30 Paths • 0% Uptime
Overlay Virtua	LPaths Underlay Member Paths	
Search	٩	
Uptime	From: Site	To: Site
0%	DCVPX_HA	dmzpod6_Clone_1_2_3
0%	dmzpod6_Clone_1_2_3	DCVPX_HA
0%	DCVPX_HA	only110wifi
0%	DCVPX_HA	Sai
0%	DCVPX_HA	chaitanya111
100%	DCVPX_HA	CB210
100%	DCVPX_HA	CB2100site
100%	DCVPX_HA	site110ltewifi
100%	DCVPX_HA	VPXLdot1x
100%	site110ltewifi	DCVPX_HA
100%	VPXLdot1x	CB2100site
100%	CB210	CB2100site
100%	VPXLdot1x	DCVPX_HA
100%	CB210	DCVPX_HA
100%	CB2100site	VPXLdot1x
100%	CB2100site	CB210
100%	CB2100site	DCVPX_HA

Click the table entry to see the detailed view.
← Virtual Path Details	
Branch - DC_MCN 100% Virtual Path Availability	
Virtual Path : DC_MCN-Branch	● Up ● Partially Up ● Down ● Unknown Virtual Path : Branch-DC_MCN
11:01pm 11:11pm 11:21pm 11:31pm 11:41pm 12:01am	11:01pm 11:11pm 11:21pm 11:31pm 11:41pm 12:01am
Member Paths : DC_MCN-Jio-1:Branch-Broadband-Airtel-1	Member Paths : Branch-Broadband-Airtel-1:DC_MCN-Jio-1
DC_MCN-Jio-1:Branch-Broadband-BSNL-2	Branch-Broadband-BSNL-2:DC_MCN-Jio-1

You can customize the threshold for each network quality parameter.

Loss : Custom Thresholds
Green 🔵 <= 5 % Loss
Citrus 🔵 5 - 10 % Loss
Yellow 🔴 >= 10 % Loss
Cancel Save

Quality of Service

N

Quality of Service (QoS) manages data traffic to reduce packet loss, latency, and jitter on the network. For more information, see <u>Quality of Service</u>. The following are two ways to view the Qualityof-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.

letwork Reports : QOS C		Re	elative Time $ \lor $ Interval: Last 1 Hour $ \lor $	Site Group: All 🗸					
				SUMMARY QOS DETAILS					
Bandwidth Distribution (%)	Traffic Type	Traffic Type Bandwidth							
bandwidth bisthouton (a)		Realtime Class	Bandwidth Utilization (%)	Data Volume					
		HDX High	0 %	0 Kb					
	Realtime	Low	0 %	0 Kb					
		Medium	0 %	0 Kb					
		High	0 %	0 Kb					
		Interactive Class	Bandwidth Utilization (%)	Data Volume					
		HDX High	0 %	0 Kb					
		HDX Medium	0 %	0 Kb					
	Interactive	HDX Low	0 %	0 Kb					
Pealtime Interactive Rulk Control		High	0 %	0 Kb					
		Medium	0 %	0 Kb					
		Low	0 %	0 Kb					
		Bulk Class	Bandwidth Utilization (%)	Data Volume					
	Bulk	High	0 %	0 Kb					
	DOIN	Medium	0 %	0 Kb					
		Low	0 %	0 Kb					
	Control	Control Class	Bandwidth Utilization (%)	Data Volume					
		ControlClass	100 %	35.35 Mb					

- 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.

Netv	vork Repo	orts : QoS	2	Relative	Time 🗸 Interva	al: Last 1 Hour	✓ Site Group:	All ~
							SUMMARY	QOS DETAILS
Site :	All	\sim	Traffic Type :	All	~ 5	Select Priority :	All	\sim
Site		Virtual Path	Traffic Type	Priority	Bandwidth	Data Volume	Drop (%)	Drop Volume
Mad	rid	Madrid-San	Control	ControlClass	28.74 KBps	12.93 MB	0 %	0 KB
New	York	NewYork-San	Control	ControlClass	28.57 KBps	12.64 MB	0 %	0 KB
San_	Francisco	San_Francisc	Control	ControlClass	0.05 KBps	21.59 KB	0 %	0 KB
San_	Francisco	San_Francisc	Control	ControlClass	0.05 KBps	21.59 KB	0 %	0 KB
San_	Francisco	San_Francisc	Control	ControlClass	12.86 KBps	5.79 MB	0 %	0 KB
San_	Francisco	San_Francisc	Control	ControlClass	12.69 KBps	5.71 MB	0 %	0 KB
				Page	Size: 25 🗸	Showing 1 - 6 of 6	items Page 1 of	f1 🔹 🕨

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.

Network Reports:	Historical Statis	ics 😋		Relative Time 🗸 Interval:	Last 1 Hour 🗸 Site	Group: All 🗸			
Sites Virtual Paths	Paths WAN Lin	s Interfaces Classes	GRE Tunnels IPSec	Tunnels					
Network Summary : Capacity Utilization Across Sites									
Select Site : All	~								Customize Columns
Site Name	Bandwidth Total	Utilization %	Bandwidth Upload	Bandwidth Download	Available Bandwidth Upload	Permitted Bandwidth Upload	Control Bandwidth Upload	Realtime Bandwidth Upload	Expand/Collapse
Kansas	96.35 Kbps	0.12 %	48.16 Kbps	48.19 Kbps	40 Mbps	40 Mbps	48.16 Kbps	0 Kbps	•
Dallas	38.73 Kbps	0.05 %	24.95 Kbps	13.78 Kbps	40 Mbps	19.61 Mbps	24.95 Kbps	0 Kbps	•

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 Upload: The maximum and the minimum upload speed through the WAN port.
- **Bandwidth Download**: The maximum and the minimum download speed through the WAN port.
- Available Bandwidth Upload: Total bandwidth allocated to all the WAN links of a site.
- **Permitted Bandwidth Upload**: Bandwidth available for transmitting information.
- **Control Bandwidth Upload**: Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.
- **Realtime Bandwidth Upload**: Bandwidth consumed by applications that belong to the realtime class type in the Citrix 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.

You can also export the filtered results in to a CSV or PDF file by using the **Export as CSV** and **Export as PDF** options. The CSV and PDF file name is prefixed with **Network Performance** followed by the date and time when the file is exported.

Virtual paths

To view the Virtual Paths statistics, navigate to Reports > Historical Statistics > Virtual Paths tab.

itrix SD-WAN Orchestrator												
Network Rep	letwork Reports : Historical Statistics C Relative Time V Interval: Last 1 Hour V Site Group: All V											
Sites Virtual	I Paths Pa	aths WAN L	_inks Inte	erfaces C	lasses GRE Tun	inels IPSec Tun	nels					
Network Summary : Uptime Across Virtual Paths												
Select Site :	All		\sim									
Virtual Path Name	Uptime %	Latency	Loss	Jitter	Bandwidth Upload	Control Bandwidth	Realtime Bandwidth	Interactive Bandwidth	Expand/Collapse			
San_Francisco - Belgium	0 %				3.12 Kbps				•			
San_Francisco - London	0 %				1.04 Kbps				•			
London - San_Francisco	0 %				0 Kbps				•			
San_Francisco - Madrid	100 %	2 ms	0 %	2 ms	12.7 Kbps	12.7 Kbps	0 Kbps	0 Kbps	•			
Madrid - San_Francisco	100 %	2 ms	0 %	2 ms	24.35 Kbps	24.35 Kbps	0 Kbps	0 Kbps	•			
NewYork - San_Francisco	100 %	2 ms	0 %	2 ms	24.22 Kbps	24.22 Kbps	0 Kbps	0 Kbps	•			
San_Francisco - NewYork	100 %	2 ms	0 %	2 ms	12.61 Kbps	12.61 Kbps	0 Kbps	0 Kbps	•			

You can view the following metrics:

- Virtual Path Name: The virtual path name.
- **Uptime %**: Rate at which the virtual path is up.
- 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 Upload: Upload (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	D view the Paths statistics, havigate to Reports > Statistics > Paths tab.										
Network Re	oorts : Histori	cal Statis	stics			Relative Time 🚿	/ Interval:	Last 1 Hour \smallsetminus	Site Group:	All v	
Sites Virtua	Paths Paths	WAN Links	s Interfac	es Clas	ises Gl	RE Tunnels IF	PSec Tunnels				
			Netv	vork Sui	nmary :	Uptime Ac	ross Paths				
100% Uptime : 25 % of Paths 0-100% Uptime : 0 % of Paths 0% Uptime : 75 % of Paths 100% Uptime = 0% Uptime											
Select Site :	All	~								Customize Columns	
From WAN Link	To WAN Link	Uptime %	Latency	Loss	Jitter	Bandwidth	Control Bandwidth	Realtime Bandwidth	Interactive Bandwidth	Expand/Collapse	
NewYork-AOL- 1	San_Francisco- Broadband- AMIS-2	100 %	2 ms	0 %	2 ms	15.14 Kbps	15.14 Kbps	0 Kbps	0 Kbps	•	
San_Francisco- Broadband- AMIS-2	Belgium- Verizon_Comm- 2	0 %	0 ms	0 %	0 ms	1.04 Kbps	1.04 Kbps	0 Kbps	0 Kbps	•	

You can view the following metrics:

- From WAN Link: The source WAN link.
- To WAN Link: The destination WAN link.
- **Uptime %**: Rate at which the path is up.
- 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.
- Uptime %: Rate at which the WAN link is up.
- Bandwidth Upload: Upload (LAN to WAN) Bandwidth usage for the selected time period.
- **Bulk Bandwidth Upload**: Upload (LAN to WAN) Virtual Path Bandwidth used by Bulk traffic for the selected time period.
- **Control Bandwidth Upload**: Upload (LAN to WAN) Virtual Path Bandwidth used by Control traffic for the selected time period.
- **Control Packets Upload**: Upload (LAN to WAN) Virtual Path Control packets for the selected time period.
- **Interactive Bandwidth Upload**: Upload (LAN to WAN) Virtual Path Bandwidth used by Interactive traffic for the selected time period.
- **Max Bandwidth Upload**: Max Upload (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.

Network Reports : H	listorical Statistic	s C	R	elative Time 🗸 Interval:	Last 1 Hour 🗸 Site	e Group: All 🗸					
Virtual Paths Paths WAN Links Interfaces Classes GRE Tunnels IPSec Tunnels											
Network Summary : Interfaces (Worst State)											
	DOWN Atleast Once : 0/13 Interfaces (0%)										
	UP Throughout : 13/13 Interfaces (100%)										
		IP	Throughout 😑 DOWN A	tleast Once							
Select Site : All	~				(Ingress = LAN To WAN, Egres	Customize Columns is = WAN To LAN)					
Site Name	Interface Name	Worst State	Tx Bandwidth	Rx Bandwidth	Errors	Expand/Collapse					
Belgium	1	Good	0 Kbps	0 Kbps	0	•					
London	1	Good	0 Kbps	0 Kbps	0	•					

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.

Network Repo	orts : Historio	al Statistics	C		Relativ	e Time 🗸 Interv	al: Last 1 Hour	∽ Site Group:	All		
Virtual Paths F	Paths WAN Lin	ks Interfaces	Classes GF	RE Tunnels IPSe	c Tunnels						
	Network Summary : Bandwidth Utilization across Classes										
Realtime Utilization : 0 % of Total Bandwidth											
	Interactive Utilization : 0 % of Total Bandwidth Bulk Utilization : 0 % of Total Bandwidth										
		Realtim	e Utilization 🛛 😑	Interactive Utiliza	tion 🛛 😑 Bulk Ut	tilization 🔵 Con	trol Utilization				
Select Site :	All	~					(Ingress = LAN To 1	WAN, Egress = WAN 1	Customize Columns To LAN)		
Virtual Path Name	Total Bandwidth	Realtime Bandwidth	Interactive Bandwidth	Bulk Bandwidth	Control Bandwidth	RealTime Bandwidth %	Interactive Bandwidth %	Bulk Bandwidth %	Expand/Collapse		
London - San_Francisco	29.03 Kbps	0 Kbps	0 Kbps	0 Kbps	29.03 Kbps	0	0	0	•		
NewYork - San_Francisco	29.07 Kbps	0 Kbps	0 Kbps	0 Kbps	29.07 Kbps	0	0	0	•		

You can view the following metrics:

- Virtual Path Name: Name of the virtual path.
- **Total Bandwidth**: Total bandwidth consumed by all packet types. Bandwidth = Control Bandwidth + Real-time Bandwidth + Interactive Bandwidth + Bulk Bandwidth.
- **Realtime 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).
- **Control Bandwidth**: Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.
- **Realtime Bandwidth** %: Rate at which bandwidth is consumed by applications that belong to the real-time class type in the Citrix SD-WAN configuration.
- **Interactive Bandwidth** %: Rate at which bandwidth is consumed by applications that belong to the interactive class type in the Citrix SD-WAN configuration.
- Bulk Bandwidth %: Rate at which bandwidth consumed by applications that belong to the bulk

class type in the Citrix SD-WAN configuration.

• **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 <u>GRE Tunnel</u>.

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

Network statistics

The Network Statistics page provides the following real time statistics information under **Reports** > **Real Time** > **Network Statistics**:

- Sites
- Virtual Paths
- WAN Member Paths
- WAN Links
- WAN Link Usage
- MPLS Queues
- Access Interfaces
- Interfaces
- Intranet
- IPsec Tunnel
- GRE

To get a real time statistical report, go to the required tab (such as sites, virtual paths, WAN links), select the site from the drop-down list, and click Retrieve latest data.

Network Statistics

Select Site *								
10790_deaths			~					
Sites Virtual Paths	WAN Memeber	r Paths WAN Lir	nks WAN Link U	sage MPLS Qu	eues Access In	terfaces Interf	aces Intranet	IPsec Tunnel GRE
Retrieve latest d	ata							
LAN to WAN Stats						Search		Q
Service	Packets 0	Bytes $\hat{}$	PktsDrop 0	BytesDrop 0	Pkts/sec 0	Kbps $\hat{\mathbb{Q}}$	PktsDrop/s	KbpsDrop 0 +
Virtual Path	713192	185429920	0	0	2	4.15	0	0
Internet	0	0	0	0	0	0	0	0
Intranet	0	0	0	0	0	0	0	0

Click the plus (+) symbol if you want to add or remove any column from the statistics table and click **Update**.

Add/Remove Cblumns $ imes$	
✓ State	
MTU MTU	
✓ Latency BOWT (ms)	
✓ Worst Jitter (ms)	
Sest Jitter (ms)	
Receive Rate (Kbps)	
Add Columns	
Virtual Path Service Type	
Since Created (s)	
WAN Link Congested	
IPsec Tunnel State	
Update	

Application statistics

The **Application Statistics** page provides the following real time statistics information under **Reports** > **Real Time > App Statistics**:

- Applications
- App QoS
- QoS Classes

- QoS Rules
- Rule Groups

To get a real time statistical report, go to the required tab (such as applications, QoS rule, QoS classes) select the site from the drop-down list, and click **Retrieve latest data**.

App Statistics

Select Site *		~				
Applications App QoS C	QoS Classes QoS Rul	les Rules Groups				
Retrieve latest data]					
				Search		Q
Application	0 Family		Bytes Received	Bytes Sent	Total Bytes	+
HyperText Transfer Protocol	Web		21806929280	1800782481932	1822589411212	
Unknown Protocol	None		0	0	0	

Click the plus (+) symbol if you want to add or remove any column from the statistics table and click **Update**.



Routes statistics

The **Routes Statistics** page provides the following real time statistics information under **Reports > Real Time > Routes Statistics**:

- ARP
- Routes
- Application Routes
- Observed Protocols
- Multicast Group

• NDP Rules Groups

To get a real time statistical report, go to the required tab (such as ARP, Routes, Application Routes) select the site from the drop-down list, and click **Retrieve latest data**.

act Site*					
Select Site		\sim			
P Routes App Ro	outes Multicast Group	NDP Rule Group	ps		
P Routes App Ro	outes Multicast Group	NDP Rule Group	ps		
P Routes App Ro	Multicast Group	NDP Rule Group	DS		
P Routes App R	Multicast Group	NDP Rule Group	DS		

Click the plus (+) symbol if you want to add or remove any column from the statistics table and click **Update**.

Add/Remove Columns	\times
Current Columns	
Vum	
✓ Interface	
VLAN	
✓ IP Address	
MAC Address	
✓ State	
🖌 Туре	
🖌 Reply Age (ms)	
	Update

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.

Netw	ork l	Reports : Real Time Flows C								Si	te Group:	All	\sim
San	Francis	co~ Retrieve latest data	Search	Q									
🗸 Upl	oad 🗸] Download										Customi	Columns
Info	No	Application	Source IP Addr	Dest IP Addr	Source Port	Dest Port	Proto IP	Packets	PPS	Class	Service Name	Age (mS)	Bytes
(i)	1	N/A	172.10.10.6	192.229.232.240	49976	80	TCP (6)	3	0.004	N/A	-	792120	156
(i)	2	N/A	172.10.10.6	192.229.232.240	49837	80	TCP (6)	3	0.001	N/A	-	4114023	156
(i)	3	N/A	172.10.10.6	192.229.232.240	49835	80	TCP (6)	3	0.001	N/A	-	4140148	156
(i)	4	N/A	172.10.10.6	192.229.232.240	49833	80	TCP (6)	3	0.001	N/A	-	4179835	156
(j)	5	N/A	172.10.10.6	192.229.232.240	49970	80	TCP (6)	3	0.002	N/A	-	1745589	156
()	6	N/A	172.10.10.6	192.229.232.240	49831	80	TCP (6)	3	0.001	N/A	-	4220070	156
(j)	7	N/A	172.10.10.6	192.229.232.240	49825	80	TCP (6)	3	0.001	N/A	-	4258507	156
()	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 statistics

The **Firewall statistics** provide the state of the connection, Network Address Protocol (NAT) policies, and filter policies related to a particular session based on the firewall action configured. Firewall statistics also provide complete details about the source and destination of the connection.

To get the real time statistic report, select the site > select the statistics type from the drop-down list (Connection, NAT Policies, Filter Policies) > select the number for maximum entries to display, and click **Retrieve latest data**.

Firewall Statistics		
Select Site *	Stats Type Maximum Entries to display	
	Connections V 100	^
Retrieve latest data	Connections NAT Policies Eliter Policies	
	Search C	
Application [©] Family [©] Routing	g Domain IP Protocol Src IP Addr Dest IP Addr Dest Service Type Related Objects +	
		_

Click the plus (+) symbol if you want to add or remove any column from the statistics table and click **Update**.

Add/Remove Columns	•	\times
✓ Direction		
✓ IP Protocol		
Service Type		
Service Name		
Add Columns		
Search Columns		Q,
Inside IP Address		
Inside Port		
Outside IP Address		
Outside Port		
Allow Related		
	Update	

Cloud Direct

The **Cloud Direct** report provides the summary of the Cloud Direct sites that are deployed in the network, along with the details about subscription used and the current operational status of those sites.

Cloud D	irect									
1 TOTAL SITES	O	1 WAN LINK ISSUES	С	ALTHY						
Search				٩						
Site Name				Subscription Bandwidth (Mbps)	Status		Billing Mode			
dmzpod6 Clo	one 1 2 3			10	Circuit Issues		Trial			
						Showing 1-1 of 1 items	Page 1	of 1	10 rows	~

- Site Name Displays the site name.
- **Subscription Bandwidth (Mbps)** –Displays the subscription bandwidth that is associated with the licensing for the Cloud Direct service.
- Status Displays the site status (active/inactive).
- Billing Mode Displays the billing mode (Demo/Production). The Billing Mode option enables the use of Cloud Direct trial/evaluation licenses. Sites operating with Cloud Direct evaluation licenses must be set to the Demo Billing Mode option. Sites upgrading to full Cloud Direct subscription licenses must be set to the Production Billing Mode option.

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

etwork Re	ports : Ap	oplication Q	uality 📿							Relative Time 🗸	Interval:	Last 3 Hour 🗸	Site Group:	All 🗸
plication QoE	/ All Applic	ations 🗸												
+ App / App G	Group	Search Applica	tions	Q										
6 Total Apps	0 Good	5 Fair	0 Poor	1 No Traffic										View by: 🔠 📰
iperf				Avg QoE: 5/10	ICA Realt	ime			Avg QoE: 5/10	ICA Bulk-	Transfer			Avg QoE: 4.01/10
2 Total Sites	0 Poor	<mark>1</mark> Fair	0 Good	1 Inactive	2 Total Sites	0 Poor	<mark>2</mark> Fair	0 Good	0 Inactive	2 Total Sites	1 Poor	1 Fair	0 Good	0 Inactive
ICA Back	ground			Avg QoE: 3,9/10	ICA Inter	active			Avg QOE: 4,96/10	Ibay.com	.mv			Avg QoE:/10
2 Total Sites	1 Poor	<mark>1</mark> Fair	0 Good	0 Inactive	2 Total Sites	0 Poor	<mark>2</mark> Fair	0 Good	0 Inactive	2 Total Sites	Poor	Fair	Good	2 Inactive
									•••					

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.

Network Reports : Application Quality 3	1 Hour 🗸 Site Group: All 🗸
Application QoE / iperf × / All Stes ×	
Search Stee Q	
2 0 0 1 1 1 treat Strees Good Fair Foor Inactive Traffic Type	: Realtime View by: 💡 🗄
Mage Satellite and the set of the	0
Maikata kai Gibboro Por Sociale Verinamial Ann Okyyu dinaufur Birthani Birt	<u>.</u>
Manual Back Strategies	+ -

You can view the following metrics for Real-time, Interactive, and Hybrid traffic for the selected timeframe:

- **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.

			_												
Network Reports : Applic	ation Qu	ality 🖸									Relative Time	✓ Interval: L	ast 1 Hour 🗸 🛛 Site	Sroup: All	\sim
Application QoE / iperf \sim / M	ICNVPX111 ~	/													
Select Virtual Path : MCNVPX111	- branc	ch_1100	√ Traffic Ty	e : Interactive	\sim										
QoE	Avg Worst Best	10.00 10.00 10.00	11 3:36pm	Realtime Interactive Hybrid	lépm	3:51pm	3:56pm	4:01pm	4:06pm	4:11pm	4:16pm	421pm	4:26pm	431pm	4:36pm
Loss(%)	Avg Worst Best	0.00 0.00 0.00	3:36pm	3:41pm	3:46pm	3:51pm	3:56pm	4:01pm	4:06pm	4:11pm	4:16pm	421pm	4:26pm	431pm	4:36pm
Latency(ms)	Avg Worst Best	1.00 1.00 1.00	2 336pm 15	3:41pm	3:46pm	3:51pm	3:56pm	4:01pm	4:06pm	4:11pm	4:16pm	421pm	4:26pm	431pm	4:36pm
Jitter(ms)	Avg Worst Best	0.00 0.00 0.00	3:36pm	3:41pm	3:46pm	3:51pm	3:56pm	4:01pm	4:06pm	4:11pm	4:16pm	4:21pm	4:26pm	431pm	4:36pm

Application QoE profiles

Click **+ App / App Group** to map applications, custom applications, or application groups to the default or custom QoE profiles.

letwork Re	ports : Ap	plication Q	uality 📿							Relative Time 🗸	Interval:	Last 3 Hour 🗸	Site Group:	All 🗸
pplication QoE	/ All Applica	itions 🗸												
+ App / App G	Group	Search Applica	tions	Q										
6 Total Apps	0 Good	5 Fair	0 Poor	1 No Traffic										View by: 🔠 🗄
iperf				Avg QoE: 5/10	ICA Realt	time			Avg QOE: 5/10	ICA Bulk	Transfer			Avg QoE: 4.01/10
2 Total Sites	0 Poor	1 Fair	0 Good	1 Inactive	2 Total Sites	0 Poor	<mark>2</mark> Fair	0 Good	0 Inactive	2 Total Sites	1 Poor	1 Fair	0 Good	0 Inactive
ICA Back	ground			Avg QoE: 3.9/10	ICA Inter	active			Avg QOE: 4,96/10	Ibay.com	.mv			Avg QoE:/10
2 Total Sites	1 Poor	<mark>1</mark> Fair	0 Good	0 Inactive	2 Total Sites	0 Poor	<mark>2</mark> Fair	0 Good	0 Inactive	2 Total Sites	Poor	Fair	Good	2 Inactive

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.

			X
Type *	Application *	QoE Profile *	<u>+ New QoE Profile</u>

Click **+ New QoE Profile** to create an 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%.

Add App/App Group					\times
Type * Application	~	Application *	~	QoE Profile * DefaultQOEProfile	<u>+ New QoE Profile</u>
Profile Configuration					
Profile Name * Test-Profile	Traffic Type * Hybrid	~			
Realtime Configuration					
One Way Latency (ms) *		Jitter (ms) *		Packet Loss (%) *	
Interactive Configuration					
Expected Burst Rate (%) *	Packet Loss p	per Flow (%) *			
60	2				
Cancel Done					

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.

O365 Metrics

Citrix SD-WAN allows you to not only perform beacon probing, but also determines the latency to reach Office 365 endpoints through each WAN link. The latency is the round trip time taken to send a request and get a response from the Office 365 beacon service over a WAN link. This enables network administrators to view the beacon service latency report and manually choose the best internet link for direct Office 365 breakout. Beacon probing is enabled only through the Citrix SD-WAN Orchestrator service. By default, beacon probing is enabled on all Internet enabled WAN links (except metered WAN links) when Office 365 break-out is enabled through the Citrix SD-WAN Orchestrator service.

The O365 Metrics dashboard displays the following information:

- Site Name: Name of the site.
- WAN Link name: Name of the WAN link.
- Availability: Availability status of the WAN link.
- Latency (ms): Average round trip time through the WAN link.
- **Lowest Latency**: The lowest latency count of the WAN link for a selected time period.
- WAN Link Selected: The number of times the WAN link was chosen for Office 365 optimization.
- **Total Decisions taken**: Total number of times a decision to choose a WAN link is taken, for the selected time interval.

									Change Role	\$ 0
Q	DASHBOARD	ĺ	Network Reports: 0365	Metrics 2			Relative 1	ime 🗸 Interval: Last 30 Mins	Site Group: All	
	REPORTS	~	Site Name	WAN Link Name	Availability	Latency (ms)	Lowest Latency (ms)	WAN Link Selected	Total Decisions Taken	
		- 1	BR1100_HF	BR1100_HF-Broadband-Airtel-1	No	21.14	16.17	0	0	
	Alerts	- 1	MCN_HF	MCN_HF-Broadband-Airtel-1	Yes	423.77	416.23	0	0	
	Usage	- 1	MCN_HF	MCN_HF-Broadband-Airtel-2	No	421.21	416.60	1	1	
	Wi-Fi	- 1								
	Inventory	- 1								
	Security	>								
	Secure Internet Servio	ce								
	HDX	>								
	Quality									
	QoS	- 1								
	Historical Statistics	- 1								
	Real Time	· ·								
	Cloud Direct									
	Application Quality	- 1								
	0365 Metrics	- 1								
	CAS Analytics									
	Top Talkers									

The application QoE report displays a dashboard that provides the Application QoE data of all the configured applications at all the sites.

Site reports

July 15, 2022

The **Site Reports** provide visibility into site-level alerts, usage trends, quality, device information, and firewall statistics.

To view the reports, navigate to **Partner > Provider > Customer > Site > Reports**.

Alerts

The site administrator can review a detailed report of all the events and alerts generated at a site.

The Alerts report includes the severity, site at which the alert originated, alert message, time, and other details.

Site Report : Alerts		
Delete Alerts	Search Q 216 TOTAL	10 17 189 HIGH MEDIUM LOW
Severity Source	Message	Time
Low APPLIANCE	The state of Virtual Path San_Francisco-Madrid has changed from BAD to GOOD	Jan 30th 2020, 12:35 am
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
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
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
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
High APPLIANCE	The Virtual Path San_Francisco-Madrid is no longer DEAD	Jan 30th 2020, 12:35 am
Low APPLIANCE	Ethernet link on device 4 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
Low APPLIANCE	Ethernet link on device 3 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
Low APPLIANCE	Ethernet link on device 2 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
Low APPLIANCE	Ethernet link on device 1 changed from ETH_LINK_DOWN to ETH_LINK_UP.	Jan 30th 2020, 12:15 am
Low APPLIANCE	The state of Virtual Path San_Francisco-Madrid has changed from BAD to GOOD	Jan 24th 2020, 12:05 pm
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
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
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
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
High APPLIANCE	The Virtual Path San_Francisco-Madrid is no longer DEAD	Jan 24th 2020, 12:05 pm
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 statistical 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.

Wi-Fi

For an SD-WAN appliance configured as a Wi-Fi access point, the Wi-Fi report provides details about the signal strength, number of devices connected to Wi-Fi and the Wi-Fi data used within the site. To view a Wi-Fi report, at the site level, navigate to **Reports** > **Wi-Fi**.

Wi-Fi												Last 1 M	Ionth 🗡
Signal Strengt 13 Devices As of current date,	th 9 Good (2 -60dBm) time	4 Fair (≥ -75dBm)	O Poor (90dBm)	Connected Devices	32 0	Sunday, No Fair: 4	15, 02:00 16. Nov	Signal Strength	n (over Last 1 Mon	th) 22. Nov	24. Nov Cood	Fair	26. Nov Poor
Connected De 13 Devices As of current date	evices 5 sdwan-110-1-r. Corporate time	8 sdwan110_1 Home		Connected Devices	32 0	14. Nov	16. Nov	Connected Devic	es (over Last 1 Mo 20. Nov sdwa	22. Nov	24. Nov an-110-1-radius	• sdv	26. Nov wan110_1
Data Utilizatio	9.05 KB sdwan-110-1-ra Corporate	35.41 KB sdwan110_1 Home		Data utilized (GB)	80 0	14. Nov	16. Nov	Data Utilization	n (over Last 1 Mor 20. Nov • sdwa	th) 22. Nov an_open • sdw	24. Nov an-110-1-radius	• sdv	26. Nov wan110_1

Signal Strength

The signal strength determines the wireless signal power level received by the wireless client. Strong signal strength indicates reliable high-speed connection. Signal strength is represented in decibels per milliwatt (dBm). The closer the value is to zero, the stronger the signal.

Signal Strength	dBm
Good	or = -60 dBm
Fair	or = -75 dBm
Poor	or = -90 dBm

You can view the average signal strength, the total number of devices connected, and the number of devices with good, fair, and poor signal strength.



You can also select the timeline to view a graphical representation of the historic data. The graph shows the number of devices that have good, fair, and poor signal strength for the selected period.



Connected devices

The **Connected devices** section displays the total number of devices, at the site, that are currently connected to Wi-Fi. You can also see the number of appliances connected to each corporate or home SSID configured on the appliance. There can be a maximum of four SSIDs.

Connected Devices



As of current date, time

You can also select the timeline to view a graphical representation of the historic data. The graph shows the number of devices connected to each SSID over the selected period. Hover the mouse over a bar to view the exact number of devices connected to each SSID at specific time.



Data utilization

The **Data utilization** section displays the total amount of Wi-Fi data used, at the site, by the connected appliances at the current moment. You can also view the data used by devices connected to each corporate or home SSIDs.

Data Utilization

 44.45 KB
 9.05 KB
 35.41 KB

 Data Utilized
 sdwan-110-1-ra
 sdwan10_1

 Corporate
 Home

As of current date, time

You can also select the timeline to view a graphical representation of the historic data. The graph shows the amount of data used by the devices connected to each SSID over the selected period. Hover the mouse over a bar to view the exact data utilization by devices connected to each SSID for specific time.



Usage

The usage table lists the Wi-Fi users and Wi-Fi authentication failure logs at the site.

Users The **Users** table lists all the Wi-Fi users at a site along with parameters such as signal strength, upload data, and download data. Click the parameter header to sort the column in descending order.

Users Authentication Lo	g Failures					
Username / MAC ID	SSID Name	Authentication Type	IP Address	Signal Strength	Upload Data	Download Data
92:14:99:3f:2d:0b	sdwan110_1	WPA2-Personal	192.168.3.76	-56 dBm	887.64 KB	951.74 KB
a2:ea:f4:19:cf:fb	sdwan110_1	WPA2-Personal	192.168.3.85	-60 dBm	4.01 MB	6.79 MB
a2:f7:69:59:b4:5d	sdwan110_1	WPA2-Personal	192.168.3.98	-53 dBm	3.06 MB	1.94 MB
andreaspo	sdwan-110-1-radius	WPA2-Enterprise	192.168.3.53	-51 dBm	119.89 MB	105.17 MB
andreaspo	sdwan-110-1-radius	WPA2-Enterprise	192.168.3.54	-56 dBm	303.05 KB	228.56 KB
andreaspo	sdwan-110-1-radius	WPA2-Enterprise	192.168.3.56	-36 dBm	82.3 KB	50.93 KB
andreaspo	sdwan-110-1-radius	WPA2-Enterprise	192.168.3.62	-53 dBm	232.22 MB	192.75 MB
andreaspo	sdwan-110-1-radius	WPA2-Enterprise	192.168.3.64	-58 dBm	114.38 MB	100.62 MB
andreaspo	sdwan-110-1-radius	WPA2-Enterprise	192.168.3.85	-56 dBm	1.16 MB	2.41 MB
c2:8f:82:ac:96:33	sdwan-110-1-radius	WPA2-Enterprise	192.168.3.68	-35 dBm	116.75 KB	84.1 KB
dc:a6:32:cf:3e:4c	sdwan110_1	WPA2-Personal	192.168.3.62	-53 dBm	525.48 KB	6.01 MB
l can ta c	1	111010 D	1001000000	ex le		007 70 1/0

Click **View more** to view all the Wi-Fi users at the site. You can select the period or search the list by user name.

Wi-Fi						Last 1 Month 🗡
Users Authenticatio	n Log Failures					
m		Q				
	COID Name	Augh and in dian Truck	ID Address	Circuit Character	Universit Data	Deverte et Data
Username / MAC ID	sold1	WDA2 Personal	IP Address	79 dBm		
mariate	ssiul	WPA2-Feisoria	192.100.1.2	-70 dbm	401.06 MD	151.00 MD
mariats	sawani iu-3_ssid2	WPAZ-Enterprise	192.108.1.20	-23 aBm	491.20 MB	101.20 MB
mariats	ssid3	WPA2-Enterprise	192.168.0.20	-25 dBm	1.03 KB	1.91 MB

Authentication failure logs The authentication failure logs table displays all the Wi-Fi authentication failures at the site. You can view the MAC address and IP address of the client that is trying to connect to a specific SSID along with authentication failure time.

Users Authentication Log Fai	Authentication Log Failures						
User ID/MAC ID	Authentication Type	SSID Name	IP Address	Authentication Failures(s)	Last Authentication Failure Time		
andreaspo	WPA2-Enterprise	sdwan-110-1-radius	192,168,3,56	1	26th Nov 2020, 16:08		

Click **View more** to view all the authentication failure logs. You can select the period or search the list by user name.

Wi-Fi					Last 1 Month 💙
Users Authentication Lo	g Failures				
m	Q				
User ID/MAC ID	Authentication Type	SSID Name	IP Address	Authentication Failures(s)	Last Authentication Failure Time
mariats	WPA2-Enterprise	sdwan110-3_ssid2	192.168.1.20	4	2nd Dec 2020, 17:50

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

Quality	2 ³						Relative Tim	e 🗸 Interval:	Last 1 Hour $ \smallsetminus $
elect Virtua	l Path : DCV	PX_HA - Sai		✓ Metric :	Availability	~	🔵 Up 🥚	Partially Up 🥚	Down 🔵 Unknow
									Export as CS
Downloa	d : Sai -> DC	VPX_HA			Upload: D	CVPX_HA	-> Sai		
Path	Uptime (%)	Good Time (%)	Bad Time (%)	Unknown Time (%)	Path	Uptime (%)	Good Time (%)	Bad Time (%)	Unknown Time (9
Overlay				-	Overlay	0	0	0	33.33
					Underlay	0	0	0	0
					Virtual Pa	ath :			

CSV export reports

With the **Export as CSV** capability, you can download the path graph points (virtual/member path) for any time series (hourly, weekly, and so on) as an excel Comma-separated Value (CSV) file and be able to plot all distinct points of data for a particular site report.

To download/export the path graph as CSV, navigate to **Reports > Quality** at site level. Select the site and metric from the drop-down list and click the **Export as CSV** link.

Select the path that you want to fetch the data for and click **Download Graph Points**.

Note: Selected Path Graph points (Time and Value) will be available in the downloaded CSV file

	Path Name
\checkmark	DCVPX_HA-Sai
	DCVPX_HA-Broadband-Telerama-1:Sai-Broadband- ACT-1
\checkmark	DCVPX_HA-Broadband-Telerama-1:Sai-Broadband- AOL-2

Download Graph Points

By default, all the path check boxes are auto selected. You can modify it as needed.

Note

If paths are selected, the Download Graph Points button remains disabled.

Path Name
DCVPX_HA - Sai
DCVPX_HA-Broadband-Telerama-1:Sai-Broadband- ACT-1
DCVPX_HA-Broadband-Telerama-1:Sai-Broadband- AOL-2

Download Graph Points

Currently, the naming convention of the downloaded CSV file is **SiteQuality** followed by the download. You can view each path with a pair of time and value along with a unique identifier. You can see the time in milliseconds and the value as in unit.

				SiteQuality_2022-01-18T13_06_12+05_30
1	DCVPX_HA - Sai-time	DCVPX_HA - Sai-value	DCVPX_HA-Broadband-Telerama-1:Sai-Broadband-ACT-1-time	DCVPX_HA-Broadband-Telerama-1:Sai-Broadband-ACT-1-value DCVPX_H
2	1642487670572	2	1642487670572	2
3	1642487730572	2	1642487730572	2
4	1642487790572	2	1642487790572	2
5	1642487850572	2	1642487850572	2
6	1642487970572	2	1642487910572	2
7	1642488030572	2	1642487970572	2
8	1642488090572	2	1642488030572	2
9	1642488150572	2	1642488090572	2
10	1642488210572	2	1642488150572	2
11	1642488270572	2	1642488210572	2

Based on the following metric selection, you can see that different values are getting generated in the excel sheet:

- Loss: Value shows in %.
- Latency and Jitter: Value shows in milliseconds.
- Throughput: Value shows in Kbps.
- Availability: Shows the path up, partially up, down, and unknown time.
 - * If the value is 4, then the path is in Up state.
 - * If the value is 3, then the path is partially Up state.
 - * If the value is lesser than 3, then the path is in Bad/down state.



Latency

Loss

Select Virtual Path :	London - New	/ork ~	Metric : Loss	~				
WAN -> LAN				LAN -> WAN				
Path	Max (%)	Avg (%)	Min (%)	Path	Max (%)	Avg (%)	Min (%)	
Overlay	0	0	0	Overlay	0	0	0	
Underlay	0	0	0	Underlay	0	0	0	
Virtual Path : London - NewYork (Percent %) 9:42am 9:52am 10:02am 10:12am 10:22am 10:42am 0								
Member Paths : Broadband-arnes-1 : Int	ternet-aol-1 (Percent %)			Member Paths : Internet-aol-1 : Broadba	and-arnes-1 (Percent %)			
0	000000000000000000000000000000000000000		9999999 - 99999990	0			000000000000000000000000000000000000000	

Jitter

Select Virtual Path :	London - New	York 🗸	Metric : Jitter	~					
WAN -> LAN				LAN -> WAN					
Path	Max (ms)	Avg (ms)	Min (ms)	Path	Max (ms)	Avg (ms)	Min (ms)		
Overlay	2	2	2	Overlay	2	2	2		
Underlay	2	2	2	Underlay	2	2	2		
Virtual Path : London - NewYork (Milliseconds) 9:43am 9:53am 10:03am 10:13am 10:23am 10:43am 2.25 1.5 0.75 0									
Member Paths :				Member Paths :					
Broadband-arnes-1 : In 3 2.25 1.5 0.75 0	ternet-aol-1 (Millisecond	5)	00000 000000000	Internet-aol-1 : Broadb 3 2.25 1.5 0.75 0	and-arnes-1 (Millisecond	5)			

Throughput

Select Virtual Path :	London -	NewYork	✓ Metric : Through	uput 🗸 Units :	Mbps	\checkmark	
WAN -> LAN				LAN -> WAN			
Path	Max	Avg	Min	Path	Max	Avg	Min
Overlay	0.01 Mbps	0.01 Mbps	0.01 Mbps	Overlay	0.01 Mbps	0.01 Mbps	0.01 Mbps
Underlay	0.01 Mbps	0.01 Mbps	0.01 Mbps	Underlay	0.01 Mbps	0.01 Mbps	0.01 Mbps
Virtual Path : London - NewYork 9,45am 0.75 0.5 0.5	(Mbps) 9:55am 10:05	5am 10:15am 10	10:45am 10:45am	Virtual Path : London - NewYork 9:45am 0.75 0.5 0.5	(Mbps) 9:55am 10:00	5am 10:15am 10	10:45am 10:45am
Member Paths	5:			Member Path	S :		
Broadband-arnes-1:	Internet-aol-1 (Mbps)		Internet-aol-1 : Bro	adband-arnes-1 (Mbps	;)	
0.75				0.75			
0.5				0.5			
0.25				0.25			
0			0000000-000000000	0		000000-0000000	

Quality of Service

Quality of Service (QoS) manages data traffic to reduce packet loss, latency, and jitter on the network. For more information, see <u>Quality of Service</u>. The following are two ways to view the Qualityof-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.

Site Report : QoS C Select Virtual Path : London - NewYork V			Relative Time 🗸	Interval: Last 1 Hour V
Bandwidth Distribution (%)	Traffic Type	Bandwidth		
		Realtime Class	Bandwidth Utilization (%)	Data Volume
		HDX High	0 %	0 Kb
	Realtime	Low	0 %	0 Kb
		Medium	0 %	0 Kb
		High	0 %	0 Kb
		Interactive Class	Bandwidth Utilization (%)	Data Volume
		HDX High	0 %	0 Kb
	Interactive	HDX Medium	0 %	0 Kb
		HDX Low	0 %	0 Kb
Realtime Interactive Rulk Control		High	0 %	0 Kb
		Medium	0 %	0 Kb
		Low	0 %	0 Kb
		Bulk Class	Bandwidth Utilization (%)	Data Volume
	Bulk	High	0 %	0 Kb
	BUIK	Medium	0 %	0 Kb
		Low	0 %	0 Kb
	Control	Control Class	Bandwidth Utilization (%)	Data Volume
	Control	ControlClass	100 %	90.2 Kb

- 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.

Site Report : QoS C				Rela	tive Time $\!$	Interval:	ast 1 Hour 🗸
					SUMN	MARY	QOS DETAILS
Select Virtual Path : London - NewYork	Traffic Type : All		\sim				
12.15 Kb		Traffic Type	Priority	Bandwidth	Data Volume	Drop (%)	Drop Volume
		Realtime	HDX High	0 Kbps	0 Kb	0 %	0 Kb
		Realtime	Low	0 Kbps	0 Kb	0 %	0 Kb
		Realtime	Medium	0 Kbps	0 Kb	0 %	0 Kb
		Realtime	High	0 Kbps	0 Kb	0 %	0 Kb
8 Kb		Interactive	HDX High	0 Kbps	0 Kb	0 %	0 Kb
		Interactive	HDX Medi	0 Kbps	0 Kb	0 %	0 Kb
		Interactive	HDX Low	0 Kbps	0 Kb	0 %	0 Kb
		Interactive	High	0 Kbps	0 Kb	0 %	0 Kb
		Interactive	Medium	0 Kbps	0 Kb	0 %	0 Kb
4 Kb		Interactive	Low	0 Kbps	0 Kb	0 %	0 Kb
		Bulk	High	0 Kbps	0 Kb	0 %	0 Kb
		Bulk	Medium	0 Kbps	0 Kb	0 %	0 Kb
•		Bulk	Low	0 Kbps	0 Kb	0 %	0 Kb
0 Kb	29am 10:49am	Control	ControlCl	12.02 Kbps	90.17 Kb	0 %	0 Kb
→ realtime → interactive → bulk → co	ntrol	Page Siz	e: 25 🗸 :	Showing 1 - 14	of 14 items	Page 1 of 1	< >

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 > Historical Statistics > Virtual Paths tab.

Site Report : Historical Statistics C [*] Interval: Last 1 Hour v											
Virtual Path	Virtual Paths Paths WAN Links Interfaces Classes Services GRE Tunnels IPSec Tunnels										
Select Virtual Path : Madrid - San Francisco \checkmark View / Hide All Graphs Customize Columns											
Virtual Path Name	Latency	Loss	Jitter	Bandwidth Upload	Control Bandwidth	Realtime Bandwidth	Interactive Bandwidth	Bulk Bandwidth	Expand/Collapse		
Madrid - San Francisco	2 ms	0 %	2 ms	24.43 Kbps	24.44 Kbps	0 Kbps	0 Kbps	0 Kbps			
Latency (ms) 10:20pm 10:30pm 10:40pm 10:50pm 11:00pm 11:20pm 2.25 1.5 0.75 0 Jitter (ms) 3 2.25 1.5 0.75 0 1.5 0.75 0 1.5 0 1									0pm 11:20pm		
30 16 8 0 Interactive B	andwidth (Kbj	ps)			Bul	0	s)				
0						0					

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 Upload: Upload (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.
- **Realtime 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	C						Relative 1	ime 🗸 Interval:	Last 1 Hour \lor
Virtual Paths	Paths WA	N Links In	terfaces C	lasses Sen	vices GRE Tunne	ls IPSec Tunnel	S			
Select Virtual Pat	h: London	- NewYo	rk	~					View / Hide All Gra	Customize Columns
From WAN Link	To WAN Link	Latency	Loss	Jitter	Bandwidth	Control Bandwidth	Realtime Bandwidth	Interactive Bandwidth	Bulk Bandwidth	Expand/Collapse
London- Broadband- ARNES-1	NewYork- AOL-1	2 ms	0 %	2 ms	12.02 Kbps	12.02 Kbps	0 Kbps	0 Kbps	0 Kbps	-•
Latency (ms)	3am 10:28am	10:38am	10:48am	10:58am	11:18am	Loss (%) 10:18a	m 10:28am	10:38am 10:	48am 10:58am	11:18aņ
2.25										
1.5	000000000000000000000000000000000000000	000000000000	00000000000	000000000000		000				0000000000000
0.75										
0 Jitter (ms)						Bandwidth (Kbp	s)			
3						14	000000000000000000000000000000000000000	000000000000000000000000000000000000000		000000000000000000000000000000000000000
1.5	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	00000000000	8				
0.75						4				
0						0				
Control Bandw	idth (Kbps)					Realtime Bandw	idth (Kbps)			
	-20000000000000000000000000000000000000	000000000000000000000000000000000000000	00000000000		10000000000					
8						098	000000000000000000000000000000000000000	000000000000000000000000000000000000000	000000000000000000000000000000000000000	- 00000000000000
4										
Interactive Ban	dwidth (Kbps)					Bulk Bandwidth	(Kbps)			
00	000000000000000000000000000000000000000	00000000000	0000000000	000000000000000000000000000000000000000	0000000000	008	0000000000000	000000000000000000000000000000000000000		- 003800380038003800
l!						L				

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 Upload: Upload (LAN > WAN) Bandwidth usage for the selected time period.
- Bulk Bandwidth Upload: Upload (LAN > WAN) virtual path bandwidth used by Bulk traffic for the selected time period.
- **Control Bandwidth Upload**: **Upload (LAN > WAN) virtual path bandwidth** used by Control traffic for the selected time period.
- Control Packet Upload: Upload (LAN > WAN) Virtual Path Control packets for the selected time period.
- Interactive Bandwidth Upload: Upload (LAN > WAN) virtual path bandwidth used by Interactive traffic for the selected time period.
- Max Bandwidth Upload: Maximum upload (LAN > WAN) bandwidth used in a minute for the

selected time period.

- Min Bandwidth Upload: Minimum upload (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 statistical 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.

/irtual Paths Paths	WAN Links Interfaces	Classes Services C	GRE Tunnels IPSec Tunnels		
ect Virtual Path : Lon	don - NewYork	~			View / Hide All Graphs Customize Co
oS Class	Bandwidth	Data Volume	Drop Volume	Drop Percent	Expand/Collapse
ontrol - ControlClass	12.03 Kbps	90.2 Kb	0 Kb	0 %	•
andwidth (Kbps) 14 11:07am 11: 000000000 8 4	17am 11:27am 11:37a 	n 11:47am 1;	Data Volume (Kb) 2:07pm 101 11:07am 60 	11:17am 11:27am 11:3	37am 11:47am 12:07 6

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 not intercepted, delayed, shaped, or changed by the SD-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.

Site Re	port : His	torical Stati	stics C	-		Relative Time	✓ Interval: Last 1 Hour ∨
Virtual Pa	aths Paths	s WAN Links	Interface	s Classes Service	s GRE Tunnels IPS	ec Tunnels	
Service :	Passthrough) v				Vier	w / Hide All Graphs Customize Columns
Site Na	Intranet		load	Packets Upload	Packets Dropped Upload	Drop Percentage Upload	Expand/Collapse
Madrid		0.01 Kbps		10	0	0 %	-•
Bandwid 1 0.75 0.5 0.25 0 Packets I	th Upload (Kt 10:29pm 1 	ops) 0:39pm 10:49p	m 10:59pr	n 11:09pm 11:2	Packets Upload (r	count) m 10:39pm 10:49pm 10:5	59pm 11:09pm 11:29pm

You can view the following metrics:

- Site Name: The site name.
- Bandwidth Upload: Upload (LAN > WAN) Bandwidth usage for the selected time period.
- Packets Upload: Upload (LAN > WAN) Packets sent for the selected time interval.
- Packets Dropped Upload: Number of upload packets dropped.
- Drop Percentage Upload: Percentage of upload 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 <u>GRE Tunnel</u>.

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

Network Statistics

You can get the following real time statistics information under **Reports > Real Time > Network Statistics**:

- Site
- Virtual Paths
- WAN Member Paths
- WAN Links
- WAN Link Usage
- MPLS Queues
- Access Interfaces
- Interfaces
- Intranet
- IPsec Tunnel
- GRE

To get the real time statistical report, go to the required tab (such as site, virtual paths, WAN links) and click **Retrieve latest data**.

Network Statistics

Sites	Virtual Pa	ths	WAN Mer	nebe	r Paths V	VAN Lii	nks WAM	N Link U	sage MP	LS Qu	eues Ac	cess Int	erfaces	Interfa	ces Intra	inet	IPsec Tunnel	GRE
Retrieve latest data																		
LAN to W	AN State	s											[Search				Q
Service			Packets		Bytes		PktsDrop		BytesDrop		Pkts/sec		Kbps		PktsDrop/s		KbpsDrop	÷ +
Virtual Pa	ath		812207877		814757469	80	0		0		1861.2		1493.6	3	0		0	
Internet			0		0		0		0		0		0		0		0	
Intranet			958149		197846568	3	0		0		2.2		3.63		0		0	

Click the plus (+) symbol if you want to add or remove any column from the statistics table and click **Update**.

Add/Remove Columns	×
Current Columns	
Service	
Packets	
Sytes	
PktsDrop	
J BytesDrop	
Pkts/sec	
✓ Kbps	
✓ PktsDrop/s	
✓ KbpsDrop	
	Update

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 Citrix SD-WAN Orchestrator service.

You can view the direction, no of packets, delta packets, and mismatched DSCP packets for Intranet and Virtual path services.

Site Reports:Real Time	e Statistics												
ARP Routes Virtual	Path Services	Classes Ethe	ernet Observe	ed Protocols	Wan Path A	Application QOS	MPLS Queu	es 🗸					
Retrieve latest data												Searc	th Q
Intranet Data Rates													
Name	Direction	Intranet Packet	3	Intranet Kbps		Delta Intranet F	ackets	Delta Intranet k	В	Mismatched DSC	P 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	
Virtual Path Service Data Ra Name	Direction	Virtual Path Se	rvice Packets	Virtual Path Se	vice Kbps	Delta Virtual Pa Packets	th Service	Delta Virtual Pa	th Service kB	Mismatched DSC	P Packets	1 to 2 of 2 I < <	Page 1 of 1 > > 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
Private MPLS Queues Private MPLS BRANCH_1-WL-2	MPLS Queue branchv6queue	1	Access Interface BRANCH_1-WL-	e 2-Al-1	IP Address b::3		Proxy Address N/A		Proxy ARP State	2	MAC N/A	1 to 2 of 2 K K	Page 1 of 1 > > > IRP Reply Age(ms)
MCN_DC-WL-2	ipvбqueue		N/A		0.0.0.0		N/A		N/A		N/A		
4													

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.

Application statistics

You can get the following real time statistics information under **Reports > Real Time > App Statistics**:

- Applications
- App QoS
- QoS Classes
- QoS Rules
- Rule Groups

To get the real time statistical report, go to the required tab (such as applications, App QoS, QoS rule) and click **Retrieve latest data**.

App Statistics				
A.				
Applications App QoS QoS C	lasses QoS Rules Rules Groups			
Retrieve latest data				
			Search	Q
Application 0	Family $\hat{\mathbf{a}}$	Bytes Received	Bytes Sent	Total Bytes 🗘 🕂
Generic Routing Encapsulation	Tunneling	0	2096880	2096880
HyperText Transfer Protocol	Web	2538169783154	30731383708	2568901166862
Internet Security Association and K	Encrypted	0	169756236	169756236

Click the plus (+) symbol if you want to add or remove any column from the statistics table and click **Update**.

Add/Remove Columns	\times
Current Columns	
Application	
🖌 Family	
✓ Bytes Received	
✓ Bytes Sent	
✓ Total Bytes	
	Update

Routes statistics

You can also get the following real time statistics information under **Reports > Real Time > Routes Statistics**:

- ARP (Address Resolution Protocol)
- Routes
- App Routes
- Observed Protocols
- Multicast group
- NDP Rule Groups

To get the real time statistical report, go to the required tab (such as ARP, Routes, App Routes) and click **Retrieve latest data**.

ARP	Routes A	pp Routes	observe	ed Protocols	Multicast	Group NDP Ru	le Grou	ps			
Ret	rieve latest d	ata									
Gateway End Use	/ ARP Timer: 1 r ARP Timer: 1	000 ms 000 ms							Search		Q
Num	Interface		VLAN 0	IP Address		MAC Address		State	Туре	Reply Age (ms)	+
4	1/2		0	172.96.2011		204771-014772		READY_ACTIVE	PERSISTENT	424	
3	1/4		0	172.96.221		204771414772		READY_ACTIVE	PERSISTENT	25	
2	1/5		0	172.96.23.51		010-29-43-24		READY_ACTIVE	END_USER	926	
1	1/5		0	172.96.23.52		00.0x 29.50 Birds		READY_ACTIVE	END_USER	977	
0	1/1		0	172.16.25.50		00.0128/064107		READY_ACTIVE	END_USER	777	
5	1/3		0	17236-213		204771454772		READY_ACTIVE	PERSISTENT	125	

Click the plus (+) symbol if you want to add or remove any column from the statistics table and click **Update**.

Add/Remove Columns	×
Current Columns 👌	
V Num	
✓ Interface	
VLAN	
✓ IP Address	
MAC Address	
State	
🗸 Туре	
Reply Age (ms)	
	Update

Firewall statistics

The **Firewall statistics** provide the state of the connection, Network Address Protocol (NAT) policies, filter policies 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.

To get the real time statistical report, select the statistics type from the drop-down list (Connection, NAT Policies, Filter Policies) > Select the number for maximum entries to display, and click **Retrieve**

latest data.

Fire	wal	l Statistic	S											
Stats Typ	0						Μ	aximum Entries to dis	play					
NAT	Polic	ies					× [100 ~						
Re	triev	e latest data												
NAT Pol NAT Pol Port Re Destina	licies licies strict tion l	Displayed: 0 In Use: 0 out of 1 ed Dynamic NAT NAT Policies In Us	000 Policies I se: 0 out c	n Use: 100 out of of 100	100					Search				Q
ID		Rule Type		Rule Parent		Direction		IP Protocol		Service Type		Service Name	۰.	+

Click the plus (+) symbol if you want to add or remove any column from the statistics table and click **Update**.

Add/Remove Columns	•	\times
✓ Direction		
V IP Protocol		
Service Type		
Service Name		
Add Columns		
Search Columns		Q,
Inside IP Address		
Inside Port		
Outside IP Address		
Outside Port		
Allow Related		
	Update	

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.

The table columns are customizable. Click **Customize Columns** at the right top corner of the table and select/deselect the options that you want to display or hide in the table.

1	Site F	Repo	rt : Real Time Flows											
	Ret	rieve la	atest data Search	Q										
	🗸 Uplo	oad 🗸] Download										Customi	Çe Columns
	Info	No	Application	Source IP Addr	Dest IP Addr	Source Port	Dest Port	Proto IP	Packets	PPS	Class	Service Name	Age (mS)	Bytes
	(i)	1	N/A	172.10.10.6	192.229.232.240	49976	80	TCP (6)	3	0.000	N/A	-	3702175	156
	(i)	2	N/A	172.10.10.6	192.229.232.240	49837	80	TCP (6)	3	0.000	N/A	-	7024077	156
	(i)	3	N/A	172.10.10.6	192.229.232.240	49835	80	TCP (6)	3	0.000	N/A	-	7050202	156
	(j)	4	N/A	172.10.10.6	192.229.232.240	49833	80	TCP (6)	3	0.000	N/A	-	7089890	156
	(i)	5	N/A	172.10.10.6	192.229.232.240	49970	80	TCP (6)	3	0.000	N/A	-	4655644	156
	(i)	6	N/A	172.10.10.6	192.229.232.240	49831	80	TCP (6)	3	0.000	N/A	-	7130125	156
	(i)	7	N/A	172.10.10.6	192.229.232.240	49825	80	TCP (6)	3	0.000	N/A	-	7168561	156
	()	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

Routing Protocols

The Routing Protocols report provides the details of the parameters associated with the routing protocols. In the **Routing Protocols** section, select the appropriate routing protocol, routing domain, and IP address type (IPv4 or IPv6) from the drop-down list. Click **Retrieve Latest Data** to view the current data.

You can view the parameter details associated with the following options:

- BGP State
- OSPF State
- OSPF Topology
- OSPF Interface
- OSPF LSADB
- OSPF Neighbors
- Route Table

Routing Protocols

Dynamic Routing Protocol	
View: Routing Domain: BGP State Control Default_RoutingDomain Control Default_Retrieve Latest Data	Pr4/IPr6: IPr6 IPr6
BGP State	

From Citrix SD-WAN 11.5 release, IPv4 and IPv6 filter is newly added. Upon selection on IPv6, user receives a new operation name for all the IPv6 data.

DHCP Server and Relay

The **DHCP Server/Relay** report provides the information on the interfaces configured as DHCP Server or Relay and its associated routing domain and status. You can search for the required DHCP server or relay information using the **Key: Value** format.

Retrieve Latest Data Restart Show Clients Clear Clients Click here to search or you can enter Key : Value format INTERFACE(S) Status + + Server DHCP MODE ROUTING DOMAIN INTERFACE(S) Status + Server Default_RoutingDomain VIF-1-Bridge-1 Running	Site R	Reports:Real T	ime DHCP Server/relay 🛛 🥄			Relative Time	\sim	Interval:	Last 1 Hour	\checkmark
Click here to search or June on enter Key : Value format INTERFACE(S) Status + DHCP MODE ROUTING DOMAIN VIF-1-Bridge-1 Running Server Default_RoutingDomain VIF-1-Bridge-1 Running	Retriev	ve Latest Data	Restart Show Clients C	Clear	r Clients					
DHCP MODE ROUTING DOMAIN INTERFACE(S) STATUS + Server Default_RoutingDomain VIF-1-Bridge-1 Running	Q Click	here to search or y	ou can enter Key : Value format							0 0 0
Server Default_RoutingDomain VIF-1-Bridge-1 Running	DH	ICP MODE	ROUTING DOMAIN		INTERFACE(S)			STATUS		+
	Se	erver	Default_RoutingDomain		VIF-1-Bridge-1			Running		
Showing 1-1 of 1 items Page 1 of 1 4 10 rows V					Showing 1-1 of 1 items	Page 1	of 1		10 rows	s ~

If the mode is **Server**, you can click **Show Clients** and view the list of DHCP clients associated with the DHCP server.

aiil	REPORTS ~	G		orver Client Data	basa			Interval:	
	Alerts	U			Dase				
	Usage	Re	etrieve Latest Data						
	Quality		Click have to coarch or y	ou con ontor Kov - Value	format		:		
	QoS	~	stick here to search or y	ou can enter key . valu	FIOTINAL		•	STATUS	
	Historical Statistics		ROUTING DOMAIN 🗘	CLIENT IP ADDRESS 🔅	LEASE START TIME	LEASE END TIME 🗘	CLIENT MAC ADDRE	Running	
	Real Time \sim		Default_RoutingDo	172.16.10.11	Sat Feb 27 10:47:06	Sat Feb 27 22:47:0	7a:ab:d9:81:ba:3b		
	Statistics							1 🔹 🕨	
	Flows			Showin	a 1-1 of 1 itoms Page		10 rows V		
	Firewall Connections			Showing	griffing rage		101003		
	DHCP Server/relay								
	VRRP						Close		
	PPPoE								
<									

Click **Clear Clients** to remove the DHCP clients that are currently associated with the DHCP server.

- 601		
	Q. Click here to search or you can enter Key : Value format	
	CLEAR DHCP CLIENTS	
	Ser Are you sure you want to clear selected DHCP Clients?	
	Yes No, Cancel Page 1 of 1 4 10 rows 🗸	
<		

Click **Restart** to restart the DHCP Server or Relay.

C DASHBOARD		
REPORTS V		
		= status = + Puening
Quality QoS	Are you sure you want to restart selected DHCP Server/Relay Daemon?	ranning
Historical Statistics Real Time V	Yes No, Cancel	Page 1 of 1

VRRP

The VRRP real-time report provides details about the configured VRRP groups. To view Virtual Router Redundancy Protocol (VRRP) report, navigate to **Reports > Real Time > VRRP**. Click **Retrieve Latest Data** to get the current data.

E citrix SD-WAN C	Orchestrator									٠	0	Abhishek Pi Orchestrator De OrgID: intf4b57	andey w US 🗸 1d7
ROOT PARENT Admin / SDWAN-Team /	PROVIDER CUSTO Abhishek / Seria	omer al_HA_Setup /	BR1_CB1000 V									Change Role	\$ 0
C DASHBOARD	Site Reports: Re	al Time VRRP	e							Relative Time	V Interval:	Last 1 Hour	~
af REPORTS V	Retrieve Latest Data	a Enable	Disable										
	Q. Click here to search	n or you can enter Key	: Value format										:
Alerts	VRRP ID	C VERSION) INTERFACE(S)	STATE	PRIORITY	÷V	IRTUAL ROUTER IP	ADVERTISEMENT IN 0	+				
Usage Quality	10	2	VIF-3-LAN-1	Master	100	17	72.16.16.200	1000					
QoS													
Historical Statistics									Showing 1-1 of	1 items Page 1	of 1 🔍	▶ 10 rov	/8 🗸
Real Time 🗸 🗸													
Statistics													
Flows													
Firewall Connections													
Routing Protocols													
DHCP Server & Relay													
IGMP													
VRRP													
PPPoE													

PPPoE

The PPPoE report provides status information of the configured virtual interface with the PPPoE static or dynamic client mode. It allows you to manually start or stop the sessions for troubleshooting purposes.

- Virtual interface: The virtual interface associated with PPPoE.
- **IP Address**: The IP address associated with the virtual interface. If the virtual interface is up and ready, display the recently received values. If the virtual interface is stopped or is in failed state, displays the last received values.
- **Gateway IP**: The IP address associated with the Gateway. If the virtual interface is up and ready, display the recently received values. If the virtual interface is stopped or is in failed state, displays the last received values.
- Session ID: The unique identifier associated with PPPoE session.
- **State**: The **State** column displays the status of the PPPoE session using three color codes; green, red, yellow. The following table describes the states and descriptions.

PPPoE session type	Status Color	Description
Configured	Yellow	A VNI is configured with PPPoE.
		This is an initial state.
Dialing	Yellow	After a VNI is configured, the
		PPPoE session state moves to
		dialing state by starting the
		PPPoE discovery. Packet
		information is captured.

PPPoE session type	Status Color	Description
Session	Yellow	VNI is moved from Discovery state to Session state, waiting to receive IP, if dynamic or waiting for acknowledgment from server for the advertised IP, if static.
Ready	Green	IP packets are received and VNI and associated WAN link is ready for use
Failed	Red	PPP/PPPoE session is terminated. The reason for the failure can be due to invalid configuration or fatal error. The session attempts to reconnect after 30 seconds.
Stopped	Yellow	PPP/PPPoE session is manually stopped.
Terminating	Yellow	An intermediate state terminating due to a reason. This state automatically starts after certain duration (5 seconds for normal error or 30 secs for a fatal error).
Disabled	Yellow	The SD-WAN service is disabled.

Site Reports: Real Time F	PPPoE 🙄		Relative Time	V Interval: Last	I Hour \lor
Retrieve Latest Data Sta	rt Stop				
\bigcirc Click here to search or you can e	enter Key : Value format				0 0 0
VIRTUAL INTERFACE		GATEWAY IP	SESSION ID	STATE	÷ +
VirtualInterface-2			0	Dialling	
VIF-2-LAN-1		10.00.00.0	3	Ready	
		Showing 1-2 of	2 items Page 1	of 1 🔹 🕨	10 rows 🗸

DNS statistics

The **DNS Statistics** provides the information on the application name, DNS service name, DNS service status, and the amount of hits to the DNS service. The information for DNS proxy and DNS transparent forwarder is displayed on two different tabs.

Proxy statistics				
Site Reports:Real Time DNS Sta	atistics 2		Relative Time V Interval:	Last 1 Hour \vee
Proxy Statistics Transparent Forwar	der Statistics			
Retrieve Latest Data				
\mathbb{Q} Click here to search or you can enter K	ey : Value format			0 0 0
PROXY NAME	APPLICATION NAME	DNS SERVICE NAME	DNS SERVICE ACTIVE	♦ HITS
> Citrix_DNS_Proxy	office365_optimize	Quad9	YES	0
> Citrix_DNS_Proxy	Any	Citrix_DNS	YES	0
Transparent forwarder statistic Site Reports:Real Time DNS Statisti	CS cs 😅	Showing 1-2 of 2 items	Page 1 of 1	10 rows ∨ Last 1 Hour ∨
Retrieve Latest Data				
Q Click here to search or you can enter Key : Va	lue format			0 0 0
APPLICATION NAME	DNS SERVICE NAME	DNS SERVICE ACTIVE	HITS	÷ +
aomain_name_based office365_optimize	Quad9	YES	0	
		Showing 1-2 of	2 items Page 1 of 1 ┥	▶ 10 rows ∨

IPsec

The IPsec real-time report provides details about the **IPsec tunnel** settings on your network.

To view details of IPsec Security Associations (IPsec SAs), navigate to **Reports > Real Time > IPsec > IPsec SAs**. Click **Retrieve latest data** to get the current data.

To view details of Internet Key Exchange Security Associations (IKE SAs), navigate to **Reports** > **Real Time** > **IPsec** > **IKE SAs**. Click **Retrieve latest data** to get the current data.

You can also purge the IPsec group data and statistical data by selecting **Purge IPsec Group** and **Purge IKE Stats** respectively.

ts / Real Time / IPsec							verity Configuration	
ec								
Psec SAs IKE SAs								
IPSec Tunnels:								
IPSEC_IPSEC V								
IPSEC_IPSEC 🗸								
IPSEC_IPSEC V	irge IPSec SAs	Purge IKE SAs						
IPSEC_IPSEC V Retrieve Latest Data	irge IPSec SAs	Purge IKE SAs						
IPSEC_IPSEC Retrieve Latest Data	irge IPSec SAs	Purge IKE SAs						
IPSEC_IPSEC ~ Retrieve Latest Data Q Click here to search or you can enter K	arge IPSec SAs	Purge IKE SAs						:
IPSEC_IPSEC P Retrieve Latest Data P Q. Click here to search or you can enter K Name © Service Type	erge IPSec SAs	Purge IKE SAs	¢ Dir	0 Host	Peer	 Source IP Start 	Source IP End	Dest IP S
IPSEC_IPSEC ~ Retrieve Latest Data Q. Click here to search or you can enter Ki Name © Service Type	urge IPSec SAs	Purge IKE SAs	¢ Dir	0 Host	Peer	 Source IP Start 	© Source IP End	¢ Dest IP S
IPSEC_IPSEC ~ Retrieve Latest Data Q Click here to search or you can enter Ki Name © Service Type >	ey : Value format	Purge IKE SAs	0 Dir	0 Host	© Peer	 Source IP Start 	Source IP End	Dest IP S
	arge IPSec SAs sy : Value format 0 Intranet Service Type 0	Purge IKE SAs	 Dir 	0 Hest	Peer	 Source IP Start 	Source IP End	2 Dest IP Si

Cloud Direct

The **Cloud Direct** report provides more granular details about the usage (bandwidth utilization, latency, and packet loss) for each of the participating WAN link and major historical events of the site.



			Reports / Cloud Direct	/ Events		Software Version : 11.4.0.123-GA
(()	DASHBOARD		Events			
ай !	REPORTS	~	Evolito			
	Alarta .		Search	Q		
	Traps.		Date $\hat{\Rightarrow}$	Severity	Event	
	Sealing 1		Jul 26th 2021, 11:13 pm	Warning	Broadband-BELNET-1 downlink-loss :Level 4 for 3 hours 20 minutes	
	0.4		Jul 26th 2021, 11:02 pm	Warning	Broadband-ASAHI_Net-2 downlink-jitter :Level 2 for 0 hours 14 minutes	
	Real Tree		Jul 26th 2021, 10:32 pm	Resolved	Broadband-ASAHI_Net-2 uplink-alarm-level :alarm resolved	
	Cloud Direct		Jul 23rd 2021, 11:07 pm	Resolved	Broadband-BELNET-1 downlink-alarm-level :alarm resolved	
	Performance					
	SaaS Optimization					
	Events					

O365 Metrics

Citrix SD-WAN allows you to not only perform beacon probing, but also determines the latency to reach Office 365 endpoints through each WAN link. The latency is the round trip time taken to send a request and get a response from the Office 365 beacon service over a WAN link. This enables network administrators to view the beacon service latency report and manually choose the best internet link for direct Office 365 breakout. Beacon probing is enabled only through the Citrix SD-WAN Orchestrator service. By default, beacon probing is enabled on all Internet enabled WAN links when Office 365 break-out is enabled through the Citrix SD-WAN Orchestrator service.

Q	DASHBOARD	Relative Time 🗸 Intervet: Last 30 Min	ns 🗸
<u>.</u>	REPORTS ~	elect WAN Link: MCN, H#-Broadband Aintel1 v	
	Alerts	12:12pm 12:15pm 12:19pm 12:25pm 12:25pm 12:32pm 12:35pm 12:35pm 12:35pm	12:42pm
	Usage		
	Quality		
	QoS		
	Historical Statistics		
	Real Time >	tency (ms);	
	Cloud Direct	515	
	0365 Metrics	300	
	Appliance Reports	150 Value : 419 ms	
	WAN Link Metering		
		owestLatency/(ms);	
(6)	CONFIGURATION >	4617	
		300-	
5			
62	TROUBLESHOUTING >		

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
- LACP LAG Groups
- Network

- CPU Usage
- Disk Usage
- Memory Usage
- LTE Signal

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 Columns** at the 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			×	C
 Select All Bytes Received Packets Received Error Count Received 	 Bytes Sent Packets Sent Frror Count Set 	nt		
		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.

Site Report : Applia	Relative Time $ \smallsetminus $ 1	fenst: Last1Hour v					
Interfaces Network	CPU Usage Disk Usage	Memory Usage					
							Customiae Columns
Interface Name	Bytes Sent	Bytes Received	Packets Sent	Packets Received	Error Count Sent	Error Count Received	Actions
Interface 1	37 Kbps	41 Kbips	3193	3427	0	0	•
Interface 3	0 Kbps	0 Kbps	0	0	0	0	—
Management Interface	8 Kbps	10 Kbps	273	321	0	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 Number of packets sent for the selected duration.
- Packets Received 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.

LACP LAG Groups

The **LACP LAG Groups** page shows the details of the interfaces that are configured with LAG and LACP.

Reports	S						Relative Time	✓ Interval:	Last1Hour 🗸
Interfaces	LACP LAG Grou	ups Network	CPU Usage	Disk Usage Memory Usage	LTE Signal				
									Customize Columns
Site Name	LAG Name	Interface Name	Selection	State	System Priority	Port Priority	Partner State	Partner System Priority	Partner Port Priority
BR2_110 (Primary)	LAG0	1/2	Selected	ACT AGG SYNC COL DIST	65535	65280	AGG SYNC COL DIST	128	128
BR2_110 (Primary)	LAG0	1/3	Selected	ACT AGG SYNC COL DIST	65535	65280	ACT AGG SYNC COL DIST	128	128

- Site name: Name of the site.
- LAG name: Name given for LAG.
- Interface name: The interface that is configured for LAG.
- Selection: The interface selection status.
- **State**: The following flags are displayed to communicate the LACP status between the site that you are using and its connected site:
 - ACT: Refers to active. Indicates that LACP is in active mode.
 - Inactive: Indicates that LACP is in inactive mode.
 - TIMEOUT: Refers to time out. Indicates that the device is requesting a fast (1 s) transmit interval with the site that it is connected with. When the TIMEOUT flag is not displayed, it indicates that a slow (30s) transmit interval is requested.
 - **AGG**: Refers to aggregation. Indicates that the port is configured for aggregation (typically always set).
 - **SYNC**: Refers to synchronization. When **SYNC** is displayed, it indicates that the device is ready to use this link in the bundle to carry traffic. When **SYNC** is not displayed, it indicates that the link is not usable or is in standby mode.
 - **COL**: Refers to collection. Indicates that the traffic received on this interface will be processed by the device.
 - **DIST**: Refers to distribution. Indicates that the device is using this link to transmit the traffic.
 - **EXP**: Refers to expired. Indicates that no LACPDUs are received by the device during the past 3 intervals. When **EXP** is not displayed, it indicates that at least one LACPDU has been received within the past three intervals.
 - **DEF**: Refers to default. Indicates that no LACPDUs are received during the past 6 intervals. When **DEF** is not displayed, it indicates that at least one LACPDU is received within the past

6 intervals. Once the default flag is displayed, any stored information of the connected site is removed.

- System Priority: The priority of the LACP system associated with the site.
- Port Priority: The priority of the interface configured for LAG.
- Partner State: The state of the site the LACP system is connected to.
- Partner System Priority: The priority of the LACP system associated with the connected site.
- Partner Port Priority: The priority of the interface configured for LAG on the connected site.

Network

The **Network** page shows the number of TCP connections for each configured site.

Site Report : Applian	Site Report : Appliance Reports								
Interfaces Network									
	D					Customize Columns			
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 Report :	Appliance Repor	Re	lative Time \vee Ir	nterval: Last 1 Day 🗸					
Interfaces N	etwork CPU Usage	Disk Usage Mem	lory Usage						
									Customize Columns
Site Name	System	Users	Nice	Idle	lo Wait	irq	Sof Irq	Steal	Actions
DC_MCN	9.34 %	21.47 %	21.47 %	€2.5 %	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 Report	: Appliance Report	c C					Relative Time 😒	interval: Last 1 Day 👳
Interfaces	Network CPU Usage	Disk Usage Memor	ry Usage					
								Customize Columns
Site Name	Disk Name	Read IOPS	Write IOPS	Latency	Read Throughput	Write Throughput	Disk Utilization	Actions
DC_MCN	loop0	0 IOS/sec	0 IOS/sec	0 ms	0 Kbps	0 Kbps	0 %	0-

- 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 Repo	Relative Time $$ in	ntervat: Last 1 Day 🗸						
Interfaces	Network CPU Usage	Disk Usage Me	mory 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.

LTE signal

The **LTE Signal** page shows the signal strength of internal and external LTE modems.

Signal strength is measured in decibels (dB) and the values are classified as follows:

- **Excellent**: >-65 dB
- Good: -65 dB to -75 dB
- Fair: -75 dB to -85 dB
- **Poor**: < -85 dB

NOTE

The **LTE Signal** page is available only for Citrix SD-WAN 110 and 210 appliances.

Site Reports:Appliance Repor	Relative Time $\ \!$	Interval: Last 1 Day 🗸		
Interfaces Network CPU Usage	Disk Usage Memory Usage LTE	Signal		
				Customize Columns
Site Name	Internal Modem Signal Strength	External Modem Signal Strengt	h Actions	
wifi210	-90 dB	0 dB	•	
Internal Modem Signal Strength (dB)		External Modem Signal Streng	th (dB)	
0 -58 -93 -128	om 12:52am 5:19am 11:32am	11:32am 3:59pm	8:26pm 12:5	2am 5:19am 11:32am

- Site Name: Displays the site name.
- Internal Modem Signal Strength: Displays the strength of the LTE signal on the internal modem.
- **External Modem Signal Strength**: Displays the strength of the LTE signal on the external modem.
- Actions: You can switch on the action button to view the network graph.

WAN Link Metering

WAN link metering reports provide details about the metered WAN link usage. You can view the reports to get insights into the data consumption of the metered WAN links. To view WAN link metering reports, navigate to **Reports** > **WAN Link Metering**.

Reports: WAN Lir	nk Metering 💈		Relative Time 🗸 Interval: Last 1 Hour
WAN Link Name:	_New_H2-Broadband-ACT-1	WAN Link Name:	New_H2-LTE-AOL_Broadband-3
Total Usage:	0.97 MBs	Total Usage:	0 MBs
Data Usage:	0.04 MBs	Data Usage:	0 MBs
Control Usage:	0.92 MBs	Control Usage:	0 MBs
Usage (%):	NA	Usage (%):	NA
Billing Cycle:	Monthly	Billing Cycle:	Monthly
Starting From:	04/01/2021	Starting From:	04/01/2021
Days Elapsed:	6 days of 30 days	Days Elapsed:	6 days of 30 days
WAN Link Name:	_New_H2-LTE-Idea-2	WAN Link Name:	New_H2-Broadband-ACT-1
Total Usage:	0.21 MBs	Total Usage:	89.5 MBs
Data Usage:	0 MBs	Data Usage:	71.67 MBs
Control Usage:	0.21 MBs	Control Usage:	17.83 MBs
Usage (%):	NA	Usage (%):	NA
Billing Cycle:	Monthly	Billing Cycle:	Monthly
Starting From:	04/01/2021	Starting From:	04/01/2021
	0.1 (00.1	Dava Elasanda	C dava of 20 dava

Diagnostics

October 18, 2021

You can use Ping, Traceroute, Packet Capture, Bandwidth test, and iPerf diagnostic utilities to test and investigate network connectivity issues on your SD-WAN network. To view the Diagnostics page, navigate to **Troubleshooting** > **Diagnostics**.

To view the diagnostics results, click **View Results** on the top right corner of the Diagnostics page. You can **Download**, **Copy**, and **Clear** the report results as needed.

Diagnostics ③	
Ping Traceroute Packet Capture Bandwidth Test iPerf	

• **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**.

iagnostics (i)				Test Results		
Ping Traceroute	Packet Capture Ba	ndwidth Test 🗹 iPerf	View Results	C ************************************	lear Copy Do	wnlo
Source Site						
Source Site*				Client connecting to 10.1.2.3, UDP port 5001		
SantaClara			~	Binding to local address 10.1.2.2 Sending 1470 byte datagrams, IPG target: 11215.21 us (kalman adjust) UDP buffer size: 208 KByte (default)		
PING				[3] local 10.1.2.2 port 45212 connected with 10.1.2.3 port 5001 [ID] Interval Transfer Bandwidth [3] 0.0.1.0 sec 131 Nertes 1.0.7 Mbits/acc		
⁹ Address	Interface	Gateway IP (Option	al)	 [3] 1.0-2.0 sec [22] ENytes 1.05 Mbits/sec [3] 2.0-3.0 sec [22] KNytes 1.05 Mbits/sec [3] 3.0-4.0 sec [22] KNytes 1.05 Mbits/sec [3] 4.0-5.0 sec [22] KNytes 1.05 Mbits/sec 		
	Default	✓ Default	~	[3] 5.0- 6.0 sec 128 KBytes 1.05 Mbits/sec [3] 6.0- 7.0 sec 129 KBytes 1.06 Mbits/sec		
outing Domain	Ping Count	Packet Size (bytes)		[3] 7.0-8.0 sec 128 KDytes 1.05 Mbits/sec [3] 8.0-9.0 sec 128 KDytes 1.05 Kbits/sec [3] 9.0-1.0.0 sec 128 KDytes 1.05 Kbits/sec		
Default_RoutingDomain $ \smallsetminus $	5	70		[3] 10.0-11.0 sec 128 KBytes 1.05 Mbits/sec [3] 11.0-12.0 sec 128 KBytes 1.05 Mbits/sec [3] 12.0-13.0 sec 129 KBytes 1.06 Mbits/sec		

• **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**.

Diagnostics ()	Test Results	<
Executing diagnostic command on appliance, this may take some time, please wait		
Ping 🗹 Traceroute 📄 Packet Capture 📄 Bandwidth Test 📄 iPerf	Citear Copy Download	
Source Site	**************************************	
Source Site *	¹ Trace Route initiated on Virtual Path SantaClara-Kansas, Path SantaClara-Internet-ATT-2->Kansas-Internet-ATT- 2.	
SantaClara V	Please wait while the trace is completed. - Trace Route Results:	
Traceroute	Vitual Path: SantaClara-Kansas Path: SantaClara-Internet-ATT-2->Kansas-Internet-ATT-2	
Destination Site Path	Trace Houte to 10.1.2.3, destination was reached after 1 nops, 1 nops attempted.	
Kansas V SantaClara-Internet-ATT-2->Kansas-Internet-ATT-2 V	hops rtt 1 rtt 2 rtt 3 mean rtt - 1 10.1.2.3 2.438ms 2.344ms 2.291ms 2.358ms	
Cancel O Processing	Hops to destination: 1	

• **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.

Diagnostics ①	Test Results ×
A Executing diagnostic command on appliance, this may take some time, please wait	Clear Copy Download
Ping Traceroute Packet Capture Bandwidth Test iPerf	
Source Site	
Source Site *	
SantaClara	~
Packet Capture	
Interface Filter Help Duration (seconds)	Max no of packets to view
1 v 5 v	1000 ~
Cancel O Processing	

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**.

Diagnostics ⁽¹⁾	Test Results
Ping Traceroute Packet Capture Bandwidth Test iPerf	
Source Site	***********************Result of bandwidth**********************
Source Site *	Minimum Bandwidth:451829 kbps Maximum Bandwidth:668430 kbps
SantaClara	Average Bandwidth:539664 kbps
Bandwidth Test	
Destination Site	
Kansas 🗸	
Path	
SantaClara-Internet-ATT-2->Kansas-Internet-ATT-2	~
Pann SantaClara-Internet-ATT-2->Kansas-Internet-ATT-2 Cancel Run	

- **iPerf** –You can run an iPerf test on a specific path of a site. The iPerf diagnostic tool is used to generate test traffic which allows you to troubleshoot network issues that might result in:
 - Frequent change in path state from Good to Bad
 - Poor application performance
 - Higher packet loss

To run an iPerf diagnostic test, from the customer level, navigate to **Troubleshooting** > **Diagnostics** and select the **iPerf** check box. Enter the transport protocol, time interval, port number, server, bandwidth measurement mode, path to test, server iPerf options, and click **Run**.

				*********************Result of iperf*******************
iPerf				Server listening on UDP port 5001 Binding to local address 10.1.2.3
Transport Protocol	Time Interval (sec) *	Port*		Receiving 1470 byte datagrams UDP buffer size: 208 KByte (default)
UDP	~ 15	5001		[3] local 10.1.2.3 port 5001 connected with 10.1.2.2 port 45212 [JD] Interval Transfer Bandwidth Jitter Lost/Total Datagra
Server	Bandwidth M	easurement Mode	Hel	[3] 0.0-1.0 sec 129 KBytes 1.06 Mbits/sec 0.254 ms 0/ 90 (0%) [3] 1.0-2.0 sec 128 KBytes 1.05 Mbits/sec 0.440 ms 0/ 89 (0%)
Select Site	✓ All Over	rlay member paths	~	[3] 2.0-3.0 sec 128 KBytes 1.05 Mbits/sec 0.554 ms 0/ 89 (0%) [3] 3.0-4.0 sec 129 KBytes 1.06 Mbits/sec 0.204 ms 0/ 90 (0%) [3] 4.0-5.0 sec 128 KBytes 1.05 Mbits/sec 0.160 ms 0/ 89 (0%)
Path to test				[3] 5.0-6.0 sec 128 KBytes 1.05 Mbits/sec 0.401 ms 0/ 89 (0%) [3] 6.0-7.0 sec 128 KBytes 1.05 Mbits/sec 0.366 ms 0/ 89 (0%)
Choose Path			\sim	[3] 7.0-8.0 sec 128 KBytes 1.05 Mbits/sec 0.360 ms 0/ 89 (0%) [3] 8.0-9.0 sec 128 KBytes 1.05 Mbits/sec 0.357 ms 0/ 89 (0%) [3] 9.0-10.0 sec 128 KBytes 1.05 Mbits/sec 0.308 ms 0/ 89 (0%)
Server iPerf Options	Client iPerf O	ptions		[3] 10.0-11.0 sec 129 KBytes 1.06 Mbits/sec 0.252 ms 0/ 90 (0%) [3] 11.0-12.0 sec 128 KBytes 1.05 Mbits/sec 0.363 ms 0/ 89 (0%)
				 [3] 12.0-13.0 sec 128 KBytes 1.05 Mbits/sec 0.328 ms 0/ 89 (0%) [3] 13.0-14.0 sec 128 KBytes 1.05 Mbits/sec 0.508 ms 0/ 89 (0%) [3] 14.0 15.0 ex 128 KBytes 1.05 Mbits/sec 0.508 ms 0/ 89 (0%) (3) 14.0 15.0 ex 1.05 Mbits/sec 0.36 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec 0.48 Mbits/sec
Cancel Run				[3] 44.04.35.0 BEC 1.60 RD1EB/BEC 0.304 BE 0/ 89 (0%) [3] 0.0-15.0 BEC 1.88 MBytes 1.03 Mbits/sec 0.304 mS 0/ 1338 (0%) [SUM] 0.0-15.0 BEC 2.00 MBytes 1.12 Mbits/sec 0.304 mS 0/ 1428 (0%)

User settings

May 5, 2022

Role-based access control (RBAC) regulates access to Citrix SD-WAN Orchestrator service 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 the Citrix SD-WAN Orchestrator service. Roles can be assigned at Provider and Customer level. Users can be assigned a role from the list of predefined roles or custom roles.

If a customer has Citrix Secure Internet Access subscription along with Citrix SD-WAN subscription, then the **Administration > User Setting** is common between Citrix Secure Internet Access and Citrix SD-WAN Orchestrator service. **Provider-Master-Admin-All** or **Customer-Master-Admin** role defined for Citrix SD-WAN can assign Citrix SD-WAN access level role (pre-defined or custom role) for other admin users. Similarly Customer-Master-Admin role defined for Citrix SIA level role (pre-defined or custom role) to other admin users.

Add users

New users can be added on Citrix Cloud. Navigate to **Identity and Access Management > Administration** tab and select **Citrix Identity** from the **Select an identity provider** drop-down list.

≡	citrix	<u>۽</u>	8	×
¢	Edit access for			
	Cancel Save			
	Full access Full access Gustom acces Gustom access Gustom access Gustom access Gustom access Gustom			
	General Management			
	Domains Library			
	Licensing Notifications			
	Resource Location Secure Client			
	Workspace Configuration			
	SD-WAN			
	Customer: Read Only Access			

While adding users at the provider level, you can set "Full access" or "Custom access". Users with "Full access" get **Provider-Master-Admin-All** role on Citrix SD-WAN Orchestrator service. If you choose "Custom access" you are prompted to select the access level again. Users with "Customer Admin: Full Access" get **Provider-Master-Admin-All** role. Users with "Customer: Read Only Access" get **Provider-Master-Admin-All** role on Citrix SD-WAN Orchestrator service.

While adding users at the customer level, you can set "Full access" or "Custom access". Users with "Full access" get Customer-Master-Admin role on Citrix SD-WAN Orchestrator service. If you choose "Custom access" you are prompted to select the access level again. Users with "Customer Admin: Full Access" get Customer-Master-Admin role. Users with "Customer: Read Only Access" get Customer-Master-ReadOnly-Admin role.

Provider roles

The following table lists the predefined provider roles.

Provider role

Description

Provider-Master-Admin-All

An administrator who can manage the provider and all of its customer information

Provider role	Description
Provider-Master-Admin-Tenant	An administrator who can manage the provider
	and a subset of its customer information
Provider-Master-ReadOnly-All	An administrator who can only view provider
	and customer information
Provider-Network-Admin	An administrator who can only view and edit the
	network related information
Provider-Security-Admin	An administrator who can only view and edit the
	security related information

The Provider-Master-Admin-All role can perform the following:

- Assign roles to users in Provider and Customer network
- Manage access to customers for all other admin roles
- Edit or delete assigned roles
- Create custom roles

Customer roles

The following table lists the predefined customer roles.

Customer 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
Customer-Network-Admin	A customer administrator who can only view and edit network related information
Customer-Security-Admin	A customer administrator who can only view and edit security related information

The **Customer-Master-Admin** role can perform the following:

- Assign customer roles
- Edit or delete assigned roles within the customer network
- Create custom roles

Customers can view the list of provider roles who have access to their network under **Administration** > **User Settings**. **Customer-Master-Admin** can assign a customer role to an existing provider role.

Once a customer role is assigned to an existing provider role, the customer role takes precedence and overrides the provider role.

Note

The **Customer Master-Admin** cannot delete or override **Provider-Master-Admin-All**, **Provider-Master-Admin-Tenant**, and **Provider-Master-ReadOnly** roles.

Support roles

For troubleshooting purposes, Providers and 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. The default validity period is for two weeks from the date the role is assigned. After the validity period expires, the support user loses access to Provider/Customer information. However, the support user details continue to appear under the **Administration > User Settings**. Based on the need, the Provider/Customer administrator can either delete or extend the validity of the support role.

You can assign support roles under **Administration > User Settings**.

Role	Description
Provider-Support-ReadWrite	A support team member who can view and edit
	the provider information
Provider-Support-ReadOnly	A support team member who can only view the
	provider information
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

Change user roles

If a user is an administrator for more than one customer or provider, then the user is assigned with multiple roles. In such scenarios, the user can change the role and switch to the desired account for which the user is an administrator.

To change the role, click **Change Role** option at the top right portion of the screen. Select a role, and click **Confirm**.

chestrator			≜ 0
1.000	the v		Change Role
Network Dashboard 🔽	3	Relative Time \lor Interval:	ast 1 Hour \vee Site Group: All 🗸
C ³ ALERTS See All O Critical	① 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 V Select Co	ountry V Search Q	113 Total Sites 113
Map Satellite	Greenland	Finland	Clustering OFF

Role settings

May 4, 2022

Citrix SD-WAN Orchestrator service allows providers and customers to create custom roles and provide access to specific features. Custom roles help to set up role-based access to manage different aspects of their network.

Only the users with **Provider-Master-Admin-All** or **Customer-Master-Admin-All** role can create custom roles.

Users with the **Provider-Master-Admin-All** role can create and assign custom roles at the customer level. The customer administrators can assign these custom roles created by the provide administrator to its users.

To create a custom role, navigate to **Administration > Role Settings** and click **New Custom Role**.

Provide a name and description for the custom role. If you are a provider administrator, then choose the scope of the custom role.

- **Provider**: The custom role can only be assigned to users at the provider level.
- **Customer**: The custom role is created at the provider level but can only be assigned to users at the customer level.

Choose the access associated with the features and categories.

- Full Access: Provides access to view and edit the configuration.
- **Read Only**: Provides access to view the configuration.
- **No Access**: Does not provide access to view or edit the configuration.

The following is an example where a custom role is created at the provider level:

← New Custom Role
Custom Role Name
test-custom-role-1
Description
test role created
Scope
Provider Customer

SD-WAN Permissions

Feature	Category	Full Access	Read Only	No Access
Advance Delivery Service	CONFIG			
Appliance	REPORT			
Appliance	CONFIG			$ \bullet $
Application Quality	REPORT			
Application Quality	CONFIG			
Apps	CONFIG			$ \bullet $
Apps	REPORT			$ \bullet $
Azure	CONFIG			
Base Network	CONFIG			
Base Network	REPORT			
Base Security	CONFIG			۲
Base Security	REPORT			
Cloud Direct	REPORT			
Cloud Direct	CONFIG			
Customer Admin	CONFIG			
Customer Admin	REPORT			
GRE	REPORT			
HDX	REPORT			
Licensing	CONFIG			۲
MSP Admin	CONFIG			۲
MSP Admin	REPORT			
QoS	CONFIG			$ \bullet $
QoS	REPORT			
Routing	CONFIG			\odot
Site	CONFIG			
MSP-Site	CONFIG			\odot
Troubleshooting	CONFIG			$ \bullet $
UTM	CONFIG			
UTM	REPORT			
WAN Opt	CONFIG			۲
Base Customer	CONFIG		۲	
Base Msp	CONFIG		۲	
GRE	CONFIG			
AWS	CONFIG			
Licensing	CONFIG			
User Settings	CONFIG			۲
Save Cancel				
The following is an example where a custom role is created at the customer level:

← New Custom Role	
Custom Role Name	
test-custom-role-2	
Description	
test role created at customer level	

SD-WAN Permissions

Feature	Category	Full Access	Read Only	No Access
Advance Delivery Service	CONFIG			\odot
Appliance	REPORT			۲
Appliance	CONFIG			۲
Application Quality	REPORT			۲
Application Quality	CONFIG			۲
Apps	CONFIG			۲
Apps	REPORT			۲
Azure	CONFIG			۲
Base Network	CONFIG			
Base Network	REPORT			
Base Security	CONFIG			
Base Security	REPORT			
Cloud Direct	REPORT			
Cloud Direct	CONFIG			۲
Customer Admin	CONFIG			
Customer Admin	REPORT			
GRE	REPORT			۲
HDX	REPORT			۲
Licensing	CONFIG			
QoS	CONFIG			
QoS	REPORT			۲
Routing	CONFIG			
Site	CONFIG			
Troubleshooting	CONFIG			۲
UTM	CONFIG			
UTM	REPORT			
WAN Opt	CONFIG			
Base Customer	CONFIG			
GRE	CONFIG			
AWS	CONFIG			
User Settings	CONFIG			۲
Save Cancel				

The features available at the provider, network, and site level are different. The following is the list of

Feature	Category	GUI Pages
Base Msp	CONFIG	Dashboard, Alerts, Usage, Inventory, Announcements
Site	CONFIG	Site Profile Templates, WAN Link Templates
Troubleshooting	CONFIG	Audit Logs, Device Logs
User Settings	CONFIG	User Settings, Role Settings
Licensing	CONFIG	Licensing, License Usage Insights

features, categories, and the corresponding GUI pages available at the provider level:

The following is the list of features, categories, and the corresponding GUI pages available at the customer level:

Feature	Category	GUI pages
Base Customer	CONFIG	Dashboard, Network Home
Base Network	CONFIG	Delivery Services Internet / Intranet / Virtual Paths, Bandwidth Allocation, Dynamic Virtual Paths, Network Location Service, Intermediate Nodes, Interlink Communication, Link Sensitive profile, DNS Servers,
Base Network	REPORT	Usage, WiFi, Quality, Historical Statistics, O365 Metrics, ADM
Base Security	CONFIG	IPSec Encryption profiles, Network Security, SSID Profiles, Radius Profiles, Firewall Zones, Firewall Defaults, Firewall Policies, Security Profiles, SSL Inspection, Intrusion Prevention, Virtual Path IPSec, Certificates, Hosted Firewall
Customer Admin	CONFIG	Alerts

Feature	Category	GUI pages
Customer Admin	REPORT	Inventory
UTM	REPORT	WebFiltering, AntiMalware, Intrusion Prevention, SSL Inspection
HDX	REPORT	HDX Sites, HDX Users, HDX Sessions
QoS	CONFIG	QoS Policies, QoS Profiles
QoS	REPORT	QoS
Appliance	REPORT	Realtime Statistics, Realtime Flows, Realtime Firewall Connections
Cloud Direct	REPORT	Cloud Direct
Application Quality	CONFIG	App Quality profiles, App Quality Config
Application Quality	REPORT	Application Quality
Advance Delivery Service	CONFIG	Zscaler / Secure Internet Access
Routing	CONFIG	Routing Policies, Routing Domains, Import Route Profiles, Export Route Profiles
Site	CONFIG	Regions, Custom Groups, IP Groups, Profiles & Templates
Apps	CONFIG	Custom Apps, App Groups, Application Settings
WAN opt	CONFIG	WAN Optimization features, WAN Optimization Tuning, WAN Optimization Apps, WAN Optimization App Groups, WAN Optimization Rules
Troubleshooting	CONFIG	Audit Logs, Device Logs, Diagnostics
User Settings	CONFIG	User Settings, Role Settings
Licensing	CONFIG	Licensing, License Usage Insights

The following is the list of features, categories, and the corresponding GUI pages available at the site

level:

Feature	Category	GUI pages
Site	CONFIG	Dashboard, Alerts, Advance Settings Delivery Services, Advance Settings DHCP, Advance Settings DNS Settings, Advance Settings NAT, Advance Settings Dynamic Routing, Advance Settings Multicast Groups, Advance Settings LAG, Advance Settings VRRP, Advance Settings WAN Optimization, Site Configuration, Advance Settings ARP, Advance Settings Prefix Delegation Group
Base Network	CONFIG	Advance Settings NDP, Advance Settings Fallback Configuration
Base Network	REPORT	Usage, Quality, Historical Statistics, O365 Metrics, WAN Link Metering
QoS	REPORT	QoS
Appliance	REPORT	Realtime Statistics, Realtime Flows, Realtime Firewall Connections, Realtime Routing Protocols, Realtime DHCP Server & Relay, Realtime IGMP, Realtime VRRP, Realtime PPPoE, Realtime DNS, Realtime IPSec, Appliance Reports
Cloud Direct	REPORT	Cloud Direct
Appliance	CONFIG	Appliance Settings, WAN Optimization Settings
Troubleshooting	CONFIG	Audit Logs, Device Logs, STS Bundles

Once the custom role is successfully created, you can assign the custom role while creating users. Se-

lect the newly created custom role from the **Role** drop-down list under **Administration > User Set-tings**.

IP access list

March 3, 2022

The IP access list page enables administrators to configure a list of enterprise-specific user source IP addresses, to allow IP address-based access to Citrix SD-WAN Orchestrator service. Configuring IP addresses on the **Network Administration: IP Access List** page enhances IP security as administrators can control the tenant access for users based on their IP address. This configuration is supported only for users with role-based access to a tenant.

Note

The IP addresses must be static public IPs to facilitate consistent access. Dynamic addresses cannot be configured on the **IP Access List** page.

To configure an IP address, at the customer level, navigate to **Administration** > **IP Access List**.

On the **Network Administration: IP Access List** page, click **Add**. You can configure up to 16 IP addresses.

To remove an IP address, navigate to the **Actions** column and click the delete icon.

The **User IP Addresses** section displays the IP addresses of users accessing the Citrix SD-WAN Orchestrator service tenant.

If an administrator configures an IP address of a user who is not a part of a tenant, then the user gets locked out of the tenant where the IP address is configured.

When an administrator attempts to remove their IP address from the Citrix SD-WAN Orchestrator service tenant, then they get locked out of the tenant.

ser IP Addresses:		
^D Address		
Eg: a.b.c.d	/32 Add	
otal Count: 0		
		Antion

Announcements

May 17, 2021

Providers can use the **Announcements** option to send out announcements or notifications to their customers.

You can create a provider announcement by navigating to **Administration > Announcements** and clicking the **+ New** option.

Provider Administration: Announcements

Customer Announcements				
+ New				
Created By	Subject	Content	Expires	Actions
admin	Maintenance activity on 16	Maintenance activity is sch	Never	Ø 💼
		Page Size: 50 V	Showing 1 - 1 of 1 items	Page1 of1

Provide a subject line and enter content in HTML or plain text format. You can also set the announcement expiration.

ity - 20 May 2021					
y is scheduled for 20 M	lay 2021 between 6	PM to 8 PM. The	e services will be u	ınavailable during	this window.
it	ty is scheduled for 20 M	ty is scheduled for 20 May 2021	ty is scheduled for 20 May 2021 between 6 PM to 8 PM. The	Ity is scheduled for 20 May 2021 between 6 PM to 8 PM. The services will be u	Ity -20 May 2021 ty is scheduled for 20 May 2021 between 6 PM to 8 PM. The services will be unavailable during

The saved announcements are displayed to all the customers.

Maintenance activ	rity is scheduled for 20 May message	2021 between 6 PM to 8	BPM. The services w	vill be unavailable du	uring this window.	Click here
Network Dashboard	Ĉ	Relative	Fime 🗸 Interval:	Last 1 Hour \smallsetminus	Site Group: All	~
ALERTS See All See All Critical	Overlay Under 100.0% 100.0%	See Details rlay 0 KB	PAPPS wn	See All © To onpr 0.04 %	DP SITES e BRAN 6 0.03 %	<u>See All</u> branc 0.02 %
+ New Site Map	List Select Contine	ent Select Country N	Search Q		Tot	3 al Sites Normal
Availability Orchestrator Connectivity	Site Name	Site Role	Device Model	Serial No		Bandwidth Tier
 Online 	onpremmcn	MCN	VPX-SE	AF19B86B-15B0-5	7F2-51F8-8ECF1	20
 Online 	BRANCH2	Branch	VPX-SE	2A302151-72A2-87	7C8-B794-2D53	20
Online	branchvpx (HA)	Branch	VPX-SE	83E78799-4F85-A	.D41-7977-74F15	20
		Pa	ge Size: 50 V	Showing 1 - 3 of 3	items Page1 o	f1 🔹 🕨

API guide for Citrix SD-WAN Orchestrator

January 22, 2021

To access the Citrix SD-WAN Orchestrator service API Guide on the Swagger UI, you need to authenticate yourself using an API key.

The following procedure provides instructions on generating an API key and using it for authentication.

 Log into your Citrix Cloud account and navigate to Identity and Access management > API Access.

Note

If you are a partner running APIs on behalf of your customer, log into the customer's Citrix Cloud account using the **Change Customer** option or obtain the authentication and relevant API parameters from the customer.

			_
Home			
My Se	rvices	~	
Library	/		
Licens	ing		
Identit	ty and Access Management		
Resou	rce Locations	_	
Suppo	rt Tickets		
Notific	cations		

Identity and Access Management

Authentication	Administrators	API Access	Domains	Recovery
Secure Clients	Product Regis	strations		
			Secur	e Clients are used to interact with Citrix Cloud APIs.
Το ι	ise this secure cl	ient in a siler	nt connecto	or install or to access any of our APIs, use the customer ID js5w46v62b3u as the customer
				parameter.
			secureclie	nt1 Create Client

2. Provide a name for your secure client and click **Create Client**. An ID and secret key is generated. Use the ID and secret to authenticate yourself when using APIs to manage your network.

Note

Download the ID and the Secret and store it securely. You cannot access the secret after closing the window.



ID and Secret have been created successfully

Download the ID and secret to store in a safe place. You cannot access the secret after you exit this modal.



Note

For security reasons, it is advised to delete the API Key entries from Citrix Cloud when you are done using the APIs.

Х

dentity and Access	Management
--------------------	------------

ients Pro	duct Registrations			
Secure Clients are used to interact with Citrix Cloud APIs. To use this secure client in a silent connector install or to access any of our APIs, use the customer ID as the customer parameter. Name your Secure Client Create Client				
Name↓		ID	Creation Date	Actions
demo_clie	nt		3:28:27 PM Feb 14, 2020	â

3. Log in to the Citrix SD-WAN Orchestrator service and click **?** at the top-right corner of the UI and then click **API Guide**.



The Swagger spec details are displayed.

Swagger Spec Details
Citrix Cloud ID : zht5ata3zz3e
Network ID: 3a91afcf-c6db-4445-b334-6a8e25bdc5f7
Swagger Spec URL : https://sdwan-policy.citrixnetworkapi.net/swagger-ui.html

- 4. Click the Swagger spec URL to access the API guide.
- 5. In the API page, navigate to **auth-controller** > /{**ccId**}/**api/v1/logon** > **Try it out**.

Done

POST /{ccId}/api/vl/logon logon		â
Parameters	Try it o	ut
Name	Description	
ccld • required string (path)	Citrix Cloud user ID	
payload * required (body)	payload	
	<pre>cxampe value _mode { "ccld": "string", "clientGd": "string", "clientSecret": "string" }</pre>	
	Parameter content type application/json	

- 6. From the Citrix SD-WAN Orchestrator service **Swagger Spec Details**, copy the **Citrix Cloud ID** and paste it in the textbox under **Citrix Cloud user ID**.
- 7. Similarly, copy and paste the Client ID, Client secret and Citrix Cloud ID in the respective payload fields and click **Execute**.

POST /{ccId}/api/v1/logon logon		â
Parameters		Cancel
Name	Description	
ccld * required string (path)	Citrix Cloud user ID	
payload * required (body)	payload Example Value Model	
	{ "clientd": ", ", ", ", "clientsecret": ", =" ", }	
		C
	Cancel Parameter contant type application/json	

8. Copy the **token** value from the **Server response**.

Server res	ponse
Code	Details
200	Response body { "princ(pal*; " ", "clockarts ", ", "clockarts ", "clockarts ", "clockarts ", "

9. Click **Authorize** on the top of the API page and paste the **token** value in the **Value** field. Click **Authorize**.

(+) swagger	Select a spec	default	~
SD-WAN Orchestrator API Guide [Base UFL: sdram-policy.ctrf:metworkapi.net/] https://sdram.policy.ctrf:metworkapi.net//jail.docs This is an API guide to manage your network through the SD-WAN Orchestrator Citrix Systems			
			Authorize
Available authorizations		:	×
apiKey (apiKey) Name: Authorization In: header Value:			
Done Authorize			

This completes the authorization process and you must now be able to access and use Citrix SD-WAN Orchestrator service APIs.

Best practices

November 16, 2021

The following topics provide the best practices to be followed when the Citrix SD-WAN solution is being designed, planned, and executed on your network.

- Routing
- QoS
- WAN links

Routing

November 15, 2021

This article outlines routing best practices for the Citrix SD-WAN solution.

Internet/Intranet routing service

When the Internet service is not configured to Internet bound traffic and instead, either a **Local** route or a **Passthrough** route is configured to reach the gateway router. The router uses the WAN links configured on the SD-WAN appliance, leading to a link over-subscription issue.

If an Internet route is configured as **Local** at the MCN, it is learned by all the branch SD-WAN sites and configured as **Virtual Path Route** by default. This implies that Internet bound traffic at the branch appliance is routed through the Virtual Path to MCN.

Routing precedence

The order of routing precedence:

- Prefix Match: Longest prefixes match.
- Service: Local, Virtual Path service, Internet, Intranet, Passthrough
- Route Cost

Routing asymmetry

Ensure that there is no routing asymmetry on the network (SD-WAN appliance is transmitting traffic in only one direction). This creates issues with Firewall connection tracking and deep packet inspection.

QoS

November 17, 2021

Consider the following practices when configuring QoS:

• Understand your network traffic patterns and requirement. You might have to observe the **QoS** class statistics, and change queue depths, and/or change the default QoS class share percentage to avoid tail-drops as shown in QoS statistics.

• Sometimes, the entire subnet is added to a Rule for ease of configuration instead of creating Rules for particular application IP addresses. Adding an entire subnet to a rule incorrectly maps all the traffic in the subnet to one Rule. So, the QoS classes associated with that Rule might lead to tail drop and poor application performance or user experience.

WAN Links

November 15, 2021

Citrix SD-WAN platforms support upto 8 public internet connections and 32 Private MPLS connections. This article outlines WAN link configuration best practices for the Citrix SD-WAN solution.

Points to remember while configuring WAN links:

- Configure the **Permitted and Physical** rate as the actual WAN link bandwidth. In cases where the entire WAN link capacity is not supposed to be used by the SD-WAN appliance, change the **Permitted** rate accordingly.
- 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.
- If the underlying link is not stable and does not guarantee fixed bandwidth (for example; 4G links), use the **Adaptive Bandwidth Detection** feature.
- It is not recommended to enable **Auto Learn** and **Adaptive Bandwidth Detection** on the same WAN link.
- Manually configure the MCN/RCN with the Ingress/Egress physical rate for all the WAN links since it is the central point of bandwidth distribution among multiple branches.
- For increased reliability of important data center workloads/services, when auto-learn is not used, use reliable links with SLAs that does not have random variation of capacity.
- If the underlying link is not stable, change the following Path settings:
 - Loss Settings
 - Disable Instability Sensitive
 - Silence time
- Use **Diagnostic tool** to check the link health/capacity.
- If SD-WAN is deployed in **one-arm** mode, ensure that you do not overrun the physical capacity of the underlying link.

Verifying ISP link Health

For new deployments, earlier than SD-WAN deployment and when adding new ISP link to the existing SD-WAN deployment:

- Verify the link type. For example; MPLS, ADSL, 4G.
- Network characteristics. For example bandwidth, loss, latency, and jitter.

This information helps in configuring the SD-WAN network as per your requirements.

Network topology

It is commonly observed that specific network traffic bypasses the Citrix SD-WAN appliances, and uses the same underlying link configured in the SD-WAN network. Because SD-WAN does not have complete visibility over link utilization, there are chances that SD-WAN oversubscribes the link leading to performance and PATH issues.

Provisioning

Points to consider while provisioning SD-WAN:

- By default, all branches and WAN services (Virtual Path/Internet/Intranet) receive an equal share of the bandwidth.
- Provisioning sites must be changed, when there is high disparity in terms of bandwidth requirement or availability between the connecting sites.
- When dynamic virtual paths are enabled between maximum available sites, the WAN link capacity is shared between the static virtual path to DC and the dynamic virtual paths.

FAQs

June 13, 2022

HA near-hitless software upgrade

- 1. What is the difference between High Availability and Secondary (Geo) appliance?
 - High Availability ensures fault tolerance. Secondary (Geo) appliance enables disaster recovery.

- High Availability can be configured for the MCN, RCN, and branch appliances. Secondary (Geo) appliance can be configured for MCN and RCNs only.
- High Availability appliances are configured within the same site or geographical location. A branch appliance in a different geographical location is configured as Secondary (Geo) MCN/ RCN appliance.
- High Availability primary and secondary appliance should be the same platform models. The Secondary (Geo) appliance might or might not be the same platform model as the primary MCN/RCN.
- High Availability has higher priority over secondary (Geo). If an appliance (MCN/RCN) is configured with High Availability and Secondary (Geo) appliance, when the appliance fails the secondary high availability appliance becomes active. If both the high availability appliances fail or if the Data Center site crashes, the secondary (Geo) appliance becomes active.
- In High Availability, the primary/secondary switchover happens instantaneously or within 10-12 seconds depending upon the high availability deployment. The primary MCN/RCN to secondary (Geo) MCN/RCN switch over, happens after 15 seconds of the primary being inactive.
- High Availability configuration allows you to configure primary reclaim. You cannot configure primary reclaim for Secondary (Geo) appliance, the primary reclaim happens automatically after the primary appliance is back and the hold timer expires.
- 2. What are the prerequisites for the HA near-hitless software upgrade?

The existing customer network must already be running on Citrix SD-WAN 11.1 or higher release which supports the near-hitless upgrade procedure for HA.

3. Is this functionality enabled by default or is there some setting to enable this?

It is enabled by default.

4. What if there are a few sites with Non-HA deployment?

The sites with non-HA deployment are activated at the second step of activation. If the entire network does not have HA deployment then the single step upgrade is activated.

5. What if the activation fails either on the Standby or Active appliance?

The software has a timeout implementation. If the activation on the Standby appliance fails, after the timeout period, activation on the Active appliances is initiated.

6. What is the duration of the timeout period?

The timeout periods for the following upgrade activations are:

- Configuration update activation: 5 minutes
- Near hitless software upgrade for HA Step 1: 20 minutes

- Near hitless software upgrade for HA Step 2: 20 minutes
- Single step software upgrade activation: 20 minutes
- 7. What if Active and Standby are in different software versions because of error/issues during upgrade?

The HA pair continues to work in different software versions. Another Change Management Activation is required to bring the HA pair to the same software version.

8. What if the standby appliance is down when we initiate software upgrade?

Citrix SD-WAN Orchestrator service cannot complete the first step of near hitless upgrade activation process, which is upgrading the standby appliances and switching the standby appliances to active. It waits for the timeout period to get over and then transitions to the second step. As part of the second step, Citrix SD-WAN Orchestrator service upgrades the active appliances. The standby appliances get upgraded once they come back online.

9. Can we time schedule software Upgrade/Activation?

This functionality is not available currently.

10. Does this process apply to RCN based deployments?

Yes.

11. Do we support partial site upgrade?

Yes. Citrix SD-WAN Orchestrator service supports partial site upgrade from Citrix SD-WAN release 11.2.2 onwards. Even for the partial software upgrade scenarios, HA hitless upgrade is effective.

12. Do we support revert-on error functionality?

This functionality is not available currently.

13. How are non-SD-WAN components such as LTE Firmware, SVM, and Citrix Hypervisor Hotfixes upgraded? Can we have scheduled installation of these non-SD-WAN components?

This functionality is not available currently.

14. What if there is any configuration change during the software upgrade? Are we going to inform the user/admin that we are not going to apply the HA near-hitless software upgrade?

Yes. User/Admin is informed that there is a configuration change during current software upgrade activity. The user is given a choice to continue with the normal single step software upgrade procedure, instead of near-hitless upgrade.

2100 Premium (Enterprise) Edition

What does the following message indicate when a 2100 EE appliance is upgraded to release 10.0?

EE provisioning error: WO redirection is enabled but WO is not provisioned. Please use single step upgrade to upgrade your network.
Clear Warning

Appliance has EE license or WANOP redirection is enabled from MCN. You can schedule installation of WANOP components to start provisioning WANOP features on this platform.

Related information

- Zero touch deployment over LTE
- Configure the secondary MCN in HA

net>scaler

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.

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