net>scaler

Citrix SD-WAN Center 11.4

Contents

System requirements and installation	4
Install and configure Citrix SD-WAN Center on ESXi Server	8
Install and configure Citrix SD-WAN Center on XenServer	20
Install and configure Citrix SD-WAN Center on Microsoft Hyper-V	27
Citrix SD-WAN Center on Azure Marketplace using solution template	35
Citrix SD-WAN Center on AWS in VM importable image format	41
Two factor authentication	47
Primary authentication	48
Secondary authentication	52
Single-region network deployment	56
Multi-region network deployment	58
Configuration	63
Configure the management interface settings	63
Install the SD-WAN Center SSL certificate	64
Install the Citrix SD-WAN SSL certificate	65
Switch the active storage to new data storage	67
Deploy Citrix SD-WAN appliance	68
Configure Citrix SD-WAN appliances	68
Configuration Editor	69
Change Management Wizard	71
Appliance settings	73
Remote LTE site management	75
Citrix SD-WAN Center as a license server	80

Deploy Citrix SD-WAN on Azure from Citrix SD-WAN Center	83
Zero Touch Deployment	91
On-prem zero touch	113
AWS	113
Azure	124
Proxy Server Settings for zero touch deployment	143
Palo Alto Network Integration	145
Microsoft Azure Virtual WAN	151
Using Citrix SD-WAN to connect to Microsoft Azure Virtual WAN	163
Cloud Direct Service	195
Integrate Citrix SD-WAN and Zscaler using Citrix SD-WAN Center	218
Monitoring	230
Dashboard	230
Diagnostic packages	256
Events	258
Event notifications	261
Memory dumps	266
Log files	268
Polling interval	269
Statistics	269
System information	273
Reporting	274
Application report	277
Application QoE report	278

Bandwidth report	280
Class report	281
Ethernet interface report	283
Event report	284
GRE tunnel report	287
HDX report	288
IPsec tunnel report	292
Link performance report	294
MOS for applications	297
MPLS queues report	299
Administration	300
Configure date and time	301
HTTPS certificates	302
Import MCN configuration	305
Manage database	308
Manage views	311
Software upgrade	312
Timeline controls	313
User accounts	315
Diagnostics	320

System requirements and installation

November 8, 2021

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

Note

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

Hardware requirements

Citrix SD-WAN Center has the following hardware requirements.

Processor

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

Memory

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

Disk space requirements

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

Estimated disk space requirement

Citrix SD-WAN Center 11.4

# Client Sites	Average # WAN Links per Site	Average # In- tranet/Internet Services per Site	Average # Virtual Paths per Site	Database Size (TB) for 1 Year
32	2	2	2	1.2T
32	4	4	4	1.8T
32	8	8	8	5.3T
54	2	2	2	1.5T
4	4	4	4	2.6T
4	8	8	8	9.6T
6	2	2	2	1.8T
6	4	4	4	3.3T
6	8	8	8	14.0T
28	2	2	2	2.0T
28	4	4	4	4.1T
28	8	8	8	18.0T
92	2	2	2	2.6T
92	4	4	4	5.6T
92	8	8	8	27.0T
56	2	2	2	3.0T
56	4	4	4	7.2T
56	8	8	8	35.0T
50	2	2	2	15.9T
50	4	4	4	41.9T
50	8	8	8	195.6T

Network bandwidth

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

Estimated network bandwidth requirements

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

Software

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

Hypervisor

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

Cloud Platform

- Microsoft Azure
- Amazon Web Services

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

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

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

Prerequisites

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

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

Note

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

Download Citrix SD-WAN Center software

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

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

ctx-sdwc-version_number-platform.extension

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

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

Gather the Citrix SD-WAN Center installation and configuration information

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

Gather or determine the following information:

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

Install and configure Citrix SD-WAN Center on ESXi Server

March 12, 2021

Install the VMware VSphere client

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

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

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

The VMware ESXi Welcome page appears.

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

Run the vSphere Client installer file that you downloaded, and accept each of the default options when prompted.

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

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

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

The vSphere Client main page appears.

<i>[]</i> 10.199.81.141	- vSphere Client						
	Inventory Administ	ration Plug-i	ns Help				
	🔄 Home						
Inventory							
쥄							
Inventory							
Administration							
8							
Roles	System Logs						
Recent Tasks				Name, Ta	rget or Status contains		Clear
Name	Target	Status	Details	Initiated by	Requested Start	Start Time	Complete
•			111				•
Tasks							root

Creating the Citrix SD-WAN Center VM using OVF template

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

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

For more information, see System requirements and installation.

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

The **Deploy OVF Template** wizard appears.

Deploy OVF Template	
Source Select the source loca	ation.
Source OVF Template Details Name and Location Storage Disk Format Ready to Complete	Deploy from a file or URL
	Browse. Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
Help	< Back Next > Cancel

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

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

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

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

8. Click Next.

The Storage page appears.

e Template Details	Select a destination st		and a second second						
Jser License Agreer	Name	Drive Type	Capacity P			Туре	Thin Provision.		Hardware Accelerat
and Location	acs_datastore1		931.00 GB 8		59.79 G		Supported	Single host Single host	
ormat ork Mapping	datastore1 datastore2	Non-SSD Non-SSD	460.75 GB 2 465.50 GB 2		252.26	VMFS5 VMFS5	Supported Supported	Single host	
	Disable Storage I Select a datastore:)RS for this virt	tual machine						
	Name	>rive Ty Cap	pacity Provision	ned Free	Туре	Thin Pro	ovisioning Acces	5	

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

Deploy OVF Template					_ 🗆 🗙
Disk Format In which format do	you want to store the v	irtual disks?			
Source OVF Template Details End User License Aareer Name and Location Storage Disk Format Network Mapping Ready to Complete	Datastore: Available space (GB): Thick Provision Lazy Thick Provision Eage Thin Provision				
Help			< Back	Next >	Cancel

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

Note:

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

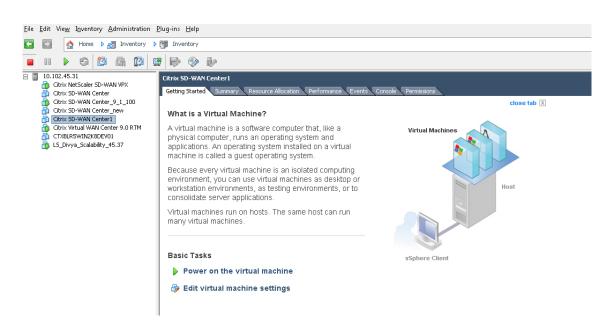
13. Click Close.

View and record the management IP address on ESXi server

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

To display the management IP address, do the following:

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



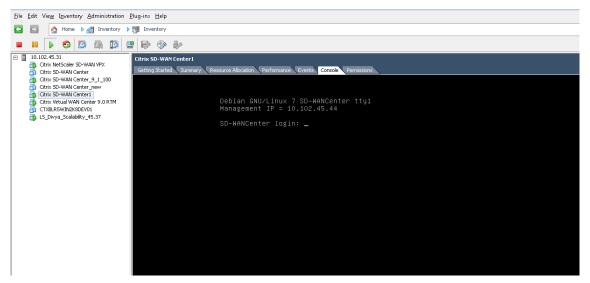
- 2. On the Citrix SD-WAN Center page, under Basic Tasks, click Power on the Virtual Machine.
- 3. Select the **Console** tab, and then click anywhere inside the console area to enter console mode.

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

Note

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

4. Press Enter to display the console login prompt.

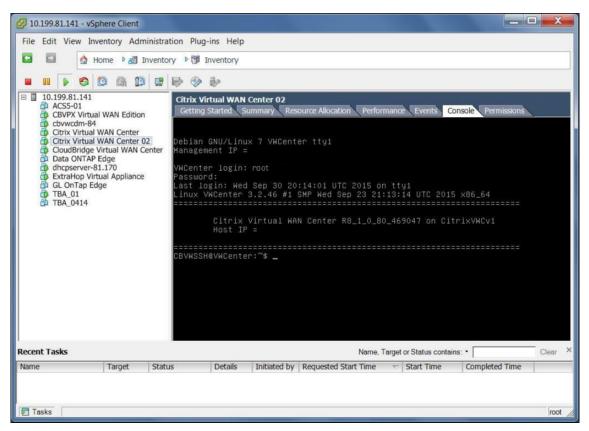


5. Log into the VM console.

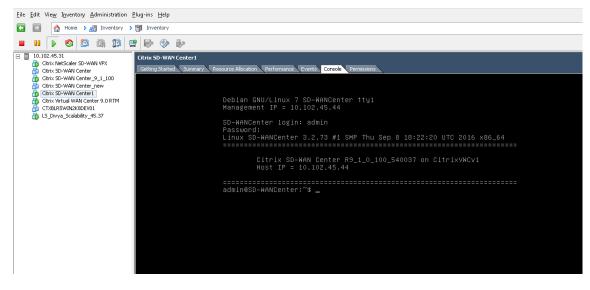
The default login credentials for the new Citrix SD-WAN Center VM are as follows:

• Login: admin

• Password: password



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



Note

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

completed.

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

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

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

Login: admin

Password: password

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

Add and Configure the Datastore on an ESXi server

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

To add and configure the datastore:

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

ardware Options Resou	rces			Virtual Machine Version: vmx	-09
Show All Devices	Add	Remove	Memory Contigura	ation	
Show All Devices	Add Summary 4096 MB 4 Video card Restricted LSI Logic SAS Virtual Disk Client Device VM Network	Remove	1011 GB 4 512 GB - 256 GB - 128 GB - 64 GB 4 32 GB - 16 GB - 8 GB - 4 GB - 2 GB - 1 GB 4 512 MB - 256 MB 4 128 MB - 64 MB - 32 MB -	Memory Size: Maximum recommended for this guest OS: 1011 GB. Maximum recommended for best performance: 65504 MB. Default recommended for this guest OS: 1 GB. Minimum recommended for this guest OS: 256 MB.	4
			16 MB - 8 MB - 4 MB -		
Help				1	1

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

For more information, see Memory Requirements.

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

🔗 Add Hardware	and the second second	X
Select a Disk		
Device Type Select a Disk Create a Disk Advanced Options Ready to Complete	A virtual disk is composed of one or more files on the host file system. Together these files appear as a sin to the guest operating system. Select the type of disk to use. Disk Create a new virtual disk C Use an existing virtual disk Reuse a previously configured virtual disk. Raw Device Mappings Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a	igle hard disk
Help	< Back Next >	Cancel

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

Add Hardware	And and a second se	-	-		×
Create a Disk Specify the virtua	al disk size and provisioning policy				
Device Type Select a Disk Create a Disk Advanced Options Ready to Complete	Capacity Disk 16 → GB ▼ Disk Provisioning	Browse			
Help		[< Back	Next >	Cancel

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

disk.

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

Name	Drive Ty	Capacity	Provisio	Free	Туре	Thin Provision.	
 acs_datasto datastore2 datastore1 	Non-SSD Non-SSD Non-SSD	465.50 GB	884.11 290.76 212.72	179.72	VMFS5	Supported Supported Supported	
elect a datastore:							
Disable Storage		s virtual mach		Free	Туре	Thin Provisioning	
elect a datastore:				Free	Туре	Thin Provisioning	

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

Add Hardware	-	-	and a second	-	1	×					
Ready to Complete Review the select		sh to add the hardware.									
Device Type Select a Disk	Options:	Options:									
Select a Dek Greate a Dek Advanced Octors Ready to Complete	Hardware type: Create disk: Disk capacity: Disk provisioning: Datastore: Virtual Device Node: Disk mode:	Hard Disk New virtual disk 16 G8 Thick Provision Lazy Zeroed acs_datastore1 SCSI (0:1) Persistent									
Нер	1		1	< Back	Firish	Cancel					

17. Click Finish.

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

18. Click **OK**.

	1		Virtual Machine Version: vm:
Show All Devices	Add	Remove	Disk File [acs_datastore1]
Show All Devices Hardware Memory CPUs Video card VMCI device SCSI controller 0 Hard disk 1 CD/DVD drive 1 Network adapter 1 New Hard Disk (add	Add Summary 4096 MB 4 Video card Restricted LSI Logic SAS Virtual Disk Client Device VM Network Virtual Disk	Remove	

Install and configure Citrix SD-WAN Center on XenServer

March 12, 2021

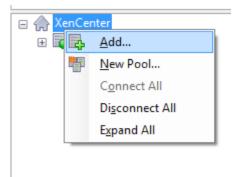
Before installing the Citrix SD-WAN Center virtual machine on a XenServer server, gather the necessary information as described in Gathering the Citrix SD-WAN Center Installation and Configuration Information.

Install the XenServer server

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

To install a XenServer server:

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



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

🔀 Add New Si	🗙 Add New Server						
	t name or IP address of the server you wa r login credentials for that server.	nt to add					
<u>S</u> erver:	10.102.29.2		~				
User login c	redentials						
<u>U</u> ser name:	root						
Password:	•••••						
	Add	Can	cel				

4. Click Add.

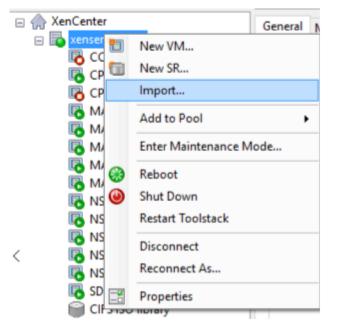
The new server's IP address appears in the left pane.

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

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

To create the Citrix SD-WAN Center VM:

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



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

Import		- 🗆 X
Socate the file y	ou want to import	3
Import Source	Enter the pathname of an exported VM or template, an OVF/OV	A package or a virtual hard disk image file or
Location	click Browse to find the file you want.	
Storage	Filename:	Browse
Networking		Drowschi
Finish		
citrix.		< Previous Next > Cancel

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

🔕 Import XVA	-
Select the location w	here the imported VM will be placed 🕜
Import Source	Click on a server to nominate it as the home server for the imported VM or for any new VMs to be based on the imported template. The home server will be used by default to start up the VM and to provide resources
Home Server	such as local storage.
Storage	Click on a pool if you do not want to nominate a home server: the most suitable available server will be
Networking	used.
	xenserver-29.2
CITRIX	Add New Server
	< Previous Next > Cancel

4. Select a storage repository where the virtual disk for the new VM will be stored, and click **Import.** For now, you can accept the default storage resource. Or you can configure the datastore. For

more information see Ad	d and configure	the Datastore on	XenServer section.
-------------------------	-----------------	------------------	--------------------

😣 Import XVA	-		×
Select target storage			?
Import Source	Select a storage repository where virtual disks for the new VM will be stored		
Home Server	Cocal storage on xenserver-29.2 758.09 GB free of 909.01 GB		
Storage			
Networking			
Finish			
citrix.			
	< Previous Import >	Can	cel

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

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

😣 Import XVA						-		Х
Select network to com	nect VM							?
Import Source Home Server Storage Networking	modify or dele When you have	te virtual e finished	ork interfaces for the t network interfaces, if r , click "Next" to contir 25 installed on the new	uue to the next page.	l are listed below.	You ca	n add,	
Finish	Name		MAC Address	Network				
	interface 0		62:c9:d5:e6:f9:3b	Network 0				•
CITRIX					Add		Delete	
				< Pr	evious Next	>	Can	cel

6. Click Finish.

View and record the management IP address on XenServer

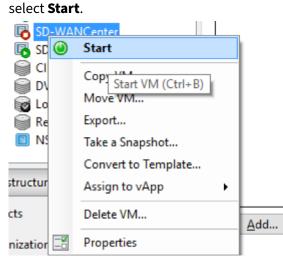
The management IP address is the IP address of the Citrix SD-WAN Center VM, use this IP address to log into the Citrix SD-WAN Center Web UI.

Note

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

To display the management IP Address:

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



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

SD	WANCen	ter on 'x	enserver-29	.2'										Logged in	n as: Local root a
eneral	Memory	Storage	Networking	Console	Performance	Snapshots	Search								
OVD Dri	ive 1: <er< td=""><td>npty></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>~</td></er<>	npty>													~
			Debi	o.o. 0.111			onton	++1							
			Mana	an GNU gement	/Linux 7 IP = 10.	102.29.	230	llyr							
			SD-W	ANCent	er login:	[34	.79134	7] fuse	init	(API \	version	7.17)			
			-												

3. Make a note of the management IP address.

Note

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

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

Login: admin

Password: password

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

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

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

Login: admin , Password: password

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

Add and configuring data storage for a XenServer server

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

To add and configure the data storage:

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

😣 Add Virtu	al Disk	?	\times
	e, description and size for your virtual disk. The size of your disk and the home so ne disk belongs to will affect which storage locations are available.	erver sett	ing
Name:	SD-WAN Center]	
Description:			
Size:	10.000 🖨 GB 🗸		
Location:	Cocal storage on xenserver-29.2 704.22 GB free of 909.01 GB		
	Add	Cance	I

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

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

March 12, 2021

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

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

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

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

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

File Action View	v Help		Hyper-V	Manager			
	?						
Hyper-V Manag		chines	-				
	New	Valual Machine	Charles	CDUUIssas	Assisted Manager		
	Import Virtual Machine Hyper-V Settings	Hard Disk Floppy Disk	State Running Off	CPU Usage 0 %	Assigned Memory 4096 MB		
	Virtual Switch Manager		Running	0 %	4096 MB		
	Virtual SAN Manager	0.0.1.27	Running	0 %	8192 MB		
	Edit Disk Inspect Disk	l WO VPX - Hyper-V-old l WO VPX - Hyper-V	Off Off Off				
	Stop Service Remove Server Refresh	hine-142 WAN SE VPXMCN_207 WAN SE VPX_10.0.1.27_MCN WAN SE VPX_10.0.1.27_Branch	Off Running Off Off	0 %	4096 MB		
	View	-WAN SE VPX 9.3.5	Running	0 %	4096 MB		
	Help	Ш					
	Checkpoin		virtual machine h	as no checkpoints.			

The New Virtual Machine Wizard appears. Click Next.

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

ð.	New Virtual Machine Wizard					
Specify Name	e and Location					
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk	Choose a name and location for this virtual machine. The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload. Name: SDWC_temp You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.					
Installation Options	Store the virtual machine in a different location					
Summary	Location: C:\ProgramData\Microsoft\Windows\Hyper-V\ Browse					
	▲ If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.					
	< Previous Next > Finish Cancel					

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

Note

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

ðv.	New Virtual Machine Wizard
Assign Memo	ory
Before You Begin Specify Name and Location Specify Generation Assign Memory Configure Networking Connect Virtual Hard Disk Installation Options Summary	 Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 93542 MB. To improve performance, specify more than the minimum amount recommended for the operating system. Startup memory: 8192 MB Use Dynamic Memory for this virtual machine. When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.
	< Previous Finish Cancel

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

a.	New Virtual Machine Wizard
Connect Vir	tual Hard Disk
Before You Begin Specify Name and Location Specify Generation Assign Memory	A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties. C Create a virtual hard disk Use this option to create a VHDX dynamically expanding virtual hard disk.
Configure Networking Connect Virtual Hard Disk Summary	Name: SDWC_temp.vhdx Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\ Size: 127 GB (Maximum: 64 TB) Isse an existing virtual hard disk Use an existing virtual hard disk Use this option to attach an existing virtual hard disk, either VHD or VHDX format.
	Location: \vhd\ys-sdwc-10.0.2.22-hyperv.vhd\ymsv1_hyperv_dynamic.vhd Browse O Attach a virtual hard disk later Use this option to skip this step now and attach an existing virtual hard disk later.
	< Previous Next > Finish Cancel

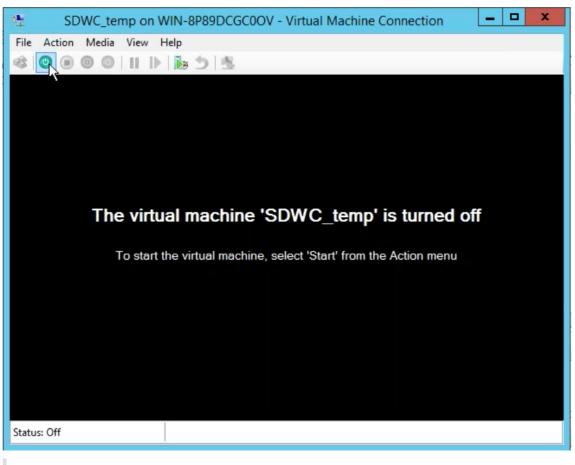
- 7. Review the VM summary and change the settings if necessary, else click **Finish**. The SD-WAN Center VM is created and is listed in the **Virtual Machines** section.
- 8. Right-click the SD-WAN Center VM and select **Settings**. Set the number of virtual processors to four and click **Apply**.

*	Hardware		D 2	
1	Add Hardware Image: BIOS Boot from CD Image: Memory 8192 MB		You can modify the number of virtual processor the physical computer. You can also modify oth Number of virtual processors:	
Ŧ	Processor		Resource control	
_	2 Virtual processors		You can use resource controls to balance res	ources among virtual machines.
	 IDE Controller 0 Hard Drive nmsv1 hyperv_dynamic.vhd 		Virtual machine reserve (percentage): Percent of total system resources:	0
	IDE Controller 1		Percent or total system resources.	
	DVD Drive None		Virtual machine limit (percentage):	100
1	SCSI Controller		Percent of total system resources:	5
Đ	Network Adapter Mgt Network	≡	Relative weight:	100
1	COM 1 None			
1	Terror COM 2 None			
I	Diskette Drive			
-	Management			
	I Name SDWC_temp			
	Integration Services Some services offered			
1	Checkpoint File Location C:\ProgramData\Microsoft\Win			
	Smart Paging File Location C:\ProgramData\Microsoft\Win			
1	Automatic Start Action Restart if previously running	~		

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

Name 🔻			State	CPU Usage	Assigned Memory	Uptime	Status	/
Windows7 waopt_buildroot		Running Off	0 %	4096 MB	12.18:44:13			
SDWC_temp			Off					
sdwan_prakhar		Connect	Running	0 %	4096 MB	5.00:02:38		
SDWAN_center_10.0.1.27		Settings	off	1%	8192 MB	6.23:35:51		
NetScaler SD-WAN WO VPX - Hyp NetScaler SD-WAN WO VPX - Hyp		Start						
Debian_2-141		Checkpoint						
Debain_virtual machine-142 Citrix NetScaler SD-WAN SE VPXN Citrix NetScaler SD-WAN SE VPX_ Citrix NetScaler SD-WAN SE VPX_		Move Export Rename Delete		0 %	4096 MB	4.00:31:13		>
Checkpoints		Enable Replication						0
		Help						0

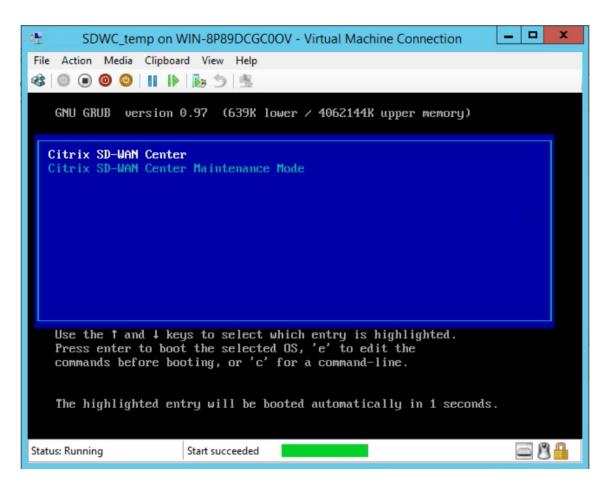
10. Click the **Start** button.



Note

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

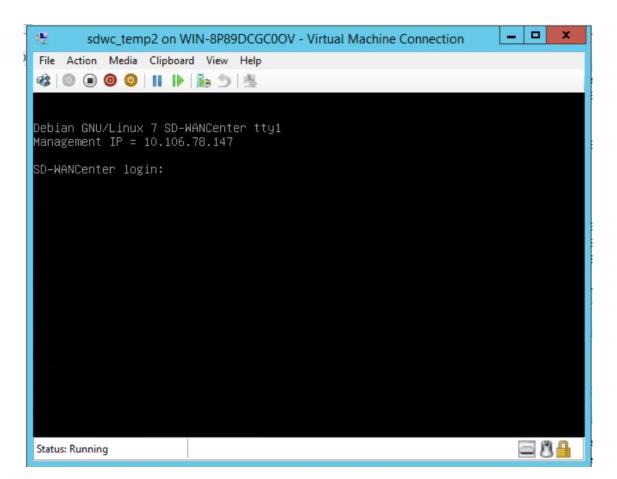
11. Once the VM is started, selected Citrix SD-WAN Center and hit enter.



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

Login: admin

Password: password



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

Note

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

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

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

Login: admin

Password: password

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

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

Citrix SD-WAN Center on Azure Marketplace using solution template

March 12, 2021

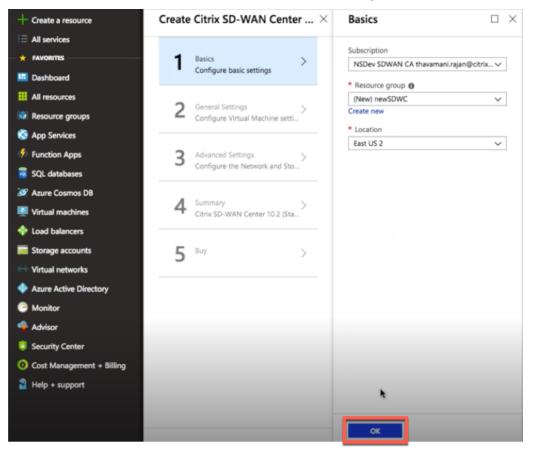
Citrix SD-WAN Center is now available in the Azure Marketplace. You can deploy Citrix SD-WAN Center as a Virtual Machine (VM) in Azure Cloud using solution template.

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

Ensure that you have access to Microsoft Azure.

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

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



NOTE:

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

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

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

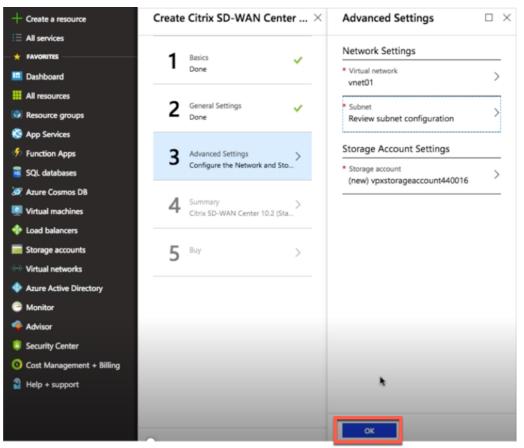
+ Create a resource	Create Citrix SD-WAN Center \times	General Settings \Box \times
E All services		* Name of the SDWAN Center Virtual machine
+ FAVORITES	Basics 🗸	 Name or the SDWAN Center Virtual machine () sdwcvm
🔲 Dashboard	Done	* User name 💿
All resources	•	adminuser123 🗸
📦 Resource groups	2 General Settings > Configure Virtual Machine setti	* Password ()
🔇 App Services		······ 🗸
🤣 Function Apps	Advanced Settings	* Confirm password
🕱 SQL databases	Configure the Network and Sto	····· V
🧟 Azure Cosmos DB	_	* Virtual machine size 0
Virtual machines	4 Summary > Citrix SD-WAN Center 10.2 (Sta	1x Standard D3 v2
🚸 Load balancers		۱ <u>۰۰۰۰</u>
Storage accounts	5 Buy >	
• Virtual networks	5	
Azure Active Directory		
Monitor		
🔷 Advisor		
Security Center		
Ost Management + Billing		
🔒 Help + support		
		ОК

NOTE:

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

Choose Browse the av	a size	heir features									Ω×
Search			Compute type Current generation		V All	type disk types		vCPUs	0		128
RECOMM											
NECONIN	SKU	TYPE	COMPUT 🕬 VCPUS	GB RAM	DATA DI	MAX IOPS	LOCAL SS	PREMIU	ADDITIO	ZONES	USD/MO
Available	sku	түре	Comput 🥬 VCPUS	GB RAM	DATA DI	MAX IOPS	LOCAL SS Th	PREMIU	ADDITIO 🖘	ZONES	14 USD/MO 14
	SKU 74	TYPE T4	COMPUT 🕬 VCPUS	14 GB RAM 14	DATA DI	MAX IOPS 14	LOCAL SS ⁺ 4	PREMIU **	ADDITIO [†] 4	ZONES 1,2,3	та USD/MO та \$136.15

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



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

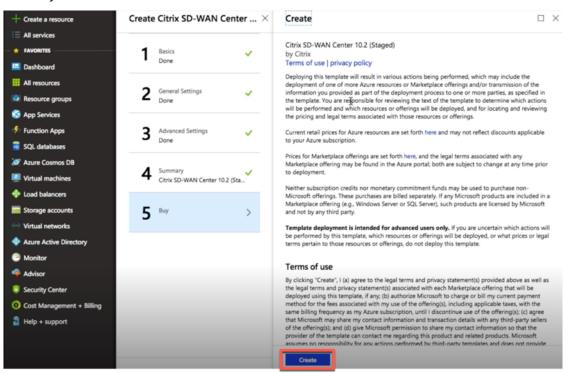
Advanced Settings	imes Choose virtual network $ imes$	Create virtual network
Network Settings		* Name
* Virtual network > (new) vnet	These are the virtual networks in the selected subscription and location 'East US 2'.	vnet * Address space
Subnet Configure subnets	+ Create new	10.12.0.0/16 10.12.0.0 - 10.12.255.255 (65536 addresses)
Storage Account Settings	ARM_Deploy_Staging-vnet ARM_Deploy_Staging	
* Storage account (new) vpxstorageaccount440016	<pre>www.example.com www.example.com www.examp</pre>	
	Vnet01 testssdwcrg	
	Vnet01 SDWCResourceDroup	
	Vnet01 SDWCresgrp	
	Vnet01 SDWANcenterRG	
OK		ОК

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

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

+ Create a resource	Create Citrix SD-WAN Cen	nter $ imes$	Summary		$\Box \times$
i≡ All services			Validation passed		
+ FAVORITES	Basics	~		¢9	
🛄 Dashboard	Done		Basics		
All resources	-		Subscription Resource group	NSDev SDWAN CA thavamani.rajan@citrix.com newSDWC	
Resource groups	2 General Settings Done	~	Location	East US 2	
🔇 App Services			General Settings		
Function Apps	Advanced Settings	~	Name of the SDWAN Center Vi	sdwcvm adminuser123	
SQL databases	Done	•	Password		
Azure Cosmos DB			Virtual machine size	Standard D3 v2	
Virtual machines	4 Summary Citrix SD-WAN Center 10.2 (S	>	Advanced Settings Virtual network	vnet01	
Load balancers	Citrix SD-WAIN Center 10.2 (s	5ta	Subnet Subnet address prefix	managementsubnet1011 10.13.0.0/24	
Storage accounts	E Buy		Storage account	vpxstorageaccount440016	
	5 Buy	>			
Virtual networks					
Azure Active Directory					
Monitor					
Advisor			•		
Security Center					
O Cost Management + Billing					
Help + support					
				late and examples	
			OK Download temp	plate and parameters	

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



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

follow the general SD-WAN Center deployment guidelines.

Add data disk

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

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

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

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

sdwcvm - Disks							\$
	🗜 Save 🗙	Discard 🖏 Refresh					
Overview Activity log Access control (IAM)		disks created since June 10, 2017 are encry		Storage Service Encryptio	n (SSE). You may also wa	nt to enable Azure Disk Encryption.	
🛷 Tags	Disk settings						
★ Diagnose and solve problems	Enable Ultra SS	D compatibility (preview) 💿					
Settings	OS disk						
A Networking							
a Disks	NAME		\$121	STORAGE ACCOUN	ENCRYPTION	HOST CACHING	
📮 Size	sdwcvm_Ost	Disk_1_0ef708b22f9c44d6981c3c85	8 GiB	Standard HDD	Not enabled	Read/write V	
C Security	Data disks						
Extensions	LUN	NAME	SIZE	STORAGE ACCOU	ENCRYPTION	HOST CACHING	
🐔 Continuous delivery (Preview)	0	additional_disk	1200 GiB	Standard HDD	Not enabled	Read/write	÷
Availability set	v	additional_disk	1200 010	Standard Hoo	Not enabled	None	۳
Configuration	+ Add data	disk				Read-only	
🐍 Identity						Read/write	
🐍 Identity						Read/write	

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

Citrix SD-WAN Center 11.4

Home > sdwcvm - Disks > Create managed disk		
Create managed disk		\times
•		
* Disk name 💿		
sdwc_Disk	~	
* Resource group		
W0sdwcissue		1
Create new	~	J
Create new		
Location		
East US 2		
Aug Habilita and a		
Availability zone 👩		1
None		
* Account type o		
Standard HDD	~	1
		·
* Size (GiB) 💿		,
1023	~	
Source type 0		
None	~	1
		1
RATILLITER DEREONLILLER		
ESTIMATED PERFORMANCE		
IOPS limit 500		
Throughput limit (MB/s) 60		
Create		

Attach a disk by filling the following mandatory details:

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

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

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

March 12, 2021

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

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

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

Note:

Amazon makes frequent changes to its AWS pages, so the following instructions may not be upto-date.

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

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

Second approach:

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

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

AWS services			Access resources on the go
	re (for example, EC2, S3 or VM, storage)		Access the Management Console using the AWS Console Mobile App. Learn more 2
 Recently visited services 			
🗆 EC2 ト	Lambda	Ş; VPC	Explore AWS
All services			
Compute	Management Tools	Haws Cost Management	Amazon Redshift
EC2 Lightsail 🔀 ECS	CloudWatch AWS Auto Scaling CloudFormation	AWS Cost Explorer AWS Budgets	Fast, simple, cost-effective data warehouse that can extend queries to your data lake. Learn more 🖸
EKS Lambda	CloudTrail Config	🛄 Mobile	Run Serverless Containers with AWS
Batch	OpsWorks	AWS Amplify	Fargate
Elastic Beanstalk	Service Catalog Systems Manager	Mobile Hub AWS AppSync Device Farm	AWS Fargate runs and scales your containers without having to manage servers or
Storage	Trusted Advisor Managed Services	Device Farm	clusters. Learn more 🖸
S3		989 AR & VR	
EFS	Da Media Services	Amazon Sumerian	Scalable, Durable, Secure Backup &
S3 Glacier	Elastic Transcoder	Amazon Sumenan	Restore with Amazon S3
Storage Gateway	Elastic Transcoder		Discover how customers are building backup 8

AWS Management Console

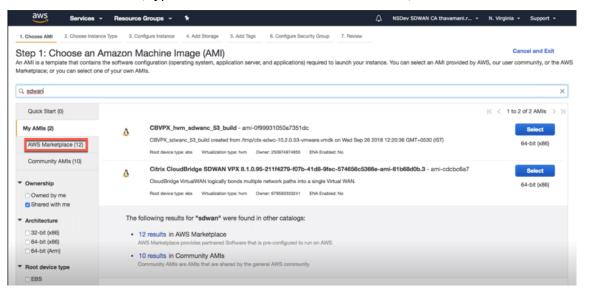
Citrix SD-WAN Center appliances offer the EC2 as an AWS service instances.

- EC2 Dashboard elastic compute cloud, resizable virtual services / instances
- 3. Click **EC2** in the **Compute** section, then select **Launch Instance**.

EC2 Dashboard Events Resources C* Account Attributes Tags You are using the following Amazon EC2 resources in the US West (N. California) region: Supported Platforms Tags 1 Running Instances 3 Elastic IPs EC2 VPC	
Livensa You are using the following Amazon EC2 resources in the US West (N. California) region: Supported Platforms Tags 1 Running Instances 3 Elastic IPs EC2 Reports 1 Running Instances 3 Elastic IPs V/C	
Reports 1 Running Instances 3 Elastic IPs CC	
Limits 0 Dedicated Hosts 2 Shapshots	
13 Volumes 0 Load Balancers Resource ID length managem	
NSTANCES 13 Key Pairs 13 Key Pairs 21 Security Groups Console experiments	
Launch Tempiates 0 Placement Groups Additional Informatio	
Shat Daguate	
opon requests Reserved Instances Learn more about the latest in AWS Compute from AWS re:Invent 2017 by viewing the EC2 Videos.	
Dedicated Hosts All EC2 Resources	
Capacity Reservations Create Instance Forums	
IMAGES To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance. Pricing	
AMIs Contact Us	
Bundle Tasks Launch Instance -	
ELASTIC BLOCK STORE Note: Your Instances will launch in the US West (N. California) region AWS Marketplace	
Volumes Find free software trial produc	ts in the AWS
Snapshots Service Health C Scheduled Events C Marketplace from the EC2 La	inch Wizard. Or
Lifecycle Manager Service Status: US West (N. California): try these popular AMIs:	
NETWORK & SECURITY JUST KALENDARY NO events Barracula CloudGen Firewall	for AWS - PAYG
Security Groups Availability Zone Status: By Barracuda Networks, Inc.	
Elastic IPs Batting #**** Elastic IPs Batting #**** Elastic IPs Batting #**** Elastic IPs Batting #****	\$4,599/vr (12%
Placement Groups Availability zone is operating normally savings) for software + AWS u	sage fees
Key Pairs View all Infrastructure Softwar	•
Network Interfaces Availability zone is operating normally Matilion ETL for Amazon Red	shift
E LOAD BALANDING Us-west-1c: By Matilion	

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

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



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

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

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

by selecting a specific insta	nce type or all in	stance type with o	current generation.
by seccetting a specific mote	nee cype of all in	iscance cype mich	Same Beneration.

1. Choose	AMI 2. Choose Instance Typ	3. Configure Instance	4. Add Storage	5. Add Tags 6. Conf	Igure Security Group 7. Review			
nazon E		of instance types optimized			tual servers that can run application or about instance types and how	, , .	,	nd networkin
iter by:	All instance types 👻	Current generation	Show/Hide Col	lumns				
Currentl	selected: t2.micro (Variable	e ECUs, 1 vCPUs, 2.5 GHz,	Intel Xeon Family, 1	GIB memory, EBS only	0			
	Family	- Туре -	vCPUs () -	Memory (GiB) ~	Instance Storage (GB) () -	EBS-Optimized Available	Network Performance () -	IPv6 Support (i
	General purpose	t2.nano	1	0.5	EBS only		Low to Moderate	Yes
	General purpose	t2.micro Free tier eligible	3	i.	EBS only		Low to Moderate	Yes
	General purpose	t2.small	1	2	EBS only		Low to Moderate	Yes
	General purpose	t2.medium	2	4	EBS only	4	Low to Moderate	Yes
	General purpose	t2.large	2	8	EBS only	,	Low to Moderate	Yes
	General purpose	t2.xlarge	4	16	EBS only		Moderate	Yes
	General purpose	t2.2xlarge	8	32	EBS only		Moderate	Yes
0	General purpose	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
0	General purpose	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

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

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

aws	Services ~ R	lesource Groups 🗸	*					SDWAN CA the	wamani.r •	N. Virginia	Support -
Choose AMI	2. Choose Instance Type	3. Configure Instance	4. Add Storage 5.	Add Tags 6. C	onfigu	re Security Group 7. Review					
	onfigure Instan stance to suit your require		nultiple instances from	the same AMI, re	quest	Spot instances to take advantage	e of the lowe	r pricing, assign	an access ma	nagement role	to the instance
	Number of instances	1	Lau	inch into Auto Sca	ling G	roup (j)					
	Purchasing option	(i) Request Sp	ot instances								
	Network	(i) vpc-257ea54	e Ruchira-VPC	•	C	Create new VPC					
	Subnet	i subnet-22945 251 IP Address	068 SDP-test us-ea	st-1c 🛊		Create new subnet					
	Auto-assign Public IP	(i) Use subnet se	etting (Disable)	÷							
	Placement group	(i) Add instance	e to placement group.								
	Capacity Reservation	(i) Open		÷	C	Create new Capacity Reservation	n				
	IAM role	(i) None		¢	C	Create new IAM role					
	CPU options	Specify CPL	J options								
	Shutdown behavior	() Stop		¢							
Enable	termination protection	Protect agai	nst accidental terminal	tion							
	Monitoring	Enable Clou Additional char	dWatch detailed monit ges apply.	oring							
							Canc	Previous	Review an	d Launah	NOT: Add Sto

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

Citrix SD-WAN Center 11.4

	Services ~	Resource Groups 👻	*					SDWAN CA thavam	ani.r 👻 N. Virg	inia - Support -
hoose AMI	2. Choose Instance Typ	3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review				
instance will he settings o					BS volumes and instance storestance, but not instance store					
ume Type ()	Device () Snapshot ()	Size	(GiB) (j)	Volume Type ①		IOPS ()	Throughput (MB/s)	Delete on Termination	Encrypted ()
ot	/dev/sda1	snap-063e7ca92	88d413e8 40		Magnetic (standard)	\$	N/A	N/A	۲	Not Encrypted
	ions and also deliver	a consistent baseline of 3 I	IOPS/GIB. Set my ro	ot volume to G	ent of volume size, to meet th eneral Purpose (SSD). age. Learn more about free u					
ree tier eligib										
ree tier eligib										
ree tier eligib										

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

×
t

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

Citrix SD-WAN Center 11.4

aws	Services ~	Resource Groups ~	*				∴ NSDev	SDWAN CA thavamani.r	N. Virginia 👻	Support +
. Choose AMI	2. Choose Instance Ty	pe 3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review				
opy of a tag c	a case-sensitive key can be applied to volu	-value pair. For example, you mes, instances or both, nd volumes Learn more abo	-							
ey (127 ch	aracters maximum)		Valu	e (255 cha	racters maximum)			Instances (i) Volum	es ()	
								0 0	8	
dd another ta	ag (Up to 50 tag	s maximum)								
						Cance	Previous	Review and Launch	Next: Configure	Security Gro

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

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

- 11	oto	
11	ULC.	

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

						7 Parlow		
1. Choose AMI	2. Choose Instance Type	3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review		
A security group is	ach your instance, add	at control the traffic for	cted access to the				or example, if you want to set up a web server an existing one below. Learn more about Ama	
	Assign a security gro							
		Select an existing	ng security group				Filter VPC s	ecurity groups \$
Security Grou	up ID Name				Description			
sg-7f55121a	California_GW				California_GW			
sg-77561112	default				default VPC security grou	p		
sg-32edab57	launch-wizard-2				launch-wizard-2 created 2	015-10-01T15:19:06.090+05:30		
sg-becfc6d9	launch-wizard-3	1			launch-wizard-3 created 2	017-06-14T16:46:00.550+05:30		
sg-0a849f01962	55e689launch-wizard-4				launch-wizard-4 created 2	018-11-12T10:29:26.790+05:30		
sg-7e888019	MCN_security_	group_ZTD			MCN_security_group_ZT	D		
sg-56d57e2e	NetScaler SD-V	AN Standard Edition 2	00 Mbns-9-3-0-76-4	AutonenBvAWS	MP-This security aroun was a	enerated by AWS Marketnlace a	and is based on recommended settings for Net	Scaler SD-WAN S
Inbound rules for	sg-7f55121a (Selecter	d security groups: sg-	7f55121a)					
Type (i)		Protocol (i)		Port Ra	nge (j)	Source (i)	Description (i)	
All TCP		TCP		0 - 655	35	122.167.227.14/32		
All traffic		All		All		14.141.5.5/32		
All traffic		All		All		192.168.0.0/16		

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

lease revie	ew your	instance co	nfiguration	is not eligib	e for the free us	age tier	Launch to assign a key pair			and usage restrictions.
			-							Don't show me this again
A	Impro	ove your ins	tances' se	curity. Your s	ecurity group, C	alifornia_GW	, is open to the world.			
	Your ins You car	istances may b in also open ad	e accessible f	rom any IP add	ess. We recommend	that you update	, is open to the world. your security group rules to ication or service you're runr	allow access from		Edit Al

Two factor authentication

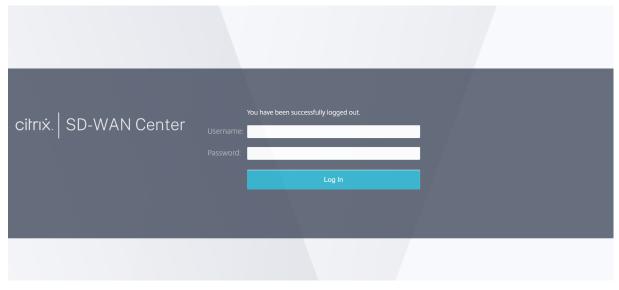
March 12, 2021

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

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

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

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



Citrix SD-WAN Center login credentials:

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

Note

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

Primary authentication

March 12, 2021

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

Note

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

RADIUS authentication server

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

To enable and configure RADIUS authentication:

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

Note

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

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

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

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

Note

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

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

Note

The **Enable Two-factor** option appears only when the secondary authentication server is configured.

Configure a secondary authentication server, either RADIUS, or TACAS+. For more information, see Secondary authentication.

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

imary Authentication			
RADIUS Authentication	0	TACACS+ Authentication	0
Timeout: Server Key: Confirm Server Key: 10 Image: Server Key: Image: Server Key:			Apply Verify
Servers +			
IP Address Port Delete ▲ ▼ 10.102.72.41 1812 1			
[Apply Verify		

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

Verify RADIUS Server Settings
Enter a valid user name and password for the authentication servers to verify your configuration.
User Name:
admin
Password:
Verify Close

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

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

TACACS+ authentication server

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

To enable and configure TACACS+ authentication:

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

Note

If RADIUS authentication is already enabled, it gets disabled.

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

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

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

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

Note

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

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

Note

The **Enable Two-factor** option appears only when the secondary authentication server is configured.

Configure a secondary authentication server, either RADIUS, or TACAS+. For more information, see Secondary authentication.

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

Primary Authentication			
RADIUS Authentication Enable RADIUS Authentication	Apply Verify	TACACS+ Authentication Image: Authentication Timeout: Authentication Type: 10 ASCII Image: Abile Tackson Type:	0
		Servers + IP Address Port Delete V 10.102.72.41 49	Apply Verify

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

Verify TACACS+ Server Settings
Enter a valid user name and password for the authentication servers to verify your configuration.
User Name:
admin
Password:
Verify Close

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

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

Secondary authentication

March 12, 2021

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

Note

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

Secondary RADIUS authentication server

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

To enable and configure RADIUS authentication:

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

Note

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

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

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

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

Note

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

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

Secondary Authentication	
RADIUS Authentication	⑦ TACACS+ Authentication ⑦
Enable Secondary RADIUS Authentication	Enable Secondary TACACS+ Authentication
Timeout: Server Key: Confirm Server Key: 10	Apply: Venty
Servers → IP Address Port Delete ▲ ▼ 10.102.166.80 1812 面	
Apply. Verifi	krify

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

Verify SECONDARY RADIUS Server
Settings
×
Enter a valid user name and password for the authentication servers to verify your configuration.
User Name:
admin
Password:
Verify Close

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

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

Secondary TACACS+ authentication server

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

To enable and configure TACACS+ authentication:

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

Note

If RADIUS authentication is already enabled, it gets disabled.

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

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

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

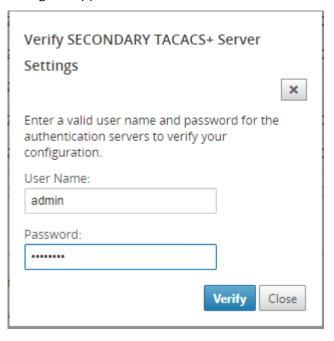
Note

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

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

Secondary Authentication		
RADIUS Authentication C Enable Secondary RADIUS Authentication	TACACS+ Authentication Enable Secondary TACACS+ Authentication Timeout: Authentication Type: Server Key: 10 ASCII ••••••	0
	Servers + IP Address Port Delete A ▼ 10.102.72.104 49 10	
		Apply Verify-

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



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

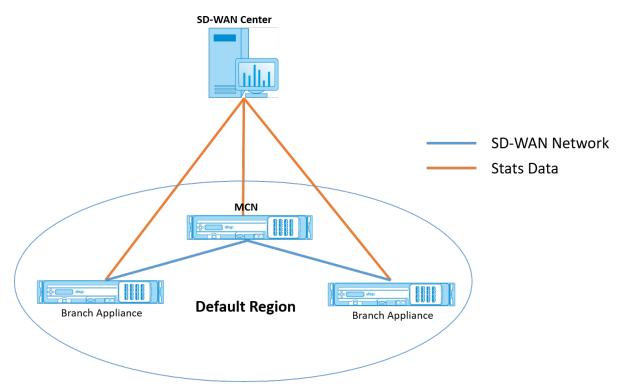
To configure more servers, repeat the steps 7 through 12.

Single-region network deployment

March 12, 2021

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

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



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

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

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

	Monitoring Configurati	on Reporting							
Network Discovery	Configuration / Network Discov	ery / Discovery Settings							
Network Configuration	SSL Certificate Disc	wery Settings	Inventory And Status						
Zero Touch Deployment	MCN Configuration								
Change Management	Master Control Node MGT IP Addr	855:							
Appliance Settings	10.102.78.154 Test								
Mobile Broadband	Discover								
Licensing	Collector Configuration								0
Cloud Connectivity	Show to V entries See	Region N	ame	RC	N IP Address	Collector IP Address		Appliance Discovery Status	
	Default,			10.102.78.154		127.0.0.1	Done		
	Showing 1 to 1 of 1 entries								Previous 1 Next
	Discover Appliance Delete								
	Note: Collector IP Address can be	configured for Multi-Regio	n Networks						
		width Limit (keps):							0
	3 100	0							
	Apply								

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

Note

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

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

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

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

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

Citrix SD-WAN Center 11.4

SSL C	ertificate	Disco	very Settings	Inventory And S	Status							
Select Reg	gion: Defau	It_Region ▼										
Showing	1 - 4 of 4									Search		C
🗌 Poll 🧥	State	Name	Region Name	MGT IP Address	Model	Serial Number	Software	Registry Timestamp	Last Succes	sful Poll	Latest Record	Download
0	Not Polling	RL-MCN-P	Default_Region	10.102.78.175	vpx	301a93fa-9e2c- fd44-b991- 6f74f25cd90f	R9_3_0_401_434810	1540786694	11/26/18 4	:08	11/22/18 4:45	÷
	Not Polling	RL-MCN-P	Default_Region									
	Not Polling	RL-MCN-S	Default_Region	10.102.78.184	vpx	98538a49-0de7- bc78-4105- 2b4f01845078	R9_3_0_401_434810	1540786694	11/26/18 4	:08	11/19/18 16:04	÷
	Not Polling	RL-CL1	Default_Region									

11. Click Apply.

Тір

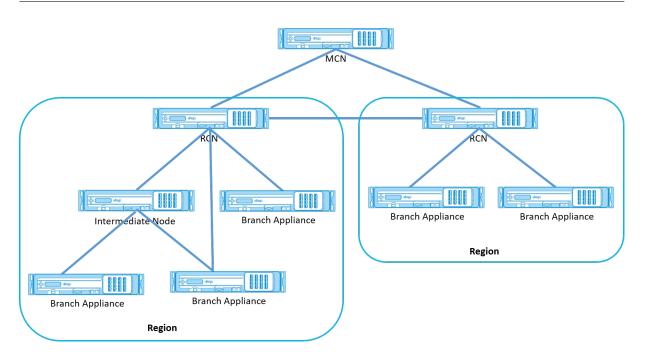
You can increase the storage size of the Citrix SD-WAN Center by creating a data store on your virtual machine and switching the data store. For more information see, Switch the active storage to new data storage.

Multi-region network deployment

March 12, 2021

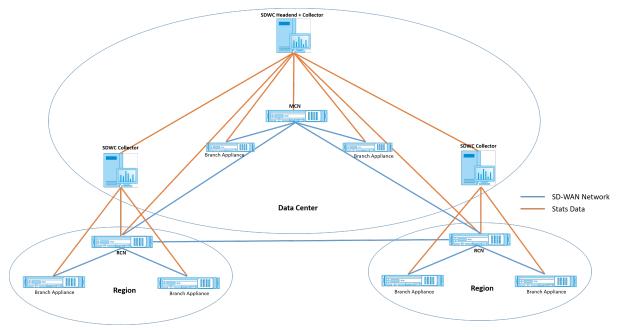
If your organization has a large network spanning multiple administrative (or geographical) boundaries, you can use Citrix SD-WAN Center in multi-region mode, with each region supporting a maximum of up to 550 sites.

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



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

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



Note

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

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

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

Note

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

Dashboard Fault	Monitoring	enfiguration Reportin) Administration	Nitro API				
Network Discovery	Configuration / Netwo	rork Discovery / Discovery Settings						
Network Configuration	SSL Certificate	Discovery Settings	Inventory And Status					
Zero Touch Deployment								
Change Management	MCN Configuration	/GT IP Address:						
Appliance Settings		Test						
Mobile Broadband	Discover							
Licensing	Collector Configura	ation						0
Cloud Connectivity	Show 10 V entries	s Search						
	•	Region	Name	RCN IP Address	Collector IP Address		Appliance Discovery Status	
		Default_Region		10.102.76.186	127.0.0.1	Done		
	0	ANZ		10.102.76.189	Empty collector IP	 Not Started 		
		APAC		10.102.76.188	Empty collector IP	 Not Started 		
	•	EMEA		10.102.76.231	Empty collector IP	🖌 Not Started		
	Showing 1 to 4 of 4 entr							Previous 1 Next
	Note: Collector IP Addr	ress can be configured for Multi-Reg	jon Networks					
	Polling Configuration							G
	Polling Interval (min):	Bandwidth Limit (kbps): 1000						

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

Note

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

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

	Monitoring	Configuration			Nitro API		
Network Discovery	Configuration / Ne	twork Discovery / Discove	ry Settings				
Network Configuration	SSL Certificate	Discovery Settings	Inventory A	nd Status			
Zero Touch Deployment							
Change Management	MCN Configuration						
Appliance Settings Mobile Broadband	Discover						
Licensing	Collector Configu	ration					0
Cloud Connectivity	Show 10 Tentri	es Search:					
	•	Region Name		P Address	Collector IP Address	Appliance Discovery S	itatus
		ult_Region	10.102.76.186		127.0.0.1	Done	
	ANZ		10.102.76.189		,	Done Done	
	_				10.102.78.173	Collector Not Reachable	
	EME Showing 1 to 4 of 4 e		10.102.76.231		10.102.78.173	Collector Not Reachable	
	Discover Appliance		r Multi-Region Networks				Previous 1 Next
	Polling Configuration Polling Interval (min): 3	n Bandwidth Limit (kap: 1000	ə):]				(

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

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

Note

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

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

 	RCN Name	RCN IP Address	Collector IP Address		Discovery Status
	Default_Region	10.102.76.186	127.0.0.1		Done
•	ANZ	10.102.76.189	10.102.78.89	/	Not Started
•	APAC	10.102.76.188	10.102.78.91	/	Not Started
•	EMEA	10.102.76.231	10.102.78.87	/	Not Started

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

SSL C	ertificate	Discov	ery Settings	Inventory And S	itatus							
Select Re	gion: All	Ŧ										G
Showing	1 - 8 of 8									Search		c
🗌 Poll 🔺	State	Name	Region Name	MGT IP Address	Model	Serial Number	Software	Registry Timestamp	Last Succe	ssful Poll	Latest Record	Download
	Not Polling	RL-MCN-P	Default_Region	10.102.78.175	vpx	301a93fa-9e2c- fd44-b991- 6f74f25cd90f	R9_3_0_401_434810	1540786694	11/26/18	4:14	11/22/18 5:19	÷
	Not Polling	RL-MCN-P	Default_Region									
	Not Polling	RL-MCN-S	Default_Region	10.102.78.184	vpx	98538a49-0de7- bc78-4105- 2b4f01845078	R9_3_0_401_434810	1540786694	11/26/18 4	1:14	11/19/18 16:06	÷
	Not Polling	RL-CL1	Default_Region									
	Not Polling	RL-R1-CL1	New_York	10.102.78.178	vpx	083e52e4-d75a- 36f8-5d1e- 30f266d40b68	R9_5_0_401_434810	1538848425	11/26/18	£11	11/26/18 4:11	÷
	Not Polling	RL-R1-CL2	New_York									
	Not Polling	RL-RCN1-P	New_York	10.102.78.177	vpx	628d9f7f-55c0- d912-b770- 856717f16f07	R9_5_0_401_434810	1538848425	11/26/18	£11	11/26/18 4:11	÷
	Not Polling	RL-RCN1-S	New_York	10.102.78.180	vpx	9f9ffa51-c34c- 77c8-b637- b8ab6a26654e	R9_5_0_401_434810	1538848425	11/26/18	k11	11/26/18 4:10	÷
4												•

Тір

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

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

Тір

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

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

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

Dashboard		ault	Monit	oring	Co	nfiguration	R	eporting	Admin	istration	Nit	ro API					
Reporti Region: Default Default New V APAC EMEA	Region V	1	e As														
Tim	e: Febru	ary 7, 201	8 10:18pm		.ast: Hou	/ Day / Week	(/ Month	1 22. jan	24. jan 2	26. Jan 28	. Jan	Mod 30. Jan	e: Relativ	e (8 hours from no	ow) 5. Feb	• C	
	10. Jan	12. Jan			5. jan	L	0. Jan	22. Jan			. Jan	30. Jan	1. Feb	a. e.	5. Feb	7. Feb	
Routing Domain:	Any		٣												Show Bandw	idth/Data in	Kbps/KB 🔻
Applications	HDX	MOS	Services	Classes	Sites	Virtual Paths	Paths	WAN Links	MPLS Queue	es Ethernet	GRE	IPsec	Events				
Report Type:	Тор Ар	plications	•	Select Site	e:		•										

Configuration

March 12, 2021

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

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

Configure the management interface settings

March 12, 2021

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

The management Interface settings include the following:

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

Secondary DNS

To configure the management interface settings:

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

By default, the User/Authentication Settings page appears.

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

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

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

Management and DNS

P Address:	Gateway IP Address
10.102.29.225	10.102.29.1
Subnet Mask:	
255.255.255.0	

4. Click Apply.

Note

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

Install the SD-WAN Center SSL certificate

March 12, 2021

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

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

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

SD-WAN Center Certificate	0
Before 50-VIAN Center can begin initial discovery of your network, an SSL certificate must be installed on the active Master Control Node. Click the Download Certificate button below, then upload the certificate to the Master Control Node's Web Console, under Configuration > SD-WAN Center Certificates	
Centificate Progenitive: 81380-39131 01 79 842 64 44 60 77 58 20 04 44 05 61 68 14 49 6 C3 Start Date: 569 24 08 31 21 2019 UTC Bipitation Date: 559 21 08 31 21 2029 UTC	
Download Centrate	

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

Dashboard Monitoring	Configuration			
+ Appliance Settings - Virtual WAN	Configuration > Virtual WAN > SD-WAN Center Certificates			
View Configuration	Certificate Management			
Configuration Editor	This page allows for the management of SD-WAN Center certificates. Installing an SD-WAN Center	r certificate will allow this Vir	rtual WAN to be managed/monitored by the	SD-WAN Center platform that generated
··· Change Management	the certificate.	_		
Restart/Reboot Network	Install Certificate: Browse Upload and Insta	1		
Enable/Disable/Purge Flows Dynamic Virtual Paths	Delete Certificate: 0D:DB:E8:12:80:91:21 V Delete			
SD-WAN Center Certificates				
+ System Maintenance	Installed Certificates			
	Certificate Fingerprint	Start Date	Expiration Date	
				1

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

Configuration > Virtual WAN > SD-WAN Center Certificates
SD-WAN Center Certificate Management
This section allows for the management of SD-WAN Center certificates. Installing an SD-WAN Center certificate will allow this Virtual WAN to be managed/monitored by the SD-WAN Center platform that generated the certificate.
Install Certificate Choose File SDWANCENTE1 (2) pem Upload and Install
Delete Certificate: 81 87 66 B8 83 8C CZ • Delete

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

Install the Citrix SD-WAN SSL certificate

March 12, 2021

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

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

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

To generate and install the SD-WANcertificate:

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



Note:

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

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



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

Configuration > Virtual WAN > SD-WAN Center Certificates							
SD-WAN Center Certificate Management							
This section allows for the management of SD-WAN Center certificates. Installing an SD-WAN Center certificate will allow this Virtual WAN to be managed/monitored by the SD-WAN Center platform that generated the certificate.							
Install Certificate: Choose File SDWANCENTEt (2) pem Upload and Install							
Delete Certificate 81.87.66 B8 83 8C.C2 • Delete							

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

Switch the active storage to new data storage

March 12, 2021

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

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

1. Log into Citrix SD-WAN Center VM.

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

Login: admin

Password: password

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

Dashboard Fault	Monitoring Configuration	Reporting Administration						
User/Authentication Settings	Administration / Storage Maintenance							
Global Settings	Storage Systems							
Database Maintenance	Host	File System	Туре	Size (MB)	Available (MB)	ActiveMigrate Data		
Storage Maintenance	Local*	/dev/xvda2	ext3	7416	4743	0		
	Local	/dev/xvdb	ext3	20480	unknown	• 🗹		
Appy								
Thresholds						0		
SD-WAN Center Database Storage and Auto Cleanup settings are misconfigured, SD-WAN Center will reach auto cleanup threshold before the configured 6 months						hs.		
Stop stats polling when storage usage exceeds 55% v) of active storage size								
	Notify user when storage usage exceeds 45% v of active storage size							
	Apply							

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

Delete All Existing Files		×			
Switching the active storage system will remove all existing files on the new file system.					
Are you sure you wish to con	tinue?				

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

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

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

Deploy Citrix SD-WAN appliance

March 12, 2021

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

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

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

Configure Citrix SD-WAN appliances

March 12, 2021

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

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

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

Configuration Editor

March 12, 2021

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

Note

You cannot push configurations to the discovered appliances directly from Citrix SD-WAN Center. You can use the Configuration Editor to edit the configuration settings and to create a configuration package. When the configuration package has been created, you can export it to the MCN and install it. The changes are then reflected in the MCN.

You have to log on with administrative rights to the Citrix SD-WAN Center appliance and the MCN, to edit the configurations on Citrix SD-WAN center and to export and install the configurations on the MCN.

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

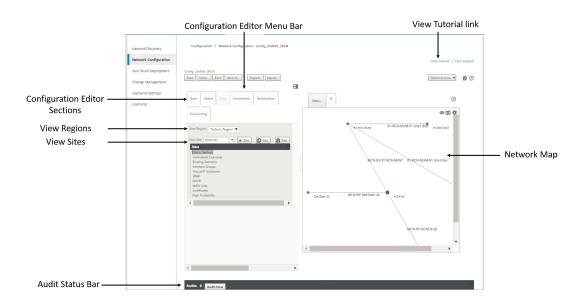
The Configuration Editor enables you to do the following:

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

To open the Configuration Editor:

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

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



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

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

Change Management Wizard

March 12, 2021

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

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

To open the Change Management Wizard:

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

Dashboard		Monitoring	Configuration	Reporting	Administration
Network Discovery		Configuration / Chan	ige Management		
Network Configurati	on				
Change Manageme	nt				
Appliance Settings					
				Click here to	
					Control Node's Change Management

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

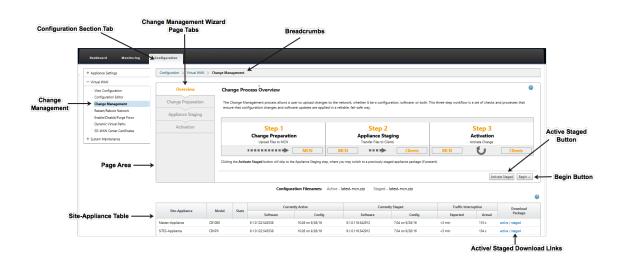
You will be automatically logged in into the MCN GUI.

Note

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

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

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



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

Note

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

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

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

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

Appliance settings

March 12, 2021

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

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

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

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

Citrix SD-	WAN	l Center				R9_2_0_82_568774 v	admin v
		Monitoring	Configuration	Reporting			
Network Discovery		Configuration / Appl	iance Settings				
Network Configuratio		New Open. Save	Save As Import	Export			0
Appliance Settings		General 🗹 Inclu	ıde in File				0
		Web Console Timeout:					
		Management Inter	face DHCP Relay	☑ Include in File			0
		DHCP Relay can only be	e enabled for appliances n	unning OS 4.5 and above.	Appliances will ignore this request if requirement is not met. DHCP Server IP Address: 10.20.10.1		
		DNS 🗌 Include in	n File				0
		Primary DNS:	Secondary DI	NS:			
		NTP 🗌 Include in	n File				0
		H Use NTP Server:	ost:				
		Timezone 🗹 in	clude in File				0
		Time Zone: EST	Y				

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

lanaged A	ppliances						
port the s	ettings file to the selected ma	anaged appliances.					
Showing	1 - 2 of 2				Search		
Select 🖌	Site Name : Appliance ID	Management IP	Model	Communication	State	Transfer Status	
	DC:0	10.102.29.235	cbvpx	not_polling		Idle	
	BranchOne:0	10.102.29.245	cbvpx	not_polling		Idle	

<		>
	Export	Cancel

Note

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

6. Click Export.

Remote LTE site management

July 16, 2021

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

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

• Citrix SD-WAN 210 SE

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

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

Perquisites for external LTE modem:

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

Note

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

Operations that are supported on internal and external modems:

O l'ann	la kana alama alama		External modem -
Operations	Internal modem	Ethernet	MBIM and NCM
SIM preference	Yes - For appliances	No	No
	that support dual SIM		
SIM PIN	Yes	No	No
APN settings	Yes	No	Yes
Network settings	Yes	No	No
Roaming	Yes	No	No

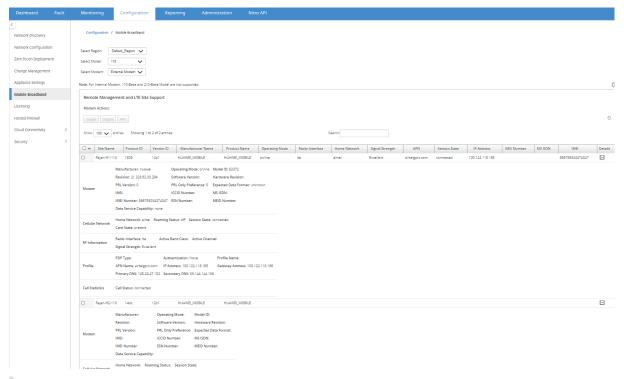
Operations	Internal modem	External modem - CDC Ethernet	External modem - MBIM and NCM
Manage firmware	Yes	No	No
Enable/Disable modem	Yes	No	Yes
Reboot modem	Yes	No	No
Refresh SIM	Yes	No	No

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

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

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

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



Note

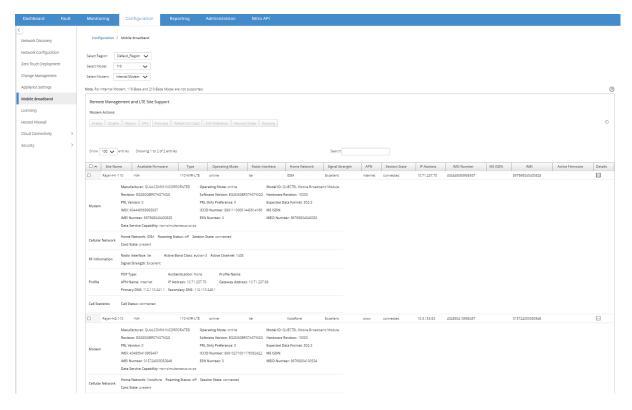
The SIM PIN and other LTE modem configurations are currently not supported for external

modems.

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

Note

The LTE operations are different for different LTE models.



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

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

Note

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

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

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

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

APN settings

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

Note

APN settings vary from carrier to carrier.

To configure APN settings:

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

APN Settings
SIM:
SIM One 🔻
APN:
fast.t-mobile.com
Username:
Password:
Authentication:
None 🔻
Apply Settings on Selected Sites
Note: APN and Username must contain a combination of only letters, numbers, underscore(_), commercial at(@), dot(.) or dash(-).

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

Citrix SD-WAN Center as a license server

March 12, 2021

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

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

SD-WAN Center.

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

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

Network_Summary		License Details		File Management				
how 100 v ent	tries					Search:		
Site Name 🔥	License Serv	er State	Model	MAXBW	Feature	Maintenance Expiry	License Expiry	License Type
u3-mcn-conf	10.102.74.42:27	000 Licensed	V100VW	100 M/S	SE	Sat Dec 1 00:00:00 2018	Sun Dec 2 00:00:00 2018	Retail
u3-mcn-conf					SE			
u3-nod1-conf	Locally Licensed	Licensed	V1000VW	1000 Mbps	SE	Sat Dec 1 00:00:00 2018	Sun Dec 2 00:00:00 2018	Retail
u3-nod2-conf	Locally Licensed	Licensed	V100VW	100 Mbps	SE	Sat Dec 1 00:00:00 2018	Sun Dec 2 00:00:00 2018	Retail
u3-nod2-conf					SE			
howing 1 to 5 of 5	entries							Previous 1 N

The following parameters are displayed:

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

Note

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

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

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

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

Note

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

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

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

Configuration / Licensing	/ File Management		
Network_Summary	License Details	File Management	
Host ld: 721b41628921			
Upload File			
Browse		Upload and Install	
Files			
File:			
	AIL_720GP_1SA_1000-Servers AIL_720GP_1SA_1000-Servers	View Delete	
CCB_2000EE-300_SSERVER			

Note

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

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

Network_Summary License Details Fil			File Management		
lost Id: 721b416				Search	
how 100 v entr Model 🔨	Used Count	Total Cou	nt Maintenance Expiry	License Expiry	License Type
2000EE-300	0	1	Sun Dec 1 00:00:00 2018	Sun Dec 1 00:00:00 2018	Retail
	2	1000	Sun Dec 1 00:00:00 2018	Sun Dec 1 00:00:00 2018	Retail

The following parameters are displayed:

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

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

March 12, 2021

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

Prerequisites

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

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

Dashboard	Fault	Monitoring	Configuration	Reporting	Administration	Nitro API	
< Network Discovery		Configuration	/ Cloud Connectivity / /	Azure / Automated A	zure Deployment		
Network Configuration	n	Cloud Connect	ivity Deployment				0
Zero Touch Deploym	ent	Cloud Connecti	vity Deployment requires lo	ogin into Citrix Workspa	ce Cloud.		
Change Managemen	t						
Appliance Settings		Cloud Connectiv	ity requires Internet conne	ctivity and authenticatio	on from Citrix Workspace Clou	ud for the Deployment feature.	
Mobile Broadband		Ensure that pop	-ups are allowed from your	SD-WAN Center IP Add	ress.		
Licensing		Login to Citrix	Workspace Cloud				
Cloud Connectivity	\sim						
Cloud Direct							
Azure	\sim						
Virtual WAN							
Automated Azur	e Deployment						
Security							

Log in with Citrix Cloud credentials.

	Citrix Secure Sign In	
https://accounts-internal.	cloud.com/core/login?signin=e0fa6531d8b50068bf	04
Citrix Cloud [™]		
Enter your Citrix credentials. (Citrix.com, My Citrix, or Citrix	(Cloud)	_
abc@citrix.com		
Remember me		
	orgot your username or password? Contact Support	
	Don't have an account?	
	Sign up and try it free	
	Sign in with my company credentials	
English (US)		
Establishing secure connection		

Automated Azure deployment

		Monitoring	Configuration	Reporting	Administration	Nitro API			
Network Discovery		Configuration /	/ Cloud Connectivity /	Azure / Automated A	zure Deployment				
Network Configuration	n	Add Site	Start	Stop Pull	Active Config Se	ttings View Stat	us Refresh		
Zero Touch Deploymer	nt								
Change Management		SITE NAM	E Û VM NAME	VM SIZE	MANAGEMENT IP	© RESOURCE GROUP ©	AZURE REGION C VNET	≎ STATUS	
Appliance Settings									
Mobile Broadband									
Licensing									
Cloud Connectivity	~								
Cloud Direct					Norr	ws found			
Azure	~				NOTO	ws round			
Virtual WAN									
Automated Azure	Deployment								
Security	>								

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

Settings		×
Azure Subscription	ID *	
Tenant ID *		
Application ID *		
Secret Key *		
•••••	•••••	
	Save	Cancel

Deploy Citrix SD-WAN in Azure

To deploy the Citrix SD-WAN in Microsoft Azure:

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

As part of this deployment, it also:

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

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

Network Discovery Configuration / Cloud Connectivity / Azure / Automated Azure Deployment Network Configuration Basic Settings Zero Touch Deployment Virtual Machine Change Management Virtual Network Appliance Settings Virtual Network Mobile Broadband Summary Licensing Summary Cloud Connectivity Ste Name* Virtual WAN Automated Azure Deployment							
Network Discovery Configuration / Cloud Connectivity / Azure / Automated Azure Deployment Network Configuration Basic Settings Zero Touch Deployment Virtual Machine Choase WM settings Azure Region* Appliance Settings Virtual Machine Choose VM settings Resource Group* Mobile Broadband Summary Licensing Confirm Cloud Direct Summary Azure Virtual WAN Automated Azure Deployment Virtual WAN				Configuration		Administration	
Basic Settings Acure Region * Virtual Machine Choose VM settings East US Appliance Settings Virtual Network Choose VM settings Summary Confirm Summary Confirm Cloud Direct Summary Confirm Azure Virtual WAN Automated Azure Deployment Virtual WAN	Network Discovery		Configuration	/ Cloud Connectivity / /	Azure / Automated Azu	re Deployment	
Change Management Virtual Machine Choose VM settings East US Appliance Settings Virtual Network Choose VM settings Resource Group * Mobile Broadband Summary Confirm Resource Group * Cloud Connectivity Site Name * Cloud Direct Azure Virtual WAN Automated Azure Deployment Kenter Settings	-		Basic Settin	igs	Basic Settings	;	
Appliance Settings Virtual Network Choose VNet settings Resource Group * Mobile Broadband Summary Confirm Conserver Licensing Summary Confirm Create new Site Name * Cloud Connectivity Br-eastus Virtual WAN Automated Azure Deployment		nt					~
Mobile Broadband Create new Licensing Summary Confirm Site Name * Cloud Connectivity Br-eastus Cloud Direct Azure Virtual WAN Automated Azure Deployment	Appliance Settings	pliance Settings Virtual Netr Choose VNet s		-	Resource Group *		
Licensing Confirm See Name Cloud Connectivity Br-eastus Cloud Direct Azure Azure Virtual WAN Automated Azure Deployment	Mobile Broadband					p1	~
Cloud Connectivity C Cloud Direct Azure C Virtual WAN Automated Azure Deployment	Licensing						
Azure Virtual WAN Automated Azure Deployment	Cloud Connectivity	~			Br-eastus		
Automated Azure Deployment		~					
	Automated Azure	Deployment					

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

NOTE:

To add a site, the resource group must be empty.

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

Create a resource group	×
Resource group * resource-group1	
Create	Cancel

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

NOTE:

Ensure that the site name maintains the SD-WAN site name requirements and is unique in the SD-WAN network.

The Azure VM name is generated from the site name in **AZ-regionname-sitename** format.

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

Introduction John Password Password Confirm Password Confirm Password	Basic Settings	Virtual Machine Settings		
Virtual Network	Virtual Machine Choose VM settings			
Summary confirm Virtual Machine Size * Standard_D3_v2	Virtual Network Choose VNet settings			
Standard_D3_v2	Summary Confirm			
		Standard_D3_v2		

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

NOTE:

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

Select	t a VM Size								
	VM SIZE	OFFERING 0	FAMILY 0	VCPUS 0	RAM (GB) 🗦	DATA DISKS 🔅	MAX IOPS 🔅	TEMPORARY S	PREMIUMDISK 🗘
	Standard_D3	Standard	General purp	4	14	16	16x500	200 GB	No
۲	Standard_D4	Standard	General purp	8	28	32	32x500	400 GB	No
	Standard_F16	Standard	Compute opti	16	32	64	64x500	256 GB	No
	Standard_F8	Standard	Compute opti	8	16	32	32x500	128 GB	No
						Showing 1 - 4 of	4 items Page	1 of 1	< ▶ ✓
							Selec	ct	Close

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

			Configuration		Administration				
Network Discovery	n	Configuration Basic Settir	/ Cloud Connectivity /						
Zero Touch Deployme Change Management		Virtual Mac	thine	Virtual Network*		×			Create Subnet
Appliance Settings		Virtual Net Choose VNet s	work	vnet1 (Resource vnet2 (Resource)	eGroup1)	¥			
Mobile Broadband Licensing		Summary Confirm		vnet3 (Resource vnet4 (Resource					
Cloud Connectivity	\sim			snet-lan - (10	0.0.1.0/24)	\sim			
Cloud Direct				WAN Subnet *					
Azure	\sim			snet-wan - (1	10.0.2.0/24)	\sim			
Virtual WAN				Route Table Name	•	Route Table Address Prefix *			
Automated Azure	e Deploymen	t							
Security	>								
							Close	Previous	

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

Create Virtual Network	\times
Name *	
VirtualNetwork1	
Address Space *	
10.1.0.0/16	
Subnet Name *	
VirtualSubnet1	
Subnet Address Space *	
10.1.0.0/24	
Create Ca	ncel

6. Select a subnet for management.

Dashboard	Fault	Monitoring	Configuration	Reporting	Administration	Nitro API		
Network Discovery			/ Cloud Connectivity /					
Network Configuratio		Basic Settir Virtual Mag	-	Virtual Network*	ork Settings			Create Subn
Change Managemen	t	Choose VM se	ttings	vnet1 (Resou	rceGroup1) Address Space:10.0.0.0/16	~		
Appliance Settings Mobile Broadband		Virtual Net Choose VNet s		Management Subr	et* (10.0.0/24)	$\overline{\mathbf{v}}$		
Licensing		Summary Confirm		snet-mgmt - (1 snet-lan - (10.0		_		
Cloud Connectivity Cloud Direct	~			snet-wan - (10 subnet4 - (10.0				
Azure Virtual WAN	~			Choose a W/		Route Table Address Prefix *		
Automated Azur	e Deployment							
Security	>							
							Close F	Previous Next

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

Create Subnet		\times
Name*		
VirtualSubnet1		
Address Space *		
10.1.2.0/24		
Virtual network: vnet1		
Resource group: ResourceGroup1		
Create	Cancel	

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

NOTE:

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

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

Dashboard	ault	Monitoring	Configuration	Reporting A	dministration	Nitro API			
etwork Discovery		Configuration	/ Cloud Connectivity / A	zure / Automated Azure De	eployment				
twork Configuration		Basic Settir	ngs	Summary					
Zero Touch Deployment Virtual Machine					Basic Settings		Virtual Netwo	rk Settings	
ange Management		Choose VM settings		Resource Group	ResourceGroup1	Virtu	al Network	vnet1	
pliance Settings		Virtual Network Choose VNet settings Summary		Azure Region	eastus	Mana	agement Subnet Name	snet-mgmt	
obile Broadband				SD-WAN Version	10.2	Mana Prefix	agement Subnet Address	10.0.0/24	
ensing				Site Name	Br-eastus		subnet Name	snet-lan	
-		Confirm		Virt	ual Machine Settings		Subnet Address Prefix	10.0.1.0/24	
oud Connectivity	~			Username	John	WAN	Subnet Name	snet-wan	
loud Direct				Virtual Machine Size	Standard_D3_v2	WAN	Subnet Address Prefix	10.0.2.0/24	
zure	~					Rout	e Table Name	customertable	
Virtual WAN						Rout	e Address Prefix	20.1.0.0/16	
Automated Azure De	ployment								
curity	>								

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

Dashboard		Monitoring	Configuration	ŀ	Reporting		Nitro API							
Network Discovery		Configuration	/ Cloud Connectivity /	Azure	/ Automated Azure D	Deployment								
Network Configuration	n	SD-WAN dep	oloyment initiated succes	sfully. T	he deployment proce	ss could take few minutes	to complete. Click \	riew Status butto	on in the deployment list	page to know the stat	tus. X			
Zero Touch Deployment Basic Settings					Summary									
Change Management		Virtual Mac	hine			Basic Settings			Virtual Networ	k Settings				
Appliance Settings			Choose VM settings					ResourceGroup1		Virtual Net	work	vnet1		
Mobile Broadband			Virtual Network Choose VNet settings Summary								Managem	ent Subnet Name	snet-mgmt	
Licensing		Choose VNet s			SD-WAN Version	10.2			ent Subnet Address	10.0.0/24				
Cloud Connectivity	~				Summary Confirm			Br-eastus		Prefix LAN Subne	t Name	snet-lan		
Cloud Direct		Comm			Vir	tual Machine Setting	js	LAN Subne	et Address Prefix	10.0.1.0/24				
Azure	~				Username	John		WAN Subn	et Name	snet-wan				
Virtual WAN					Virtual Machine Size	standard_D3_v2		WAN Subr	et Address Prefix	10.0.2.0/24				
Automated Azure	Deployment							Route Tabl	e Name	customertable				
	Deployment							Route Add	ress Prefix	20.1.0.0/16				
Security	>													
										Close				

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

As part of the deployment:

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

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

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

Network Discovery	Configuration / Cloud Con	nectivity / Azure / /	Automated Azure Deplo	yment				
Network Configuration	Please make sure that the	single step upgrade fil	e (ctx-sdw-sw-xxxxxxxxx	zip) is uploaded in cha	nge management scre	en on the MCN.		×
Zero Touch Deployment	Add Site Sta	rt Stop	Pull Active Co	onfig Settin	gs View Sta	itus Refresi	h	
Change Management								
Appliance Settings	SITE NAME	VM NAME	VM SIZE	MANAGEMENT IP	RESOURCE GROUP ©	AZURE REGION	VNET 0	STATUS 0
Mobile Broadband	az5245	AZ-westus-az5245	Standard_D3_v2	<u>138.91.243.113</u>	SDC5245	West US	vnet2	Running/Configu
	az5247	AZ-westus-az5247	Standard_D3_v2	104.42.196.163	SDC5247	West US	vnetaaa	Running
Licensing								
Cloud Connectivity \checkmark								
Cloud Direct								
Azure 🗸								
Virtual WAN								
Automated Azure Deployment								
Security >								

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

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

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

Zero Touch Deployment

March 12, 2021

Note

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

- SD-WAN 110 Standard Edition
- SD-WAN 210 Standard Edition
- SD-WAN 410 Standard Edition
- SD-WAN 2100 Standard Edition
- SD-WAN 1000 Standard Edition (reimage required)
- SD-WAN 1000 Enterprise Edition (Premium Edition) (reimage required)
- SD-WAN 1100 Standard Edition
- SD-WAN 1100 Premium (Enterprise) Edition
- SD-WAN 2000 Standard Edition (reimage required)
- SD-WAN 2000 Enterprise Edition (Premium Edition(reimage required)
- SD-WAN AWS VPX instance

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

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

ZTD High-Level Architecture and Workflow

Data Center Site

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

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

Note

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

for Zero Touch Deployment.

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

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

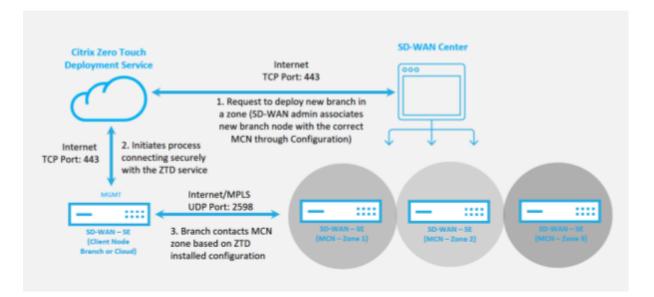
Remote Site

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

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

Note

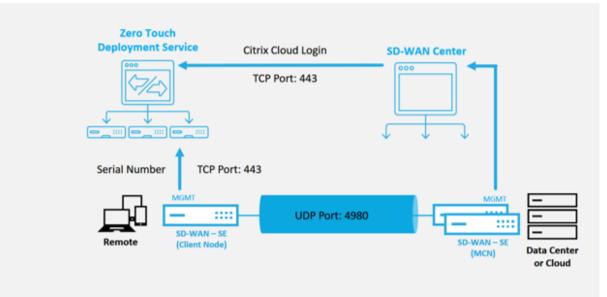
The interface layout is different each model, so please reference the documentation for identification of data and management ports.



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

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

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



Zero Touch Deployment Service Overview

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

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

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

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

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

The Zero Touch Deployment Cloud Service automates the following actions:

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

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

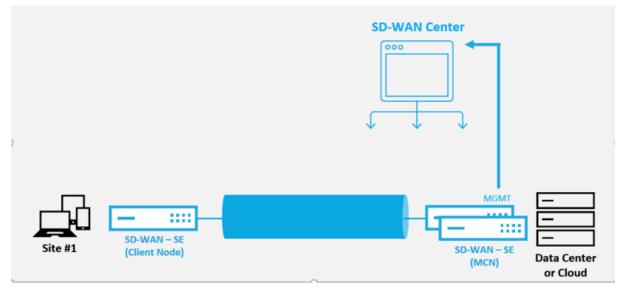
branch appliance.

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

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

Zero Touch Deployment Service Procedure

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



How to Configure Zero Touch Deployment Service

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

Configuration workflow:

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

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

To configure Zero Touch Deployment service:

- 1. Install SD-WAN Center with enabled Zero Touch Deployment capabilities.
 - a) Install SD-WAN Center with DHCP assigned IP address.
 - b) Verify that SD-WAN Center is assignment a proper management IP address and network DNS address with connectivity to the public internet across the management network.
 - c) Upgrade the SD-WAN Center to the latest SD-WAN software release version.
 - d) With proper internet connectivity, the SD-WAN Center initiates the Zero Touch Deployment (ZTD) Cloud Service and automatically download and install any firmware updates specific to ZTD, if this call home procedure fails the following Zero Touch Deployment option will not be available in the GUI.

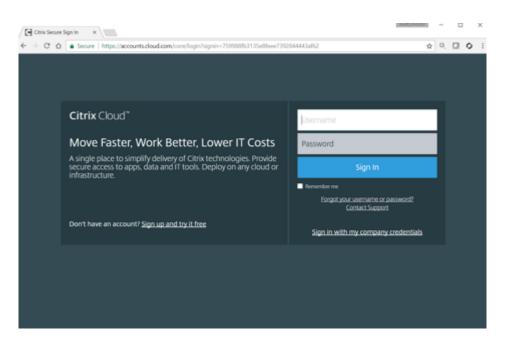
	Citrix SD-WAN	Center				R9_2_1_23_588434 ∽	admin 🗸
	Dashboard Fault	Monitoring	Configuration	Reporting	Administration		
	Network Discovery	Configuration / Zer	ro Touch Deployment				
6	Network Configuration	Zero Touch Deployment					
L	Zero Touch Deployment	Zero Touch Deployme	ent requires Login into Otrix	Workspace Cloud.			
	Change Management						
	Appliance Settings	Your participation in t	his Tech Preview, including y	our use case of Citrix Ze	ro Touch Deployment Services, is subject to your	acceptance of the [Citrix Terms of Service].	
		Login to Creix Workspa	t I have read and agree to th	e above Terms and Conc	leons.		

- e) Read the Terms and Conditions, and then select "I acknowledge that I have read and agree to the above Terms and Conditions."
- f) Click the "Login to Citrix Workspace Cloud" button if a Citrix Cloud account has already been created.
- g) Login into the Citrix Cloud account, and upon receiving the following message of successful login, PLEASE DO NOT CLOSE THIS WINDOW UP, THE PROCESS REQUIRES ANOTHER
 ~20 SECONDS FOR THE SD-WAN CENTER GUI TO BE REFRESHED. The window should close on its own when it is complete.**



- h) To create a Cloud Login account follow the below procedure:
 - Open a web browser to https://onboarding.cloud.com
 - Click on the link for "Wait, I have a Citrix.com account."

Creix Cloud ×	2	BARCER - D X "
← → C Secure https://onboarding.cloud.com		०. 🖈 🔍 🖬 🗄
	Citrix Cloud™	
	Sign Up Net Liber & Clincom account	
	Business Email Address	
.	First Name Last Name	
	Company Name	
	Phone Number	
	Address	
	Oli	
	USA •	
	AA •	
	Zip er Pestal Code	
	Ive read, understand and agree to the <u>literal of Sension</u>	
	Continue	
	Geriet Support	



- i) Sign-in with an existing Citrix account.
- j) Once logged into SD-WAN Center Zero Touch Deployment page, you may notice that no sites are available for ZTD deployment because of the following reasons:
 - The active configuration has not been selected from the Configuration drop-down menu
 - All the sites for the current active configuration have already been deployed
 - The configuration was not built using the SD-WAN Center, but rather the Configuration Editor available on the MCN
 - Sites were not built in the configuration referencing zero touch capable appliances (e.g. 410-SE, 2100-SE, Cloud VPX)
- 2. Update the configuration to add a **new remote** site with a **ZTD capable SD-WAN appliance** using SD-WAN Center Network Configuration.

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

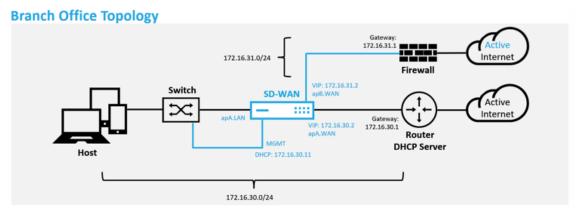
Design the new site for SD-WAN appliance deployment by first outlining the details of the new site (that is, Appliance Model, Interface Groups usage, Virtual IP Addresses, WAN Links with bandwidth and their respective Gateways).

Important

You may notice any site node that has VPX selected as the model is also listed, but currently ZTD support is only available for the AWS VPX instance.

Note

- Make sure that you are using a support web browser for Citrix SD-WAN Center
- Make sure the web browser is not blocking any pop-up windows during the Citrix Workspace Login



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

Note

The SD-WAN appliances automatably assign a default IP address of 192.168.100.1/16. With DHCP enabled by default, the DHCP Server in the network may provide the appliance a second IP address in a subnet that overlaps the default. This can possibly result in a routing issue on the appliance where the appliance may fail to connect to the ZTD Cloud Service. Configure the DHCP server to assign IP addresses outside of the range of 192.168.0.0/16.

There are various different deployment modes available for SD-WAN product placement in a network. In the above example, SD-WAN is being deployed as an overlay on top of existing networking infrastructure. For new sites, SD-WAN Administrators may choose to deploy the SD-WAN in Edge or Gateway Mode deployment, eliminating the need for a WAN edge router and firewall, and consolidating the network needs of edge routing and firewall onto the SD-WAN solution.

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

Citrix SD-WA	N Center		-	R9_2_1_23_588434 ~	admin 🗸
		Configuration	Reporting		
Network Discovery	Configuration / Net	work Configuration - SD-W	ANConfiguration		
Network Configuration				View Tutorial /	Citrix Support
Zero Touch Deployment	SD-WANConfiguration New Open., Save	Save As Import	Export_	Q Al * Global Actions *	8 0
Change Management				4	
Appliance Settings					
	Easic Advanced				
				G	
	View: Networ	k Sites			
	+ Site DC AWSBR AzureBR TweBR TweBR		0		

- b) Make sure a working configuration is already in place, or import the configuration from the MCN.
- c) Navigate to the Advanced tab to create a site.
- d) Open the Sites tile to display the currently configurated sites.
- e) Quickly built the configuration for the new site by utilizing the clone feature of any existing site.

SD-WANConfiguration New Open Save Save As Import Export
Basic Advanced
Global Sites + Add
DC AWSBR AzureBR TreBR D TreBR Clone
Connections
Optimization
Provisioning

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

te Name: ThiBR	Applianc EE100		Secure Keyi 752a7ebe58cdd9a6	
Name EnableD	efault 2			
Name VLAN ID NieR_Link1 0 NiBR_Link2 0	DHCP	Virtual IP Addresses Include Virtual Interfac ThBR_Link1 ThBR_Link2	 Virtual IP Address/Trafis 172.16.30.2/24 172.16.31.2/24 	
An Links Andrew Reventing Dar An Links And Links And Links Access Interfaces Include Access Interface Include ThIDR-Link2-Ai-1	WOAN Link Virtual Interface Vir	Access Type Public Internet teal IP Address Gateway 16.31.2 172.16.31.1		
ThiBR-Link1		Public Internet		
		tual IP Address Gateway 16.30.2 172.16.30.1		
Access Interfaces Include Interface Th/BR-Link1-Al-1				

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

Global			
Sites + Ad	d		
DC AWSBR AzureBR TenBR	0 @		
ThiBR (D 自 Settings)?		
	Appliance Name: EE1000 Model: CB1000	Secure Key: 548d734bda6d306d Mode: client	Regenerate
	Default Direct Route (5	Cost	
	Gateway ARP Timer (* 1000 Enable Source MA		
E Routi	on Domains	a and the	

- h) The SD-WAN model for the site can be updated, but do be aware that the Interface Groups may have to be redefined since the updated appliance may have a new interface layout then what was used to clone.
- i) Save the new configuration on SD-WAN Center, and use the export to the "**Change Management inbox**" option to push the configuration using Change Management.
- j) Follow the Change Management procedure to properly stage the new configuration, which makes the existing SD-WAN devices aware of the new site to be deployed via zero touch, you need to utilize the "Ignore Incomplete" option to skip attempting to push the configuration to the new site that still needs to go through the ZTD workflow.
- 3. Navigate back to the SD-WAN Center Zero Touch Deployment page, and with the new active configuration running, the new site is available for deployment.
 - a) In the Zero Touch Deployment page, under the **Deploy New Site** tab, select the running network configuration file
 - b) After the running configuration file is selected, the list of all the branch sites with undeployed SD-WAN devices that are supported for zero touch will be displayed

Buchboard Monitoring	Configuration		
+ Applance Settings	Configuration > Visual WMI > 4	Dange Management	
= Vrhuel INAN			
- View Configuration	Overview	Appliance Staging	0
Configuration Editor			
Change Management	Change Preparation	The prepared changes will now be distributed to all appliances in your network. To begin, click Stage Appliances. To stop the process at any time, click Albert.	
Restart/Reboot Network		Once the desired applications are explored, click New To continue to the Activate screen.	
- Enable Disable Purge Flows	Appliance Staging		
Dynamic Virtual Paths			
SD-WAN Center Certificates	Activation	Sandar Propess	
# System Maintenance		28% 27 Papelancan Related	
		0 / 313.35 Mityles hundrend	
		Stops Applances Root View Roomphree	ĩ

Citrix SD-WAI	N Center					R9_2_1_23_588434 ~	admin ~
Dashboard Fault	Monitoring	Configuration	Reporting	Administrati	on		
Network Discovery	Configuration / Zero	Touch Deployment / Dep	ploy New Site				
Network Configuration	Deploy New Site	Activation Histor	y Pending	Activation			
Zero Touch Deployment	Configuration: SD-WA	NConferration2					0
Change Management	Showing 1 - 1 of 1	Congustor.				Search	-
Appliance Settings		Site Name 🔺			Appliance Type	Enab	ie
	ThiBR			cb1000		6]

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

Deploy New Site	Activation History	Pending Act	ivation			
Configuration: SD-WANC	onfiguration2	•			arch	0
Showing 1.1 of 1	Site Name 🔺			Appliance Type	 Enable	1
ThiBR			cb1000			
Deploy						

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

Deploy New Site		×
Site Name:		
ThiBR		
Serial Number:		
SECONDALION.		
Street Address:		
123 Street Dr		
Installer Email:		
ztdinstaller@edicek.com		
Additional Notes:		
Installer, 1) Cable all WAN and LAN interfaces to mal and configuration built in earlier steps 2) Cable the management interface (MGMT	*	
	Deploy	Cancel

Note

The Serial Number entry field is optional and depending if it is populated or not, will result in a change in on-site activity the Installer is responsible for.

- If Serial Number field is populated The installer in not required to enter serial number into the activation URL generated with the deploy site command
- If Serial Number field is left black The installer will be responsible for entering in the correct serial number of the appliance into the activation URL generated with the deploy site command
- a) After clicking the **Deploy** button, a message will appear indicating that "The Site configuration has been deployed."
- b) This action triggers the SD-WAN Center, which was previously registered with the ZTD Cloud Service, to share the configuration of this particular site to be temporality stored in the ZTD Cloud Service.
- c) Navigate to the Pending Activation tab to confirm that the branch site information populated successfully and was put into a pending installer activity status.

Deploy New Site	Activation History	Pending Activation			
Showing 1 - 1 of 1				Search	
Showing to tot t					
Site Name	Sertal No	Installer Email	Address	Status	Action

Note

A zero touch deployment in the Pending Activation state can optionally be chosen to Delete or Modify, if information is incorrect. If a Site is deleted from the pending activation page, it becomes available to be deployed in the Deploy New Site tab page. Once you choose to delete the branch site from Pending activation, the activation link send to the installer becomes invalid.

If the Serial Number field was not populated by the SD-WAN Administrator, the Status Field indicates "Waiting for Installer" instead of "Connecting."

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

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

NetScaler SD-WAN Cloud Service Activation Link @ThiBR
Citrix Zero Touch Service <sdwanservice@citrix.com> Thu 5/1/2017 b47 PM To: ThuBR (ptelinstalier@outlook.com) #</sdwanservice@citrix.com>
Your NetScaler SD-WAN Appliance Activation Information for: ThiBR
Hello,
To activate your appliance please use the following URL: https://sdwanzt.citrixmetworkapl.net/root/sdwanzt/v1/appliance/activate?activationcode=3720fe46-fa1b-4662-bab1-#3bbd40d357
Installer Notes from the Admin: Installer, Please power and cable the appliance for internet.
Site Name: ThiBR
Address: 123 Street Dr
Cheers,
The team at Citrix Cloud Services

- b) Open the zero touch deployment Activation URL in an internet browser window.
- c) If the SD-WAN Administrator did not pre-populate the serial number in the deploy site step, then the Installer would be responsible for locating the serial number on the physical ap-

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

Zero Touch Deployment Service	Serial Number:		
		Activate	

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

Site Name: ThiBR				
wARNING: The operation	n is taking longer than usual. P	Applying Config lease check if the appl gured, perform a confi	Activated	
	WARNING: The operatio	Connecting Downloading Config WARNING: The operation is taking longer than usual P	0-0-0-0-0-	

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

Note

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

- 5. The next series of steps are automated with the help of the Zero Touch Deployment service, but requires that the following pre-requisites are available.
 - The branch appliance should be powered up
 - DHCP must be available in the existing network to assign management and DNS IP address
 - Any DHCP assigned IP address requires connectivity to the internet with ability to resolve FQDNs

- IP assignment can be configured manually, as long as the other pre-requisites are meet
- a) The appliance obtains an IP address from the networks DHCP Server, in this example topology this is achieved through the bypassed data interfaces of a factory default state appliance.

Power on NetScaler SD-WAN 172.16.31 172.16.31.0/24 Interne VIP: 172.16.31.2 Switch SD-WAN Activ Interne 172.16.30.2 172.16.30. Router DHCP Server Hos CP: 172.16.30.11 172.16.30.0/24

- b) As the appliance obtains the web management and DNS IP addresses from the underlay network DHCP Server, the appliance initiates the Zero Touch Deployment Service and download any ZTD related software updates.
- c) With successful connectivity to the ZTD Cloud Service, the deployment process automatically perform the following:
 - Download the Configuration File that is stored earlier by the SD-WAN Center
 - Applying the Configuration to the local appliance
 - Download and Install a temporary 10 MB license file
 - Download and Install any software updates if needed
 - Activate the SD-WAN Service



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

Dashboard Fault	Monitoring	Configuration	Reporting	g Administr	ation				
Network Discovery Configuration / Zero Touch Deployment / Activition History									
Network Configuration	Deploy New Site	Activation His	itory Pi	ending Activation					
Zero Touch Deployment	Showing 1 - 1 of 1						Search		
Change Management	Site Name 🔺	Serial No	Installer Email	Addres	s Status Details	Activation Date	Status	Action	
Appliance Settings	THBR	3F6P82j307	ztdinstaller@outioo	ak.com 123 Street Dr	Appliance Activated	May 11 22:18:03 2017 UTC	Activated		

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

Management IP Address: 172.16.10 Appliance Uptime: 3 weeks,	Configuration
Model: VPX Appliance Mode: MCN Serial Number: 1079975/ Management IP Address: 172.16.10 Appliance Uptime: 3 weeks, Service Uptime: 1 weeks, Routing Domain Enabled: Default J Local Version: 9.2.1.23.5884 Built On: Apr 21 2017 / Hardware Version: VPX OS Partition Version: 4.6 Virtual Path Service Status	
Appliance Mode: MCN Serial Number: 1079975 Management IP Address: 172.16.14 Appliance Uptime: 3 weeks, Service Uptime: 1 weeks, Routing Domain Enabled: Default F Local Versions Software Version: 9.2.1.23.5884 Built On: Apr 21 2017 a Hardware Version: VPX OS Partition Version: 4,6 Virtual Path Service Status Virtual Path DC-AWSBR:	
Serial Number: 1079975 Management IP Address: 172.16.11 Appliance Uptime: 3 weeks, Service Uptime: 1 weeks, Routing Domain Enabled: Default J Local Versions Software Version: 9.2.1.23.5884 Built On: Apr 21 2017 a Hardware Version: VPX OS Partition Version: 4.6 Virtual Path Service Status Virtual Path DC-AWSBR:	
Management IP Address: 172.16.11 Appliance Uptime: 3 weeks, Service Uptime: 1 weeks, Routing Domain Enabled: Default J Local Versions Software Version: 9.2.1.23.5884 Built On: Apr 21 2017 a Hardware Version: VPX OS Partition Version: 4,6 Virtual Path Service Status	
Appliance Uptime: 3 weeks, Service Uptime: 1 weeks, Routing Domain Enabled: Default J Local Versions Software Version: 9.2.1.23.5884 Built On: Apr 21 2017 a Hardware Version: VPX OS Partition Version: 4,6 Virtual Path Service Status	b-b067-ae77-1718-d7bdf0375a2b
Service Uptime: 1 weeks, Routing Domain Enabled: Default, F Local Versions Software Version: 9,2,1,23,5884 Built On: Apr 21 2017 a Hardware Version: VPX OS Partition Version: 4,6 Virtual Path Service Status Virtual Path DC-AWSBR:).51
Routing Domain Enabled: Default J Local Versions Software Version: 9.2.1.23.5884 Built On: Apr 21 2017 a Hardware Version: VPX OS Partition Version: 4,6 Virtual Path Service Status Virtual Path DC-AWSBR:	5 days, 22 hours, 45 minutes, 35.2 seconds
Local Versions Software Version: 9.2,1.23,5884 Built On: Apr 21 2017 a Hardware Version: VPX OS Partition Version: 4,6 Virtual Path Service Status Virtual Path DC-AWSBR:	2 days, 20 hours, 58 minutes, 57.0 seconds
Software Version: 9.2.1.23.5884 Built On: Apr 21 2017 a Hardware Version: VPX OS Partition Version: 4.6 Virtual Path Service Status Virtual Path DC-AWSBR:	loutingDomain
OS Partition Version: 4,6 Virtual Path Service Status	
Virtual Path Service Status	
Virtual Path DC-AWSBR:	
Virtual Path 'DC-AzureBR' is currently	Uptime: 1 hours, 12 minutes, 48.0 seconds.
LO LO LO DO TODO TODO LO	dead.
7	ead (Configuration version mismatch)
Virtual Path DC-FouBR' is currently of	

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

pliance Settings	Configuration () Virtual INNN ()	Change Manager	nenk							
tual INAN										
liev Configuration	Overview	Change	Process	Overview						
Configuration Editor	Change Preparation	The Char	or Managara	ant concess allows a coar-	to unload channel to the net	and whether it he a configuration	software or both. This three	stan workflow is a set of shee	de and processes	that encore that
Nampe Management			The Change Management process allows a user to upload changes to the network, whether it be a configuration, software, or both. This three-step workflow is a set of checks and processes that configuration changes and software updates are applied in a reliable, fail-safe way.							
nable Disable Purge Rows	Appliance Staging									
ynamic Virtual Paths	Activation									
D-WAN Center Certificates	Activition			Step 1		Step 2			Step 3	
stem Maintenance			0	hange Preparatio	•	Appliance St			Activation Activate Change	
					aurai	MACRA DE LA DELLA DE LA DELLA DE LA DELLA DE LA DELLA	Cliente			
		Cicking the		ed button will ship to the Ap	MCN pplanot Staging they, where you	MCN		MCN	U	Clients
		Closing the	Activate Stage	ed turten wil slip to the Ap paration Pilenames	pplanor Staging Higs, where you Active - 9x2-2TD-Ten/TweTI	a may switch to a previously-staged ap	plance package (Fpresent).	fguration.zip	6	citute Staped] [Begin
	Site Applance	Cicking the	Activate Stage	ed button will skip to the Ap paration Pilenames: C	Active - 9x2-210-SenflweTi arrently Active	a may solidy to a providually obspect ap holder/SAgure-DO-NOT-ALTER-dg Gam	plance package (F present). Staged - SD-WMVC and rently Staged	fguration.zip Traffic Inter	(A	tionic Staged [Begin
		Hadd	Activate Stop	ed button will skip to the Ap peration Pitenames: G Software	Active - \$42-270-TenflweT	n may solido to a previously staged ap hulkevSAzure: DC-NOT-ALTER.etg Cam Software	planet package IP presents Stagend - SD-WANKCent rently Stagend Counting	Iguration.zip Traffic Inter Expected	maption Actual	citute Staped [Begin Download Package
	DC-VPK	Blooded	Activate Stop	ed button will skip to the Ap paration Pilenames: G Software 9.2.1.23.508404	Active - 992-2710-TenTowT	to may solido to a previously obspect ap hollowise. DO-NOT ALTER.etg Com Software 8.2.1.2.3.00434	plance package if presents. Stapped - 50-WMAVCord result Stapped fact or S/11/17	figuration.zip Touffic.tote Expected <1 min.	Actual 198 ms	tione Staped [Bege Develope active / doped
	DC-VPX ANY58-ANY-ANY	Model Clurk Class	Activate Stop	ed button will skip to the Approximation Pilenames: 0 Software 9.2.1.23.588404 9.2.1.23.588404	Active - \$42-270-TenflweT	n may solido to a previously staged ap hulkevSAzure: DC-NOT-ALTER.etg Cam Software	planet package IP presents Stagend - SD-WANKCent rently Stagend Counting	figuration.zip figuration.zip	maption Actual	toure Staped Begin Deventional Package active / diaged active / diaged
	DC-VPX AVS88-ANS-ANS Apure\$8-Apure17M	Model CEURX CEURX CEURX CEURX	Activate Stop	ed botton will alige to the Ap paration Filenamest 0 Software 9.2.123.58604 9.2.123.58604 Not Connected	Active - 992-2710-TenTowT	to may solido to a previously obspect ap hollowise. DO-NOT ALTER.etg Com Software 8.2.1.2.3.00434	plance package if presents. Stapped - 50-WMAVCord result Stapped fact or 5/11/17	fguration.zip fguration.zip fguration.zip ct asis ct asis ise Org Mgt	Actual 198 ms	cloure Daged [Beger Deventional Package active / staged active / staged
	DC-VPR ANYSPEARS ANE ApureREApure VM PouRESSA10	Bloodel CBURK CBURK CBURK CBURK CBURK CBURK	Activate Stop	ed button vill skip to the Ap paration Fidenames: 0 Safhaure 0.2.122338434 9.2.122338434 9.2.122338434 9.2.122338434 9.2.122338434 9.2.122338434 9.2.122338434	Active - 992-2710-TenTowT	to may solido to a previously obspect ap hollowise DO-NOT ALTER.etg Com Software 8.2.1.2.508454	plance package if presents. Stapped - 50-WMAVCord result Stapped fact or 5/11/17	figuration.zip Traffic bits figuration.zip figurati	Actual 198 ms	cloure Dagest [Regen Deventioned Package active / stagest active / stagest active / stagest
	DC-VPX AVS88-ANS-ANS Apure\$8-Apure17M	Model CEURX CEURX CEURX CEURX	Activate Stop	ed botton will alige to the Ap paration Filenamest 0 Software 9.2.123.58604 9.2.123.58604 Not Connected	Active - 992-2710-TenTowT	to may solido to a previously obspect ap hollowise DO-NOT ALTER.etg Com Software 8.2.1.2.508454	plance package if presents. Stapped - 50-WMAVCord result Stapped fact or 5/11/17	fguration.zip fguration.zip fguration.zip ct asis ct asis ise Org Mgt	Actual 198 ms	cloure Daged [Beger Deventional Package active / staged active / staged

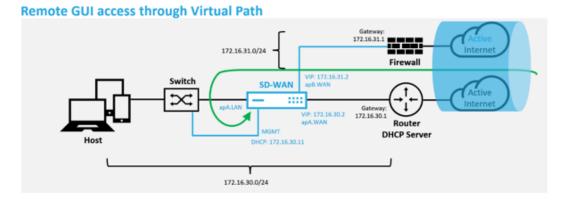
g) The SD-WAN Administrator can monitor the head-end MCN web management page for the established Virtual Paths of the remote site.

Statistics	Monitoring	> Statistics					
Flows							
Routing Protocols	Statistics	1					
Firewall	Show: Paths	s (Summary)	Enable Auto Refre	sh 5 seconds	Stop 🗹 Show late	st data. Processing	
IKE/IPsec							
IKE/IPsec Performance Reports	Path Stat	tistics Summary					
	Path Stat		Any column	• Apply			
Performance Reports			Any column	Apply			
Performance Reports Qos Reports			Any column To Link	Apply Path State	Virtual Pa	th Service State	
Performance Reports Qos Reports Usage Reports Availability Reports	Filter: Thi	in A			Virtual Pa GOOD	th Service State	Static
Performance Reports Qos Reports Usage Reports Availability Reports Appliance Reports	Filter: Thi	in A	To Link	Path State		th Service State	Static Static
Performance Reports Qos Reports Usage Reports Availability Reports	Filter: Thi Num *	in A From Link DC-A5	To Link Thi8R-Wifi	Path State GOOD	GOOD	th Service State	

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

Dashboard Fault	Mo	nitoring	Configura	tion Rep	porting	Administ	ration				
etwork Discovery	Config	puration / Netwo	rk Discovery	/ Inventory And Sta	atus						
etwork Configuration	55L	Certificate	Discovery	Settings	Inventor	ry And Status					
ero Touch Deployment											
hange Management											
ppliance Settings	Showing	:1-7of7								Search	
	e Poll A	State	Name	MGT IP Address	Model	Serial Number	Software	Registry Timestamp	Last Successful Poll	Latest Record	Downloa
	~	Stats in Sync	DC	172.16.10.51	cbvpx	1079975b- b067-ae77- 1718- d7bdf0375a2b	89,2,1,23,588434	1494551952	05/11/17 19:02	05/11/17 19:01	÷
		Unknown	AWSER								
		Not Reachable	AzureBR	192.168.202.4							
		Unknown	FouBR								
		Not Reachable	TenBR	192.168.10.11							
		Not Reachable	ThiBR	192.168.30.11							
		 Unknown 	TweBR								

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



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

Citrix SD-WAN Center 11.4

Dashboard	Monitoring Configuration	
Warning: Grace license insta Clear Warning	led. Please obtain license from Citrix license portal and install it.	×
System Status		
Name:	ThiBR	
Model:	1000	
Appliance Mode:	Client	
Serial Number:	3F6P8CMH9R	
Management IP Address	192.168.30.11	
Appliance Uptime:	20 minutes, 42.4 seconds	
Service Uptime:	19 minutes, 32.0 seconds	
Routing Domain Enable	t Default_RoutingDomain	
Local Versions		
Configuration Created C	m Fri May 12 01:19:12 2017	
Software Version:	9.2.1.23.588434	
Built On:	Apr 21 2017 at 04:42:14	
Hardware Version:	1000	
OS Partition Version:	4.6	
Virtual Path Service	Status	
Virtual Path DC-ThiBR U	ptime: 2 minutes, 49.0 seconds.	

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

Citrix SD-WAN Center 11.4

	Dashboard Monitoring	Configuration
	Warning: Grace license installed. Please obtain Clear Warning	license from Citrix license portal and install it.
(+ Appliance Settings	Configuration > Virtual WAN > View Configuration
	- Virtual WAN	
	- View Configuration	Configuration
	- Enable/Disable/Purge Flows - Dynamic Virtual Paths	View: Site •
	SD-WAN Center Certificates	Site Configuration
4.6		Site 4 = ThiBR Network Properties: Encryption Modewaes128 Encryption Modewaes128 Encryption Rekey is Enabled. Gateway ABP Timer (ms): 1000 Max dynamic virtual paths configured is 8. Routing Domains Enabled: Default_moutingDomain(ID: 0) Interface Group 0: Properties: secure zonewtrusted is overlaywtrue bypass modewfail_to_wire Ethernet Interfaces: apa.LAM, apa.LAWN Bridge Pairs: apa.LAM, apa.LAMN Bridge Pairs: apa.LAM, apa.LAMN Bridge Pairs: apa.LAMN

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

	Dashboard Monitoring	Configuration	
	Warning: Grace license installed. Please obtain liv Clear Warning	cense from Citrix license portal and	install it.
	- Appliance Settings	Configuration > Appliance Setti	ings > Licensing
	Administrator Interface Logging/Monitoring Network Adapters	License Status	
	- Net Flow - Net Flow	License Server Location:	Licensed Local 02c47a512af0
ч	Licensing	System Platform:	NetScaler SD-WAN 1000 Series
1	+ Virtual WAN	Model: Maximum Bandwidth (MAXBW):	1000VW-020 10 Mbps
ĺ	+ System Maintenance	Action Required: Maintenance Expiration Date:	N/A Grace license installed. Please obtain license from Citrix license portal and install it. N/A Sat May 27 02:48:57 2017
		License Configuration * Local © Remote Upload License for this Ap Filename: Choose File No fi	

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

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

On-prem zero touch

March 12, 2021

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

AWS

March 12, 2021

Deploying in AWS

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

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

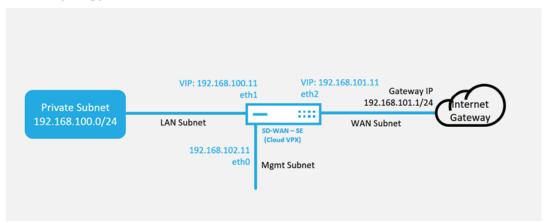
If the SD-WAN configuration was not built using the SD-WAN Center Network Configuration, import the active configuration from the MCN and begin modifying the configuration using SD-WAN Center. For Zero Touch Deployment capability, the SD-WAN Administrator must build the configuration using SD-WAN Center.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

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

Note

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

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



Cloud Topology with NetScaler SD-WAN

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

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

Citrix SD	-WA	N Center			R9_2_1_23_588434 v	admin 🗸
			Configuration	Reporting		
Network Discovery		Configuration / Net	twork Configuration - SD-W/	WConfiguration		
Network Configurat	tion				View Tutorial /	Citrix Support
Zero Touch Deploym	ent	SD-WWNConfiguration New Open Save	Save As Import	Eurort	Q All · Global Actions	. 8 0
Change Managemer	rt.	THE OPEN AND	and un-	Experiment in a	Que -	
Appliance Settings						
		Basic Advanced				
					C	2
		View: Networ	k Sites			
		Filter Sites				
		+ Site		0		
		DC				
		AWS8R Azure8R				
		Ten8R Twe8R				

- c) Make sure a working configuration is already in place, or import the configuration from the MCN.
- d) Navigate to the Basic tab to create a new site.

- e) Open the Sites tile to display the currently configured sites.
- f) Quickly built the configuration for the new cloud site by utilizing the clone feature of any existing site, or manually build a new site.

Basic Ac	lvanced		
View: Filter Sites:	Global	Sites	
+ Site DC AWS-SE Azure-SE Branch DavidS410 ZTDBR1000 ZTDBR2000 ZTDBR2100 ZTDBR410	0		

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

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

Citrix SD-WAN Center 11.4

	the following field	s and mak	e the appropriate	changes for th	e new Site	2.	
e Name:			Ap	pliance Name:			Secure Key:
WS-SE			A	WS-SE-CBVP	X		4a460b14f0228091
uting Domain	15						
Name	Enable.D)efault					
efault_Routing	gDomain 🖉						
tual Interfaces	5				Virtual I	P Addresses	
Name	VLAN ID	DHCP			Include	Virtual Interface	Virtual IP Address/Prefix
1Vlan0	0					E1Vlan0	192.168.100.11/2
2Vlan0	0				1	E2Vlan0	192.168.101.11/2
	Address Routing Do	mainGatew	vay				
	Address Routing Do	main Gatew WAN Li			Ad	ccess Type	
lude Network / AN Links Include Link	Address Routing Do			0		ccess Type lic Internet	
AN Links Include Link	WS-INET	WAN Li		U Virtual IP Ad	Pub		

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

	Edit Site Settings				×	
Basic Advanced	Appliance Name:		Model:			
	AWS-SE-CBVPX		CBVPXL •			
View: Global Site	Enable Site as Intermediate Node		CB400			
Filter Sites:	Enable Dynamic Virtual Paths		CB410			
			CB1000		_	
+ Site			CB2000		Cancel	
			CB2100			
DC AWS-SE		Appliance	CB4000		1	
AWS-SE D 1		AWS-SE-CB	CB4100			
Branch DavidS410		_	CB5100	_		
ZTDBR1000		Interfa es Ethernet Por	CBVPX		1 +	
ZTDBR2000 ZTDBR2100		Etherner Por	CBVPXL	ntru ted		
ZTDBR410		Ethernet Por		<mark>.11/2</mark> 4)		
			 Mode: Fail-to-Block , Tr VLANS: 0 (192.168.101 			

- i) Save the new configuration on SD-WAN Center, and use the export to the "**Change Man-agement inbox**" option to push the configuration using Change Management.
- j) Follow the Change Management procedure to properly stage the new configuration, which

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

Bushboard Musiforing	Configuration		
# Applance Settings	Configuration > Visual WMI > 4	Dange Matageneed	
- Vetual WAN			
Wex Configuration Configuration Editor	Overview	Appliance Staging The prepared duringst will now be distributed to all appliances in your network. To begin, click Stoge Appliances	•
Change Management Restart/Relocat Natwork	Change Preparation	To stop the process at any time, dick Abert.	
Enable/Disable/Purge Rows	Appliance Staging	Once the desired appliances are staged, slick Next to continue to the Activate sovern.	
Dynamic Virtual Paths SD-WAN Center Certificates	Activation	hundre Progress	
+ System Maintenance		28% 217 replaces fielded	
		0/3133 Mights kandered	
		Tops Appliances About 2 Ispace Incomplete	Next -

- 2. Navigate back to the SD-WAN Center Zero Touch Deployment page, and with the new active configuration running, the new site will be available for deployment.
 - a) In the Zero Touch Deployment page, under the **Deploy New Site** tab, select the running network configuration file.
 - b) After the running configuration file is selected, the list of all the branch sites with undeployed Citrix SD-WAN devices that are supported for zero touch will be displayed.

Citrix SD	-WAN	Center				R9_3_0_161_	612290 🗸
Dashboard		Monitoring	Configuration	Reporting	Administration		
Network Discovery		Configuration / Zero	Touch Deployment / Pr	epare New Site			
Network Configurat	ion	Prepare New Site	Activation Histo	ory Pendir	g Activation		
Zero Touch Deployn	nent	Configuration: OnPrem	Appliance-ZTDv5 🔻	1			
Change Manageme	nt	Showing 1 - 7 of 7					Search
Appliance Settings			Site Name 🔺			Appliance Type	Enable
		Azure-SE			cbvpxl		
		Branch			cbvpx		
		DavidS410			cb410		
		ZTDBR1000			cb1000		
		ZTDBR2000			cb2000		
		ZTDBR2100			cb2100		
		ZTDBR410			cb410		

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

Site Name 🔺	Appliance Type	Enable
AWS-SE	cbvpxl	
Azure-SE	cbvpxl	
Branch	cbvpx	
DavidS410	cb410	
ZTDBR1000	cb1000	
ZTDBR2000	cb2000	
ZTDBR2100	cb2100	
ZTDBR410	cb410	
Deploy Provision and Deploy		

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

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

Provision and Deploy	
Site Name:	
AWS-SE	
Installer Email:	
ztdinstaller@outlook.com	
Provision Type	
AWS	•

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

Provision and Deploy AWS				×
AWS Region				
US West (Oregon)	٠			
AWS Instance Size				
m4.2xlarge	•			
SSH Key Name:				
aws-ztd		0		
Role ARN:				
arn:aws:iam::******:role/ZeroTouch		0		
			Back	Deploy

Note

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

- f) Click **Deploy**, triggering the SD-WAN Center, which was previously registered with the ZTD Cloud Service, to share the configuration of this site to be temporality stored in the ZTD Cloud Service.
- g) Navigate to the **Pending Activation** tab to confirm that the site information populated successfully and was put into a provisioning status.

Prepare New Site	Activation History	Pending Activation			
Showing 1 - 1 of 1				Sear	ch
Site Name 🔥	Serial No	Installer Ema	II Address	Status	Action
NS-SE	2E20EFCF-1A26-42DC-86D0- 5624FD27C37F	ztdinstaller@outlook.c	om AWS - US West (Oregon)	Provisioning	

- 3. Initiate the Zero Touch Deployment process as the Cloud Admin.
 - a) The Installer will need to check the mailbox of the email address the SD-WAN Administrator used when deploying the site.

c	Citrix Zero Tou Today, 11:01 AM You &	uch Service <sdw< th=""><th>vanservice@citrix.com></th><th>^</th><th></th><th>Þ</th><th>Reply all</th><th>$$ \checkmark</th></sdw<>	vanservice@citrix.com>	^		Þ	Reply all	$ $ \checkmark
nbax								
		NetScaler SD	-WAN Appliance Activation Information					
			process of activating your appliance, <u>click here</u> . s URL into your browser					
			zt.citrixnetworkapi.net/root/sdwanzt/v1/applianc ==67940818-abb8-47f0-9f17-9a20a3955d57)	e/activate'	?			
		Site Name						
		Address	AWS - US West (Oregon)					
		Additional	Notes					
		The NetScale	r SD-WAN Team					
			*** This is an automatically generated email, please do not reply ***					

NetScaler SD-WAN Cloud Service Activation Link @AWS-SE

- b) Open the activation URL found in the email in an internet browser window.
- c) If the SSH Key and Role ARN are properly inputted, the Zero Touch Deployment Service will immediately start provisioning the SD-WAN instance, otherwise connections errors will immediately be displayed.



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

	dFormation	n 🛩 Stack							
				g StackSet et is a contain		/S CloudF	ormation stack	s and allows you to create staci	is across multiple AWS Accounts a
Create Star	x • A	ctions •	Design te	emplate					
Filter: Act	ve • By St	ack Name							
Stack	Name	Cre	ated Time		Statu	5		Description	
AWS-	se	201	7-08-18 17:5	7.331070-07	00 0054	TE COM			
					w chu	1 E_0000	ALC I C		
Overview	Outputs	Resources	Events	Template	Parameters	Tags	Stack Policy	Change Sets	
	Outputs	Resources			Parameters			Change Sets	Status reason
2017-08-18	Outputs		Events	Template	Parameters	Tags			Status reason
2017-08-18 17:50:57		Status	Events	Template Typ AW	Parameters	Tags		Logical ID	Status reason
2017-08-18 17:58:57 17:58:55	UTC-0700	Status CREATE_CON CREATE_CON CREATE_CON	Events APLETE APLETE APLETE	Template Typ AW AW	Parameters e rS. CloudFormati	Tags on Stack		Logical ID AWS-SE	Status reason
2017-08-18 17:58:57 17:58:55 17:58:53 17:58:51	UTC-0700 UTC-0700 UTC-0700 UTC-0700	Status CREATE_CON CREATE_CON CREATE_CON CREATE_CON	Events APLETE APLETE APLETE APLETE	Template Typ Ann Ann Ann Ann	Parameters H S. CloudFormati S. EC2. Instance S. EC2. EIPAsso S. EC2. EIPAsso S. EC2. EIPAsso	Tags on: Stack sciation sciation		Logical ID AWS-SE VpxInstance	Status reason
2017-08-18 17:58:55 17:58:53 17:58:53 17:58:51 17:58:39	UTC-0700 UTC-0700 UTC-0700 UTC-0700 UTC-0700	Status CREATE_COI CREATE_COI CREATE_COI CREATE_COI CREATE_IN_I	Events APLETE APLETE APLETE APLETE PROGRESS	Template Typ Ann Ann Ann Ann Ann Ann	Parameters e S. CloudFormatio S. EC2: Instance S. EC2: EIPAsso S. EC2: EIPAsso S. EC2: Instance	Tags on: Stack exclation sciation		Logical ID AWS-SE VpxInstance MgmtElpAssociation VanElpAssociation VpxInstance	Status reason Resource creation Initiated
2017-08-18 > 17:50:57 > 17:50:55 > 17:58:53 > 17:58:51 > 17:58:39 > 17:58:38	UTC-0700 UTC-0700 UTC-0700 UTC-0700 UTC-0700 UTC-0700	Status CREATE_COI CREATE_COI CREATE_COI CREATE_COI CREATE_IN_I CREATE_IN_I	Events APLETE APLETE APLETE APLETE PROGRESS	Template Typ Ann Ann Ann Ann Ann Ann Ann Ann	Parameters e S CloudFormati S EC2 Instance S EC2 EIPAsso S EC2 Instance S EC2 EIPAsso S EC2 EIPAsso S EC2 EIPAsso	Tags on: Stack control to the control to the contro		Logical ID AWS-SE Vpsinstance MgmtElpAssociation WamElpAssociation Vpsinstance MgmtElpAssociation	
2017-08-18 17:50:57 17:50:55 17:50:55 17:58:53 17:58:51 17:58:39 17:58:38 17:58:39 17:58:38 17:58:37	UTC-0700 UTC-0700 UTC-0700 UTC-0700 UTC-0700 UTC-0700 UTC-0700	Status CREATE_CON CREATE_CON CREATE_CON CREATE_CON CREATE_IN_J CREATE_IN_J CREATE_IN_J	Events APLETE APLETE APLETE APLETE PROGRESS PROGRESS	Template Typ Ann Ann Ann Ann Ann Ann Ann Ann Ann An	Parameters e S. CloudFormati S. EC2: Instance S. EC2: EIPAsso: S. EC2: EIPAsso:	Tags on:Stack controls control		Logical ID AWS-SE Vprinstance MgmtElpAssociation VanElpAssociation Vprinstance MgmtElpAssociation MgmtElpAssociation	Resource creation initiated
2017-08-18 17:50:57 17:50:55 17:50:55 17:58:53 17:58:51 17:58:39 17:58:38 17:58:39 17:58:37 17:50:37	UTC-0700 UTC-0700 UTC-0700 UTC-0700 UTC-0700 UTC-0700 UTC-0700 UTC-0700	Status CREATE_CO CREATE_CO CREATE_CO CREATE_NJ CREATE_NJ CREATE_NJ CREATE_NJ	Events APLETE APLETE APLETE PROGRESS PROGRESS	Template Typ Ann Ann Ann Ann Ann Ann Ann Ann Ann An	Parameters e S CloudFormat9 S EC2 Instance S EC2 EIPAsse S EC2 Instance	Tags on:Stack ciation ciation ciation ciation		Logical ID AWS-SE Vpsinstance MgmtEipAssociation Vpsinstance MgmtEipAssociation MgmtEipAssociation MgmtEipAssociation Vpsinstance	Resource creation Initiated Resource creation Initiated
2017-08-18 > 17:50:57 > 17:50:55 > 17:50:53 > 17:50:53 > 17:50:53 > 17:50:39 > 17:50:37 17:50:37 > 17:50:36	UTC-0700 UTC-0700 UTC-0700 UTC-0700 UTC-0700 UTC-0700 UTC-0700	Status CREATE_CON CREATE_CON CREATE_CON CREATE_CON CREATE_IN_J CREATE_IN_J CREATE_IN_J	Events APLETE APLETE APLETE APLETE PROGRESS PROGRESS PROGRESS	Template Typp Ann Ann Ann Ann Ann Ann Ann Ann Ann A	Parameters e S. CloudFormati S. EC2: Instance S. EC2: EIPAsso: S. EC2: EIPAsso:	Tags on:Stack ciation ciation ciation ciation ciation		Logical ID AWS-SE Vprinstance MgmtElpAssociation VanElpAssociation Vprinstance MgmtElpAssociation MgmtElpAssociation	Resource creation initiated

- e) Allow the provisioning process ~8-10 minutes and activation another ~3-5 minutes to fully complete.
- f) With successful connectivity of the SD-WAN cloud instance to the ZTD Cloud Service, the service will automatically perform the following:
 - Download the site-specific Configuration File that was stored earlier by the SD-WAN Center
 - Applying the Configuration to the local instance
 - Download and Install a temporary 10 MB license file
 - Download and Install any software updates if needed
 - Activate the SD-WAN Service



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

Dashboard Faul	t Monitoring	Configuration	Reporting	Administration				
	Configuration / 7	ero Touch Deployment /	Activation History					
letwork Discovery			,					
letwork Configuration	Prepare New Site	Activation His	story Pending /	Activation				
ero Touch Deployment								
hange Management	Showing 1 - 1 of 1						Search	
and ge management	Site Name 🔥	Serial No	Installer Email	Address	Status Details	Activation Date	Status	Action
oppliance Settings	AWS-SE	2E20EFCF-1A26-42DC- 86D0-5624FD27C37F	ztdinstaller@outlook.com	AWS - US West (Oregon)	Appliance Activated	Aug 19 01:16:55 2017 UTC	Activated	

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

Dashboard	Monitoring Configu	ration
System Status		
Name:	DC	
Model:	VPX	
Appliance Mode:	MCN	
Serial Number:	b536a38c-5f48-b720-4f8	d-b3f50b23f69f
Management IP Add	ress: 172.16.10.30	
Appliance Uptime:	1 weeks, 2 days, 3 hours,	50 minutes, 18.3 seconds
Service Uptime:	1 weeks, 2 days, 3 hours,	42 minutes, 19.0 seconds
Routing Domain Ena	bled: Default_RoutingDomain	
Built On: Hardware Version: OS Partition Version:		
	ice Status	
Virtual Path Serv		
	ch:	Uptime: 1 days, 1 hours, 1 minutes, 12.0 seconds
Virtual Path DC-Brar	ch: idS410' is currently dead.	Uptime: 1 days, 1 hours, 1 minutes, 12.0 seconds.
Virtual Path DC-Brar	idS410' is currently dead.	Uptime: 1 days, 1 hours, 1 minutes, 12.0 seconds. Uptime: 1 days, 1 hours, 1 minutes, 12.0 seconds.
Virtual Path DC-Brar Virtual Path 'DC-Dav Virtual Path DC-ZTD	idS410' is currently dead.	
Virtual Path DC-Brar Virtual Path 'DC-Dav Virtual Path DC-ZTD Virtual Path 'DC-ZTE	idS410' is currently dead. BR1000:	
Virtual Path 'DC-Dav Virtual Path DC-ZTD Virtual Path 'DC-ZTD Virtual Path 'DC-ZTD Virtual Path 'DC-ZTD	idS410' is currently dead. BR1000: BR2000' is currently dead.	Uptime: 1 days, 1 hours, 1 minutes, 12.0 seconds.

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

Citrix SD-WAN Center 11.4

Dashboard Monitoring					
+ Appliance Settings	Configuration > Virtual WAN >	Change Management			
Virtual WAN					
View Configuration Configuration Editor	Overview	Change Process	Overview		
Change Management	Change Preparation			ser to upload changes to	
 Change Management Settings Restart/Reboot Network 	Appliance Staging	processes that ensure	hat configuration cha	nges and software updat	tes are applied in a relia
 Enable/Disable/Purge Flows Dynamic Virtual Paths 	Activation		Step 1		Ste
SD-WAN Center Certificates			ige Preparation bload Files to MCN	1	Applian Transfer Fil
+ System Maintenance				MCN	
		Clicking the Activate Stag	ed button will skip to th	e Appliance Staging step, w	
	Search	Configur	ation Filenames:	Active - OnPremApplia	ance-ZTDv5.zip St
		-		Active - OnPremApplia	ance-ZTDv5.zip St
	Search Site-Appliance	Configur Model State			
		-	Curr	ently Active	Cur
	Site-Appliance	Model State	Curr	ently Active Config	Cur Software
	Site-Appliance	Model State CBVPX	Curr Software 9.3.0.161.612290	ently Active Config	Curi

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

Statistics	Monitoring >	Statistics									
Flows Routing Protocols	Statistics										
Firewall	Show: Paths (Si	mmary)	 Enable Auto R 	efresh 5 • seco	nds Start 🖉 Show latest data.						
IKE/IPsec											
Performance Reports	Path Statist	cs Summary									
Performance Reports Qos Reports	Filter: AWS		Any column	 Apply 						Sho	ow 100 ▼ ent
	Filter: AWS	in	Any column								
Qos Reports	Filter: AWS			Apply Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	Sho	
Qos Reports Usage Reports	Filter: AWS	in	Any column		Virtual Path Service State	Virtual Path Service Type Static	BOWT 26	Jitter (mS)	Loss %		W 100 • ent Congestion

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

	Dashboard Monit	toring	Configuration							
	Warning: Grace license installed. Please obtain license from Citrix license portal and install it. X Clear Warning									
<	Statistics	Monitorin	g > Statistics							
	Flows									
	Routing Protocols	Statisti	cs							
	Firewall	Show: AR	>	• Enabl	le Auto Refresh 5 🔹	seconds Refresh				
	IKE/IPsec									
	Performance Reports	ARP St								
	Qos Reports	Gateway AR	P Timer: 1000 ms							
	Usage Reports	Filten	ir	Any column	 Apply 					
	Availability Reports	Show 100	entries Showing	ng 1 to 2 of 2 en	tries			First Previous 1 Next Last		
	Appliance Reports	Num 🔺	Interface	VLAN	IP Addr	MAC Addr	State	Reply Age(mS)		
	DHCP Server/Relay	1	1	0	192.168.100.1	06:83:d9:d7:a8:02	READY_INACTIVE	19174		
		2	2	0	192.168.101.1	06:e3:b3:cb:bb:14	READY_ACTIVE	104		
		Showing 1 to	o 2 of 2 entries					First Previous 1 Next Last		

Azure

March 12, 2021

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

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

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

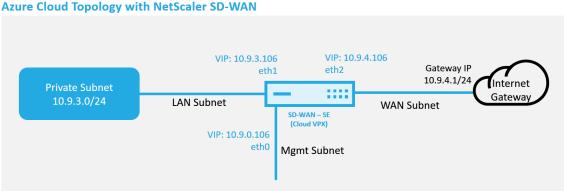
1. Design the new site for SD-WAN cloud deployment by first outlining the details of the new site (i.e. VPX size, Interface Groups usage, Virtual IP Addresses, WAN Link(s) with bandwidth and their respective Gateways).

Note

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

and WAN (in that order).

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



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

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

Citrix SD-WA	N Center		•		R9_3_1_35_624646 ∨	admin ∨
	t Monitoring	Configuration	Reporting	Administration		
Network Discovery Network Configuration Zero Touch Deployment Change Management Appliance Settings	OnPremAppliance-ZTD_MRS New Open Save	work Configuration - OnPre	mAppliance-ZTD_MRS		View Tutorial / C Q All V Global Actions V	itrix Support
	Basic Advanced Global Sites + Add DC Branch ZTDAWS Connections Optimization Provisioning Provisioning		0 0 0 0 0 0 0 0 0	Netv + Weahington Mortana Oregon Idaho Wyoming Nevada Ltan Colorado	North Dakota Minnesola Weconsin Minnesola Weconsin Minnesola Weconsin Missouri Kansas Missouri Ter	

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

± -
Basic Advanced
View: Global Sites Filter Sites:
+ Site (7) DC Branch ZTDAWS

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

Keep in mind that the template available for Azure cloud ZTD deployments is currently hardset to obtain the 10.9.4.106 IP for the WAN, 10.9.3.106 IP for the LAN, and 10.9.0.16 IP for the Management address. If the configuration is not set to match the expected VIP address for each interface, then the device will not be able to properly establish ARP to the cloud environment gateways and IP connectivity to the Virtual Path of the MCN. It is import that the site name be compliant with what Azure expects. The site name must be in all lower case, at least 6 characters, with no special characters, it must confirm to the following regular expression **^[a-z][a-z0-9-]{1,61}[a-z0-9]\$.**

	e review the f	following field:	s and m	ake the appropriat	e changes for	the new Site.			
e Na	ime:			A	ppliance Nam	ie:		Secure Key:	
daz	ure				azure-CBVPX	(L		f6796bba4d1c8da2	
uting	g Domains								
	Name	EnableD							
fau	lt_RoutingDo	main 🗹	I.						
Jal	Interfaces					Virtual IP	Addresses		
	Name	VLAN ID	DHCP			Include	Virtual Interface	Virtual IP Address/Prefix	
Vla	an0	0					E1Vlan0	10.9.3.106/24	
Vla	an0	0				√	E2Vlan0	10.9.4.106/24	
_	inks								
I	nclude Link	e-INET	WAN	Link			cess Type		
1	nclude Link	e-INET	WAN	Link			cess Type		
I	Access Inter	faces				Publi	ic Internet		
I	Access Inter	faces Access Interfac	e	Virtual Interface	Virtual IP	Publi	Gateway		
_	Access Inter	faces	e		Virtual IP 10.9.4.106	Publi	ic Internet		
1	Access Inter	faces Access Interfac	e	Virtual Interface		Publi	Gateway		
	Access Inter	faces Access Interfac	e	Virtual Interface		Publi	Gateway		
	Access Inter Include Interface Maximum Access Inter Include Interface Az	faces Access Interfac	E	Virtual Interface 2Vlan0		Publi	Gateway		

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

Edit Site Settings			×
Appliance Name:		Model:	
azure-CBVPXL		CBVPXL V	
Enable Site as Intermediate Node		CB400	
Enable Dynamic Virtual Paths		CB410	
		CB1000	Grand
		CB2000	Apply Cancel
		CB2100	
	Appliance azure-CBVP		/
		CB4100	
	Interface	CB5100	/ +
	Ethernet Fo	CBVPX	
		CBVPXL	sted

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

Appliance Staging		0					
The prepared changes will now be distributed to all appliances in your network. To stop the process at any time, click Abort . Once the desired appliances are staged, click Next to continue to the Activate screen.							
40% 2/5 appliances finished							
0.04 / 213.19 Mbytes transferred							
Prepare Packages	Stage Packages	Done					
Ø							
	Abort Ignore Incomplete	Next →					
	The prepared changes will now be distribute To stop the process at any time, click Abort . Once the desired appliances are staged, click Transfer Progress: 40% 2 / 5 appliances finished 0.04 / 213.19 Mbytes transferred	The prepared changes will now be distributed to all appliances in your network. To stop the process at any time, click Abort. Once the desired appliances are staged, click Next to continue to the Activate screen. Transfer Progress: 40% 2 / 5 appliances finished 0.04 / 213.19 Mbytes transferred Prepare Packages Stage Packages					

Configuration Filenames: Active - OnPremAppliance-ZTD_MR4_1.zip Staged - OnPremAppliance-ZTD_MR4_1.zip

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

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

Citrix SD-WAN	itrix SD-WAN Center							admin ∨
Dashboard Fault	Monitoring	Configuration	Reporting	Administration				
Network Discovery	Configuration / Zero	Touch Deployment / Pr	epare New Site					
Network Configuration	Prepare New Site	Activation Hist	ory Pending	Activation				
Zero Touch Deployment Change Management	Configuration OnPrem Showing 1 - 3 of 3	Appliance-ZTD_MR5 🔻					Search	0
Appliance Settings		Site Name 🔺			Appliance Type		Enable	
	Branch			cbvpx				
	ZTDAWS			cbvpxl				
	ztdazure			cbvpxl				
	Deploy Provision and	Deploy						

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

Configuration / Zero Touch Deployment / Prepare New Site							
Prepare New Site Activation History		Pending Activation					
Configuration: OnPremAppliance-ZTD_MR5 Showing 1 - 3 of 3 Search							
	Site Name 🔺		Appliance Type	Enable			
Branch		cbvpx					
TDAWS		cbvpxl					
tdazure		cbvpxl					
Deploy Provision and Dep	loy						

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

Provision and Deploy		
Site Name:		
ztdazure		
Installer Email:		
ztdinstaller@outlook.com		
Provision Type		
AZURE	•	

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

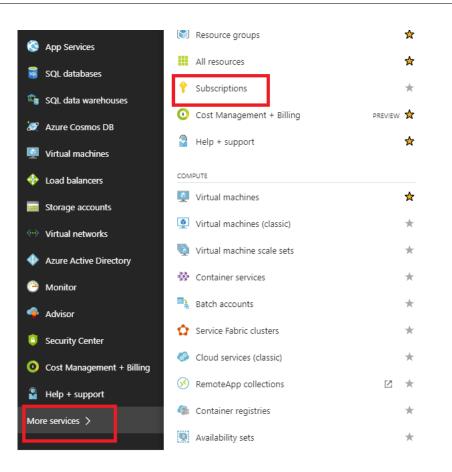
Copy and paste each required field after obtaining the information from your Azure account. The steps below outline how to obtain the required Subscription ID, Application ID, Secret Key, and Tenant ID from your Azure account, then proceed by clicking **Next**.

1

Provision and Deploy Azure (step 1 of 2)	
Subscription ID:	
52dd5bd9-2671-4cd3-8029-0f7d68108d53	
Application ID:	
2382ebde-09b4-4ec8-9098-0bdd6e113a54	
Secret Key:	
om5RZX9bY2T+GzJbP0qoCgtm1fBEMS	
Tenant ID:	
335836de-42ef-43a2-b145-348c2ee9ca5b	
SSH Public Key:	
ssh-rsa	
AAAAB3NzaC1vc2EAAAABJQAAAQEAm9l2mEuhPLsVINVh+ s2piG3uv2lshYlBaE4nH3y3lazetEhhl6Ng4rAf+LPSoZcBJLHh3	
nAEAJmcyJTfwmt61Yd4y339ciasEDmPEWEzgcyFGaQ0i/DFi	
Back Next	

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

Citrix SD-WAN Center 11.4



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

	(/	citri _{Azure}	x systems inc App regist Active Directory	trations			
+	New	0	Overview	📥 New appl	lication registration	Endpoints	🗙 Troubleshoot
12	Dashboard	1 1	Quick start	To view and n	nanage your registrat	ions for converged	applications, plea
	All resources	MAN	AGE	Search by n	ame or Appld		
(*)	Resource groups	x ^Q	Users and groups				
۲	App Services	15	Enterprise applications	DISPLAY			APPLICATION TYPE
) \$	SQL databases		Devices (Preview)	CA	casonboarding	701 4401 -004 -11	Web app / API
i Regionale de la composición	SQL data warehouses	15	App registrations		citrix-xd-61cb4ba6-		
2	Azure Cosmos DB	18	Application proxy	SH	shashispahd1	SunDymoloidi IP:	Web app / API
	Virtual machines	Å	Licenses		ANZSEEBC(Old)		Web app / API
	Load balancers	•	Azure AD Connect	XM	xm-devops1-cloudo	ips	Web app / API
	Storage accounts		Domain names	ci	citrix-xd-26e05661-		
<>	Virtual networks	٢	Mobility (MDM and MAM)	WE	WebApp-contosoev		
× 77			Company branding	сі	CitrixCloudStein		Web app / API
*	Azure Active Directory	¢	User settings	XM	XM-EMS-UiTestVaul	tAccess	Web app / API
0	Monitor	111	Properties		- 0400 F		

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

	×
~	
~	
~	

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

sdwanztd Registered app	* >
🏟 Settings 💉 Manifest 🗴 🛱	elete
Essentials 🔨	
Display name sdwanztd	Application ID 2382ebde-09b4-4ec8-9098-0bdd6e113a54
Application type Web app / API	ರಶ್ರಕರ್ d3c4eec8-94d8-4641-8cc3-f7022658cb48
Home page https://citrix.com	Managed application in local directory sdwanztd
	All settings →

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

sdwanztd Registered app	* X	Settings	×	Required permissions		□ ×
🌣 Settings 💉 Manifest 📋 I	Delete			🛨 Add 🕩 Grant Permissions		
Essentials ^		GENERAL		API	APPLICATION PERMIS	DELEGATED PERMISSI
Display name sdwanztd Application type	Application ID 2382ebde-09b4-4ec8-9098-0bdd6e113a54 Object ID	Properties	>	Windows Azure Active Directory (Microsoft Azure Act	0	1
Web app / API	d3c4eec8-94d8-4641-8cc3-f7022658cb48	🖂 Reply URLs	>			
Home page https://citrix.com	Managed application in local directory sdwanztd	2 Owners	>			
	All settings →	API ACCESS				
		Required permissions	>			
		💡 Keys	>			
		TROUBLESHOOTING + SUPPORT				
		🗙 Troubleshoot	>			
		New support request	>			

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

Citrix SD-WAN Center 11.4

Add API access	×	Select an API	□ ×
Select an API >		Search for other applications with Service Principal name	~
		Windows Azure Active Directory (Microsoft Azure Active Directory)	
2 Select permissions		Office 365 Exchange Online (Microsoft.Exchange)	
	_	Microsoft Graph	
		Office 365 SharePoint Online (Microsoft.SharePoint)	
		Office Hive	
		Skype for Business Online (MicrosoftLync)	
		Office 365 Yammer (Microsoft YammerEnterprise)	
		Power BI Service (Microsoft.Azure.AnalysisServices)	
		Microsoft Rights Management Services (Microsoft.Azure.RMS)	
		Microsoft Intune API (MicrosoftIntuneAPI)	
		Azure Key Vault	
		Windows Azure Service Management API	
		Azure Data Lake	
		Office 365 Management APIs	
		OneNote	
		Microsoft Visual Studio Team Services (Microsoft Visual Studio Online)	

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

Add API access	×	Enable Access	□ ×
1 Select an API Windows Azure Service Manag •		APPLICATION PERMISSIONS ⁺ + REQUIRES ADMIN No application permissions available.	τţ
2 Select permissions > O role, 1 scope		DELEGATED PERMISSIONS T+ REQUIRES ADMIN Access Azure Service Management as organization users (preview) O No	↑↓
Done		Select	

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

s inc App registrations 🚿 sdwanz	ztd > Setting	s > Keys			
Settings	×	Keys			
♀ Filter settings		R Save X Discar	d		
GENERAL		DESCRIPTION	EXPIRES		VALUE
Properties	>	key1	✓ In 1 y	ear 🗸	Value will be disp.
📒 Reply URLs	>		Durat	ion	
			In 1 y	ear	
🔛 Owners	>		In 2 y	ears	
API ACCESS			Neve	r expires	
品 Required permissions	>				
💡 Keys	>				
TROUBLESHOOTING + SUPPORT					
🗙 Troubleshoot	>				
New support request	>				

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

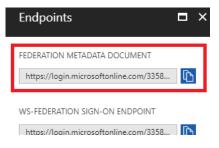
Keys			
R Save X Discard			
Copy the key value.	You won't be able to retriev	re after you leave this blade.	
DESCRIPTION	EXPIRES	VALUE	
key1	10/10/2018	om5RZX9bY2T+GzJbP0qoCgtm1fBEMS36ogK5nAWbd4M=	
Key description	Duration	✓ Value will be displayed on save	

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

citrix systems inc App regis	strations
Overview	
🥳 Quick start	To view and manage your registrations for converged applications, please visit the Microsoft Application Cons
MANAGE	sdwan
g ^R Users and groups	DISPLAY NAME
Enterprise applications	5D sdwan-report-api
Devices (Preview)	sp sdwan-report-svc
App registrations	SD sdwanztd
Application proxy	

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

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

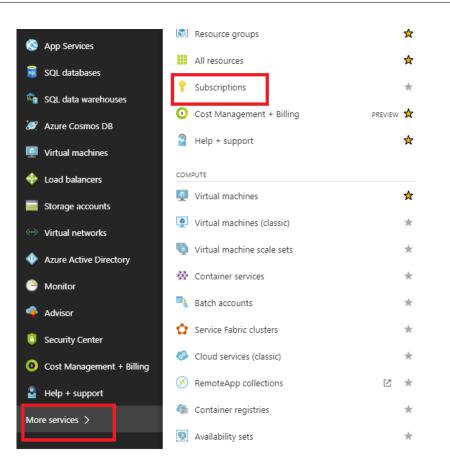


 The last item required is the SSH Public Key. This can be created using Putty Key Generator or ssh-keygen and will be utilized for authentication, eliminating the need for passwords to log in. The SSH public key can be copied (including the heading ssh-rsa and trailing rsa-key strings). This public key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

PuTTY Key Generator				\times
File Key Conversions	Help			
Key Public key for pasting in	to OpenSSH authorize	d keys file:		
+s2piG3uv2lshYlBaE4 +LPSoZcBJLHh3nAE4 RXN3dUnw4s96zV7k7	nH3y3lazetEhhl6Ng4rA AJmcyJTfwmt61Yd4y33 /KWOc0qv/17WyUHqw	EAm912mFuhPLsVINVh f 9ciasEDmPEWEzqcyF0 w4psHm7UfmM+8XPoX S5rYhqNKeCyMzK75j0lq	GaQ0i/DFjROvdM (hbTzF8px	^
Key fingerprint:	ssh-rsa 2048 04:c6:35:	6b:13:ba:7d:0d:4e:15:4e	e:f3:aa:04:b6:a9	
Key comment:	rsa-key-20171010			
Key passphrase:				
Confirm passphrase:				
Actions				
Generate a public/priva	te key pair		Generate	
Load an existing private	e key file	[Load	
Save the generated key	/	Save public key	Save private key	y
Parameters				
Type of key to generate	e: OSA OECDS	GA OED25519	SSH-1 (RS	SA)
Number of bits in a gen	erated key:		2048	

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

Citrix SD-WAN Center 11.4



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

Subscriptions * X Citrix Systems Inc.	Pay-As-You-Go - Access con Subscription	ntrol (IAM)	
🕂 Add		🕂 Add 🟛 Remove 🔹 Roles	🖔 Refresh 🛛 ? Help
My role Status T selected Sel	Overview Access control (IAM) Diagnose and solve problems COST MANAGEMENT + BILLING Invoices	Name 0 Search by name or email 1 items (1 Users) NAME OWNER	Type

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

Role		
Owner		~
Assign acce	55 10 0	
Azure AD	user, group, or application	~
Select 🛛 ztd		~
	mbx_ztduser	
МВ	mbx_ztduser@citrite.net	
	mbx_ztduser@citrite.net	
Selected me	mbx_ztduser@citrite.net	Remove
	mbx_ztduser@citrite.net	Remove
	mbx_ztduser@citrite.net	Remove
	mbx_ztduser@citrite.net	Remove

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

Azure Authentication Failure	×
Access is denied	
	Back

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

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

Provision and Deploy Azu	(step 2 of 2)	×
Azure Region		
West US	•	
Azure Instance Size		
Standard_D4_v2	•	
WAN subnet address prefix:		
10.9.4.0/24		
LAN subnet address prefix:		
10.9.3.0/24		
Management subnet prefix:		
10.9.0.0/24		

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

Citrix SD-WA	N Center	R9_3_1_35_624646 ∨	admin ∨				
		Configuration					
Network Discovery	Configuration / Zero	Touch Deployment / Pending	Activation				
Network Configuration	Prepare New Site	Activation History	Pendi	ng Activation			
Zero Touch Deployment Change Management	Showing 1 - 1 of 1					Search	
change Management	Site Name 🥆	Serial No		Installer Email	Address	Status	Action
Appliance Settings	ztdazure	B0F20EC1-9DEE-4902-B07 D593536C6C02	2-	ztdinstaller@outlook.com	AZURE - West US 2	Provisioning	
	Delete Modify						

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

Focused Other Filter -	NetScaler SD-WAN Cloud Service Activation Link @uswestazure	
NetScaler SD-WAN Team NetScaler SD-WAN Cloud Service A 3:44 PM NetScaler SD-WAN Appliance Activation Info	NT NetScaler SD-WAN Team <sdwanservice@citrix.com> Today, 3:44 PM You ¥</sdwanservice@citrix.com>	<u>∧</u> ■ ■ \$ ∨
	converse in the second s	
	NetScaler SD-WAN Appliance Activation Information	
	To check the activation statu <mark>s, click here</mark> (Or copy and paste this link into your Browser's address bar https://sdwanzt.citrixnetworkapi.net/root/sdwanzt/v1/appliance/activate? activationcode=4f19b443-7e89-4b59-9872-0f7ebeaa8ac2).	
	Site Name uswestazure Address AZURE - West US	
	Additional Notes The NetScaler SD-WAN Team	
	••• This is an automatically generated email, please do not reply •••	

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

Zero Touch Deployment Service	
Site Name: ztdazure	
Appliance provisioning	
Connecting	Pending
Downloading config	Pending
Downloading software	Pending
Installing software	Pending
Applying config	Pending
Activating	Pending

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

≡	Resource groups	× NetScalerSDWAN-ztdazur	e - Activity log					
- New	🕂 Add 🌒 Assign Tags 🛛 🚥 More		≣≣ Columns ↑ Export 🔗	Log Analytics	Operation log	g (classic)		
Dashboard	Subscriptions: Pay-As-You-Go	(C) Overview	Select query 🗸 🗜			Last 24 hours): outage notifica	1 failed deployment 0 role as	signments 1 error
All resources	Filter by name			ource group 0	Resource	0	Resource type 0	Operation 0
	1 items	Activity log		etScalerSDWAN-z.			All resource types	
Resource groups	NAME 14	Access control (IAM)		nt category 0 Il categories	 Event s 4 select 	severity 🖲	Event initiated by 0	Search 🖲
App Services	(NetScalerSDWAN-ztdazure ····	I Tags	Apply Reset	coregones				•
SQL databases		SETTINGS	Query returned 10 items. Click her	re to download all	the items as csv.			
SQL data warehouses		📣 Quickstart	OPERATION NAME	STATUS TI	ME TI	ME STAMP	SUBSCRIPTION	EVENT INITIATED BY
Azure Cosmos DB		Resource costs	▼ 🚯 Purchase	Succeeded Ju	ust now Fr	ri Oct 13 20	Pay-As-You-Go	ztd
Virtual machines		Deployments	Write Deployments	Succeeded 5	min ago Fr	ri Oct 13 20	Pay-As-You-Go	
Load balancers		Policies	Write NetworkSecurit	Succeeded 5	min ago Fr	ri Oct 13 20	Pay-As-You-Go	
Storage accounts		E Properties	Write VirtualNetwork	Accepted 5	min ago Fi	ri Oct 13 20	Pay-As-You-Go	
Virtual networks		Locks	Write PublicIPAddress	Succeeded 5	min ago Fr	ri Oct 13 20	Pay-As-You-Go	
Azure Active Directory		Automation script	Write NetworkInterface	Succeeded 4	min ago Fr	ri Oct 13 20	Pay-As-You-Go	
Monitor		MONITORING	Write StorageAccount	Succeeded 5	min ago Fr	ri Oct 13 20	Pay-As-You-Go	
Advisor		Metrics	Write VirtualMachines	Succeeded Ju	ust now Fr	ri Oct 13 20	Pay-As-You-Go	
		Alert rules	 Validate 	Started 6	min ago Fr	ri Oct 13 20	Pay-As-You-Go	ztd
Security Center		Diagnostics logs	 Update resource group 	Started 6	min ago Fr	ri Oct 13 20	Pay-As-You-Go	ztd
Cost Management + Billing		Application insights						
Help + support		(OMG)						

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

≡	Virtual machines * X Citrix Systems Inc.	virtual machine				
+ New	🕂 Add 🌒 Assign Tags 🛛 🚥 More		🏎 Connect 🕨 Start 🤗 R	Nestart 🔳 Stop 🔿 M	Nove 🗊 Delete 💍 Refresh	
🔲 Dashboard	Virtual machines and Virtual	Q Overview	Resource group (change) NetScalerSDWAN-ztdazure Status		Computer name ztdazure Operating system	
All resources	machines (classic) can now be managed together in the combined	Activity log	Running		Linux Size	
Resource groups	list below.	Access control (IAM)	West US 2 Subscription (change)		Size Standard D4 v2 (8 vcpus Public IP address	s, 28 GB memory)
🔇 App Services	Subscriptions: Pay-As-You-Go	🖉 Tags	Pay-As-You-Go Subscription ID		52.247.213.21 Virtual network/subnet	
SQL databases	Filter by name	X Diagnose and solve problems	52dd5bd9-2671-4cd3-8029-0f7d68	108d53	vnetbranch/branchmgt DNS name	
📬 SQL data warehouses	1 items	SETTINGS			ztdazuremgmtdnsname ≈	westus2.cloudapp.azure.com
遼 Azure Cosmos DB	ztdazure •••	🚨 Networking	Show data for last: 1 hour 6 h	hours 12 hours 1 day	7 days 30 days	
Virtual machines		air Disks				
🚸 Load balancers		👰 Size	CPU (average)	2 *	Network (total)	2 *
Storage accounts		Extensions	100%		1008	
Virtual networks		💽 Availability set	50%		508	
Azure Active Directory		Configuration				
Monitor		Properties	0%	1 9:45 AM	08	9:45 AM

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

Zero Touch Deployment Service	
Site Name: ztdazure	
Appliance Activated	
Connecting	Completed
Downloading config	Completed
Downloading software	Completed
Installing software	Completed
Applying config	Completed
Activating	Completed

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

Dashboard M	Monitoring Configuration	
Warning: Grace license instal Clear Warning	lled. Please obtain license from Citrix license portal and install it.	:
System Status		
Name:	ztdazure	
Model:	VPXL	
Appliance Mode:	Client	
Serial Number:	0000-0005-7786-4927-4958-4331-78	
Management IP Address	s: 10.9.0.106	
Appliance Uptime:	6 minutes, 52.3 seconds	
Service Uptime:	1 minutes, 58.0 seconds	
Routing Domain Enabled	d: Default_RoutingDomain	
Local Versions		
Configuration Created O	Dm: Fri Oct 13 16:30:55 2017	
Software Version:	9.3.1.35.624646	
Built On:	Oct 2 2017 at 21:01:31	
Hardware Version:	VPXL	
OS Partition Version:	4.6	
Virtual Path Service	Status	
Virtual Path DC-ztdazure	e Uptime: 1 minutes, 15.0 seconds.	

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

Grace license installed	. Please obtain	1 license from Ci	trix license porta	l and install it.							
Statistics	Monito	oring > Statisti	cs								
Flows											
Routing Protocols	Stati	stics									
Firewall	Show: F	Paths (Summary) •	Enable Auto Refr	esh 5 🔻 seconds Refresh	Show latest data.					
IKE/IPsec											
Performance Reports	Path	Statistics Sun	nmary								
Qos Reports	Filter:		in Any colu	ımn	Apply					Show 10	10 v entri
				1		1					
Usage Reports	Num ⁴	From Link	To Link	Path State	Virtual Path Service State	Virtual Path Service Type	BOWT	Jitter (mS)	Loss %	kbps	Congesti
Availability Reports			DC-INET	GOOD	GOOD	Static	2	2	0.00	10.83	NO
	1	Azure-INET	DC-INET								

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

Citrix SD-WA	N Center	R9_3_1_35_624	1646 V	admin ∨				
Dashboard Fault	: Monitori	ng Confi	guration Repo		Administration			
Network Discovery	Configuration	/ Zero Touch Dep	loyment / Activation His	tory				
Network Configuration	Prepare Nev	w Site A	ctivation History	tory Pending Activation				
Zero Touch Deployment	Showing 1 - 1 of	1					Search	
Change Management	Site Name 🔺	Serial No	Installer Email	Address	Status Details	Activation Date	Status	Action
Appliance Settings	ztdazure	C736A440-0A37- 4676-AF5D- CCDB74220783	ztdinstaller@outlook.com	AZURE - West US	Appliance Activated	Oct 14 15:10:13 2017 UTC	Activated	

Proxy Server Settings for zero touch deployment

March 12, 2021

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

1

Note

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

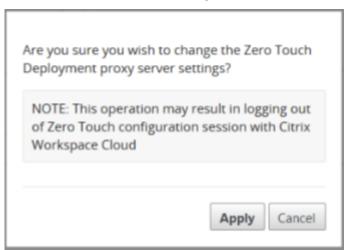
To configure zero touch proxy server settings:

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

Note

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

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



4. Click Apply.

Note

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

To remove proxy server settings:

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

3128
assword:
•••••

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

 nt proxy cor is operatior	-	ing out
ouch config	-	

4. Click Remove.

Palo Alto Network Integration

March 12, 2021

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

Citrix SD-WAN Center 11.4

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

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

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

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

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

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

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

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

 Template—The Prisma Access service automatically creates a template stack (Remote_Network_Template_ and a top-level template (Remote_Network_Template) for the Prisma Access service for remote networks. To Configure the Prisma Access Service for Remote Networks, you configure the top-level template from scratch or leverage your existing configuration, if you are already running a Palo Alto networks firewall on premise. The template requires the settings to establish the IPsec tunnel and Internet Key Exchange (IKE) configuration for protocol negotiation between your remote network location and the Prisma Access service for remote networks, zones that you can reference in security policy, and a log forwarding profile so that you can forward logs from the Prisma Access service for remote networks to the Logging Service.

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

Note:

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

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

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

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

Palo Alto network in SD-WAN Center

Ensure that the following prerequisites are met:

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

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

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

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

Dashboard			ing Co	nfiguration								
< Network Discovery		Configuration	n / Security / I	alo Alto Networks								
Network Configuration		Palo Alto Ne	etworks									
Zero Touch Deployment	:	Add										Subscription
Change Management		Show 25 \$	entries Sea	rch:			Subscription for Pa Panorama IP:	alo Alto Networks 🛛 🗙				
Appliance Settings		+				Region 🔺	34.229.137.184				Deployed Sites	Action
Mobile Broadband		US Eas	it (Ohio)				Username:				2	
Licensing		Add Sites					citrix Password:					
Cloud Connectivity	>	Show 10										
Security			Sit	• ^	Primary WAN Li	nk Subs	Log Level:				Status	Details
	Ť		Select Site	*	Select Primary WAN	Link 🔹 🕷 Select	Debug	•	• *			8
Zscaler		0	Branch		Branch-WL-1	2 Mbp		Apply Cancel	•	Connection Active		0
Palo Alto Networks		0	DC		DC-WL-1	2 Mbps	٣	zscalerappobject		Connection Active		0
												Previous 1 Next
		Showing 1 to 1										Previous 1 Next

Add and deploy sites

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

Note:

Traffic flow is impacted if the selected bandwidth exceeds available bandwidth range.

You can choose to redirect all internet bound traffic to the PRISMA ACCESS service by selecting the **All traffic** option under the Application object selection.

	ault	Monitoring	Configuration	Reporting	Administration	Nitro API					
<		Configuration / Secur	ity / Palo Alto Network								
Network Discovery											
Network Configuration		Palo Alto Network	s								
Zero Touch Deployment		Add									Subscription
Change Management		Show 25 \$ entries	Search:								
Appliance Settings		-			Region 🛧				Depl	loyed Sites	Action
Mobile Broadband		US East (Ohio)					*			0	Û
Licensing		Ad US East (N. Virgi	iola)								
Cloud Connectivity >		Shov US East (Ohio)									
Security 🗸		US West (N. Cali					bje	ct	St	tatus	Details
Zscaler		US West (Orego Canada (Montre					Obj	e • *			Û
Palo Alto Networks		South America (Previous 1 Next
		Showing EU (Frankfurt)									
		Deploy Delete									Previous 1 Next
Dashboard Fa	ault	Monitoring	Configuration	Reporting	Administration	Nitro API					
	ault	Monitoring	Configuration	Reporting	Administration	Nitro API					
	ault	Monitoring Configuration / Securi			Administration	Nitro API					
<		Configuration / Securi	ity / Palo Alto Networks		Administration	Nitro API					
Network Discovery	5	Configuration / Securi Palo Alto Networks	ity / Palo Alto Networks		Administration	Nitro API					Subscription (C)
Network Discovery Network Configuration Zero Touch Deployment	5	Configuration / Securi Palo Alto Networks	ity / Palo Alto Networks		Administration	Nitro API					Subscription .
Network Discovery Network Configuration Zero Touch Deployment Change Management	5	Configuration / Securi Palo Alto Networks Add Show 25 entries	ity / Palo Alto Networks			Nitro API					
Network Discovery Network Configuration Zero Touch Deployment Change Management Appliance Settings	5	Configuration / Securi Palo Alto Network: Add Show 25 entries	ity / Palo Alto Networks		Administration	Nitro API			Depi	loyed Sites	Action
Network Discovery Network Configuration Zero Touch Deployment Change Management Appliance Settings Mobile Broadband	5	Configuration / Securi Palo Alto Networks Add Show 25 9 entries IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	ity / Palo Alto Networks			Nitro API	•		Depi	loyed Sites 0	
Network Discovery Network Configuration Zero Touch Deployment Change Management Appliance Settings Mobile Broadband Licensing	5	Configuration / Secur Palo Alto Networks Add Show 25 e entries US East (Ohio) Add Stres	ity / Palo Alto Networks S Search			Nitro API	•		Depi		Action
Network Discovery Network Configuration Zero Touch Deployment Change Management Appliance Settings Mobile Broadband	5	Configuration / Securi Palo Alto Networks Add Show 25 9 entries IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	Ity / Palo Alto Networks 5 Search	, ,	Region A					0	Action
Network Discovery Network Configuration Zero Touch Deployment Change Management Appliance Settings Mobile Broadband Licensing	1	Configuration / Securit Palo Alto Networks Add Show 25 ± entries US East (Ohio) Add Sites Show 10 ± entries	Ity / Palo Alto Networks 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	Primary WAN Link	Region A Subscription	Bandwidth	Application Object				Action B Details
Network Discovery Network Configuration Zero Touch Deployment Change Management Appliance Settings Mobile Broadband Licensing Cloud Connectivity >	1	Configuration / Secur Palo Alto Networks Add Show 25 e entries US East (Ohio) Add Stres	Ity / Palo Alto Networks 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	, ,	Region A Subscription	Bandwidth				0	Action
Network Discovery Network Configuration Zero Touch Deployment Change Management Appliance Settings Mobile Broadband Licensing Cloud Connectivity Security	1	Configuration / Securit Palo Alto Networks Add Show 25 ± entries US East (Ohio) Add Sites Show 10 ± entries	Ity / Palo Alto Networks 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	Primary WAN Link	Region A Subscription	Bandwidth	Application Object			0	Action B Details
Network Discovery Network Configuration Zero Touch Deployment Change Management Change Management Licensing Cloud Connectivity Security Zscaler	1	Configuration / Securit Palo Alto Networks Add Show 25 ± entries US East (Ohio) Add Sites Show 10 ± entries	Ity / Palo Alto Networks 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	Primary WAN Link	Region A Subscription	Bandwidth	Application Object			0	Action Details Previous 1 Next
Eetwork Discovery Network Configuration Zero Touch Deployment Change Management Change Management Licensing Cloud Connectivity Security Zscaler	1	Confguration / Securit Add Show (51) entries (1) US East (Dhio) Add Sites Show (101) entries (2) Sect (5)	Ity / Palo Alto Networks 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	Primary WAN Link	Region A Subscription	Bandwidth	Application Object			0	Action
Network Discovery Network Configuration Zero Touch Deployment Change Management Change Management Licensing Cloud Connectivity Security Zscaler	1	Configuration / Securit Add Show 25 entries C US East (Dhio) Add Stress Show 10 entries Show 10 entries Show 10 entries	Ity / Palo Alto Networks 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	Primary WAN Link	Region A Subscription	Bandwidth	Application Object			0	Action Details Previous 1 Next
Network Discovery Network Configuration Zero Touch Deployment Change Management Change Management Licensing Cloud Connectivity Security Zscaler	1	Configuration / Securit Add Show 25 entries C US East (Dhip) Add Stress Show 10 entries Show 10 entries Show 10 entries	Ity / Palo Alto Networks 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	Primary WAN Link	Region A Subscription	Bandwidth	Application Object			0	Action Details Previous 1 Next

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

		ilt	Monitori	ing Config	uration	Reporting	Administration	Nitro API				
Network Discovery			Configuration	/ Security / Palo	Alto Networks							
Network Configurati	ion	Pa	lo Alto Ne	tworks								
Zero Touch Deploym	nent	Ad	ld									Subscription
Change Managemer	nt	s	how 25 \$ e	ntries Search:								
Appliance Settings			•			,	Region 🔺				Deployed Sites	Action
Mobile Broadband			US East	t (Ohio)							2	
icensing			Add Sites									
Cloud Connectivity	>		Show 10	-								
Security	~			Site A		Primary WAN Link		tion Bandwidth	Application Object		Status	Details
Zscaler			2	Select Site	*	Select Primary WAN Link	Select Banc	dwidth 👻 🕷	Select Application Obje •			8
Palo Alto Network	3			Branch		Branch-WL-1	2 Mbps	Ŧ	All Traffic (send to Palo *	Connection Active		0
				DC		DC-WL-1	2 Mbps	Ŧ	zscalerappobject *	Connection Active		0
												Previous 1 Next
		s	howing 1 to 1 o	of 1 entries								Previous 1 Nex
			Deploy De	lete								

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

				ing	Configuration								
Network Discovery					ty / Palo Alto Networks								
Zero Touch Deploymen		Add	Alto N	etworks	i								Subscription
Change Management			25 \$	entries	Search:								
Appliance Settings			+				Region 🛧					Deployed Sites	Action
Mobile Broadband			US Ea	it (Ohio)								2	
Licensing			Add Site				Deploy Sites		×				
Cloud Connectivity	>		Show 10	¢ entries			Deploying sites will Do you want to cor	initiate Change Man. tinue?	igement.				
Security	~		0	Branch	Site A	Primary WAN La Branch-WL-1	Yes	No		ation Object end to Palo *	Connection Active	Status	Details
Zscaler				DC		DC-WL-1					Connection Active		
Palo Alto Networks				DC		DC-WC-1	2 Mbps	*	zscalerapp	pobject v	Connection Active		0
													Previous 1 Next
		Shi	owing 1 to 1	of 1 entries									Previous 1 Next
			eploy D	elete									

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

ion Object			
tion Object Name: appobject			
Criteria			
Match Type	Application	Application Family	Protocol
application	Office 365 Default(office365_default)		
nnels			
	panw_service_		
Local IP: 192.168.100.3		eer IP: 3.52.159.66	
MTU:	F	irewall Zone:	
-	-		
IKE Version:		H Group:	
		roup2	
ikev2			
ikev2 IKE Hash Algorithm: sha256	b st	KE Integrity: ha256	
IKE Hash Algorithm: sha256 IKE Encryption:	st	ha256 KE Identity:	
IKE Hash Algorithm: sha256	st	ha256	
IKE Hash Algorithm: sha256 IKE Encryption: ass256 Identity Data:	53 18 30 19	KE Identity: uto Psec Tunnel Type:	
IKE Hash Algorithm: sha256 IKE Encryption: aes256	si no a fi e	kE Identity: uto	

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

Dashboard Fault	Monitor	ring Configuration	Reporting Ad	ministration	Nitro API				
etwork Discovery	Configuratio	n / Security / Palo Alto Netwo	ks						
twork Configuration	Palo Alto N	etworks							
ro Touch Deployment	Add								Subscription
ange Management	Show 25 \$	entries Search:							
pliance Settings	+		Regi	on A			D	ployed Sites	Action
bile Broadband	📼 US Ea	st (Ohio)						2	
ensing	Add Site	5							
ud Connectivity >		entries							
urity ~		Site 🔺	Primary WAN Link	Subscription Ba	ndwidth	Application Object		Status	Details
caler		Branch	Branch-WL-1	2 Mbps	Ŧ	All Traffic (send to Palo *	Connection Active		0
lo Alto Networks		DC	DC-WL-1	2 Mbps	Ŧ	zscalerappobject *	Connection Active		0
									Previous 1 Next
	Showing 1 to 1	of 1 entries							
	Deploy D	elete							Previous 1 Nex

Verify end-to-end traffic connection:

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

Microsoft Azure Virtual WAN

March 12, 2021

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

Microsoft Azure Virtual WAN allows you to enable simplified connectivity to Azure Cloud workloads and to route traffic across the Azure backbone network and beyond. Azure provides 54+ regions and multiple points of presence across the globe Azure regions serve as hubs that you can choose to connect to the branches. After the branches are connected, use the Azure cloud service through hub-tohub 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 is supported hub-to-hub communication using **Stan-dard** type method.

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

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

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

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

There are two types of virtual WAN:

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

Microsoft Azure		P Search resources, services, and docs (G+/)	>_ 💀 🖓 🛞 ? 💿 praveen.radjassegarin@ 🧉 critika sistimus, inic
Iome > Resource groups > h2h	val > New > Marketplace > Virtual WAN > Create WAN		
Create WAN			
Basics Review + create			
	ts a virtual overlay of your Azure network and is a collection of multiple resource	rs. Learn	
Project details			
ubscription *	NSDev SDWAN CA praveen.radjassegarin@citrix.com	~	
Resource group *	h2twal	~	
	Create new		
/irtual WAN details			
tesource group location *	Central US	¥	
lame *	h2hvalid	✓	
lype 💿	Standard	<u>^</u>	
	Standard		
	Basic		
Review + create	Provious Next : Review + create >		

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 P Search resources, services, and docs (G+/)									Ģ	Q	ŝ	?
	Azure services												
	+ 📀 📦 🚸 📍 💻 🐡								6			۲	
			Virtual WANs	Resource groups	Azure Active Directory	Subscriptions	Virtual machines	Virtual networks	Virtual ne gatew			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, SD-WAN Orchestrator will not have sufficient permissions to authenticate to Azure Virtual WAN APIs that enable automated connectivity.

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

- 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		\checkmark

- 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.

Virtual WANs Citrix Systems, Inc.	K AVWAN_USWEST Hu	ubs		
+ Add ≡≡ Edit columns ····		+ New Hub	🕐 Refresh	
Filter by name Name ↑↓	Overview Activity log Access control (IAM)		er	Clear all filters
📄 👵 avwan_uswest 🛛 😶	 Tags 	Hub	Hub status	Regio
	Settings	No results ∢		
	Configuration			
	Properties			
	🔒 Locks			
	Export template			
	Connectivity			
	💥 Hubs			
	VPN sites			
	Liser VPN configurations			
	A ExpressRoute circuits			
	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 gains it now will save time and reduce the risk of			VPN sites. You can do this after hub creation, but learn more	doing	
Do you want to create a Site to site (VPN gateway)?	Yes No				
AS Number i	65515			Ð	
*Gateway scale units ()	1 scale unit - 500	Mbps x 2	2	\sim	

5. Click **Review + create**.

6. Review the settings and click **Create** to start the virtual hub creation.

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

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

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

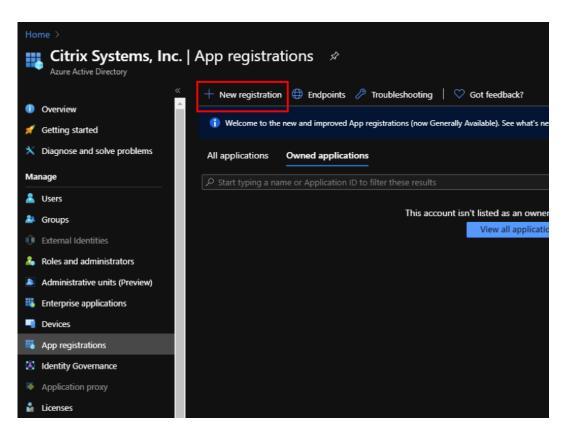
- Subscription ID
- Client ID
- Client Secret
- Tenant ID

Note

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

Perform the following steps to create a new application registration:

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



- 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 SD-WAN Orchestrator for authentication to the Azure subscription for usage of API.

Home > Citrix Systems, Inc. App registra	Home > Citrix Systems, Inc. App registrations >						
🚜 AZURE_API 🛛 🖉							
	🗊 Delete 🌐 Endpoints						
😽 Overview	Display name : AZURE_API	Supported account types					
🗳 Quickstart	Application (client) ID : Scheeses 1101 4edc adds 17dc174ceser	Redirect URIs	: 1 web, 0 spa, 0 public client				
🚀 Integration assistant (preview)	Directory (tenant) ID : 33585662, 46675825, 105-34802, 599961	Application ID URI	: Add an Application ID URI				
	Object ID : a 666495 200 4849 con 25,6416089 for	Managed application in I	: AZURE_API				
Manage		*					
Branding							
Output Authentication	Welcome to the new and improved App registrations. Looking to learn how it's chang	ed from App registrations (Legacy)?					

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**.

	ates & secrets 🛛 🖈				
		pplications to identify themselves to the auth urance, we recommend using a certificate (in			e location (using an HTTPS
nuickstart	Certificates				
🚀 Integration assistant (preview)	Certificates can be used as secrets	s to prove the application's identity when rec	uesting a token. Als	to can be referred to as public keys.	
Manage	[↑] Upload certificate				
Branding	Thumbprint	Start d	ate	Expires	
Authentication	No certificates have been added f	for this application.			
Certificates & secrets					
Token configuration					
API permissions	Client secrets				
📤 Expose an API	A secret string that the application	n uses to prove its identity when requesting	a token. Also can be	referred to as application password.	
Owners	+ New client secret				
Roles and administrators (Preview)	Description	E	xpires	Value	
Manifest	No client secrets have been create	ed 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 clier	Add a client 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 SD-WAN Orchestrator.

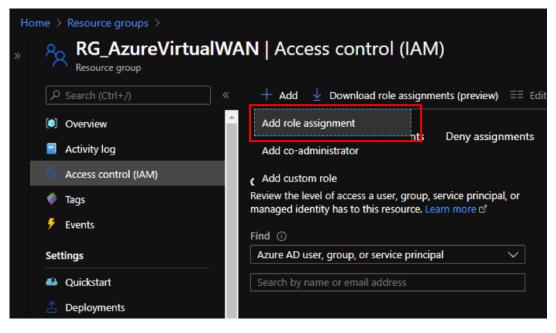
Home > Citrix Systems, Inc. App registra	itions >					
AZURE_API Certifica	ates & secrets 🖉					
₽ Search (Ctrl+/) «	Copy the new client secret value. You won't be a	ble to retrieve it after you perform another op	eration or leave this blade.			
Cvenview Quickstart	Credentials enable confidential applications to iden scheme). For a higher level of assurance, we recome		e when receiving tokens at a web addressable location (using a secret) as a credential.	n HTTPS		
🛒 Integration assistant (preview)						
Manage	Certificates	Festive's Martikesskan manuation a takan	Also can be called at an exciting base			
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.					
Authentication	Thumbprint	Start date	Expires			
Y Certificates & secrets		Start uate	cipii es			
Token configuration	No certificates have been added for this application					
API permissions						
Expose an API	Client secrets					
Swiners	A secret string that the application uses to prove its	identity when requesting a token. Also car	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	an sale for the feature of the factor	D 📋		
Troubleshooting						
New support request						

Note

You must copy and store the secret key value before reloading the page because, it will no longer be displayed afterwards.

Perform the following steps to assign the appropriate roles for authentication purpose:

- 1. In the Azure portal, navigate to the **Resource Group** where the Virtual WAN was created.
- 2. Navigate to Access control (IAM).
- 3. Click + Add and select Add role assignment.



4. To add role assignment, provide values for the following fields:

- **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 assignment ×				
Role ①				
Owner (i)		~		
Assign access to ①				
Azure AD user, group, or	service principal	\sim		
Select ①				
Azure_API				
No users, groups, or servi	ce principals found	I.		
Selected members:				
AZURE_API		Remove		
		Kentove		
Save				

Lastly, you need to obtain the Subscription ID for the Azure account. You can identify your **Subscription ID** by searching for Subscriptions in the Azure portal.

Citrix SD-WAN Center 11.4

Home > Subscriptions & Citrix Systems, Inc.							×
+ Add	+ 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 Citrix Systems, Inc. directory. Don't see a subscription? Switch directories							
My role 💿			Status 🛈				
8 selected V			3 selected				
Apply Showing 1 of 5 subscriptions Show only subsc	Apply Showing 1 of 5 subscriptions						
Subscription name	Subscription ID	¢↓	My role		Current cost	Status	
😐 Demo Center - Sittise Mictore Stale int Decit			Owner		Not available	Active	

Once you created the virtual WAN, log in to **SD-WAN Center UI > Configuration > Azure > Virtual WAN**.

Dashboard	Fault	Monitorir	g Configuration	Reporting	Administration	Nitro /	API		
Network Discovery		Configur	Configuration / Cloud Connectivity / Azure / Virtual WAN						
Network Configuration	'n	Secure	cure Connections to Azure Network O						
Zero Touch Deploymer	nt	Active Config:	auto_azvwan_habranch_dhcpenal	bled					
Change Management		Add Add	Multiple				Subscription	resh WAN Pull Active Config	Settings O365 Policy
Appliance Settings								Search:	
Mobile Broadband			Sites 🗸		WAN Link		Azure WAN	Status	Details
Licensing			branch2_azvwan	branch2_azvv	van-WL-1	h2hvalid		Tunnels Deployed	
Hosted Firewall			branch1_azvwan to 2 of 2 entries	branch1_azvv	van-WL-1	h2hvalid		Tunnels Deployed	
Cloud Connectivity	~	ReDeploy	Delete						
Cloud Direct									
Azure	~								
Virtual WAN									
Automated Azure (Deployment								
Security	>								

Select two different sites and start the deployment. Once the sites are deployed, you can associate both the sites to two different hubs.

NOTE

By default branch-to-branch and BGP is disabled. You can create a static route or enable BGP (under Settings) and branch-to-branch connectivity.

Enable BGP and branch-to-branch check box and deploy the tunnels. After the tunnels are deployed successfully, you can verify the status in **Microsoft Azure > Resource groups >** select the **resource group** that you created and click **VPN sites**.

Citrix SD-WAN Center 11.4

Microsoft Azure		🔎 Search resources, services, and docs (G+/) 💦 🔪 🖓 🔅 ? 🙂 praveen.re					
Home > Resource groups > h2hval	> h2hvalid - VPN sites						
h2hvalid - VPN sites							
P Search (Ctrl+/)		te-to-Site VPN c + New hub con	nection 🕐 Refresh				
Overview	▲ Search by site name ×	Clear all filters					
Activity log	transformation the text of text o						
Access control (IAM)	Select all sites						
Settings	VPN Sites ①						
Configuration	Site	Site Provisioning Status	Hub	Location	Link IP Address		
Properties	□ ■ branch1_azwan	Provisioned	∨1 hubs	Central US	∨ 1links		
🔒 Locks			🛛 h1westus - (Connected			
👤 Export template					20.190.49.59		
Connectivity	branch2_azwan	Provisioned	1 hubs	Central US	∨ 1links		
🖶 Hubs			📀 h2sthindia -	Connected			
VPN sites					104.211.231.115		
User VPN configurations							
ExpressRoute circuits							
Virtual network connections							
Support + troubleshooting							
 Continue standard 							

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

August 10, 2021

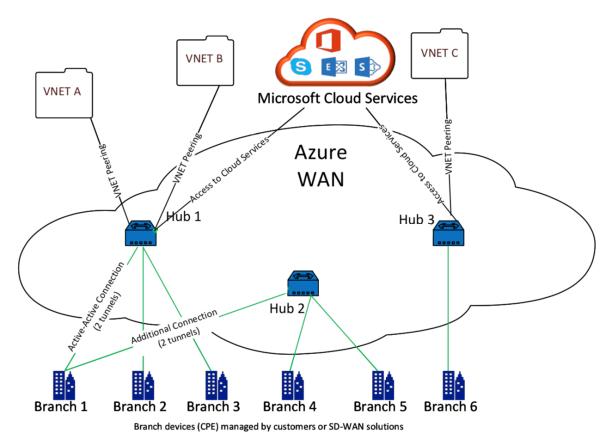
For on-premises devices to connect into Azure a controller is required. A controller ingests Azure APIs to establish site-to -site connectivity with the Azure WAN and a Hub.

Microsoft Azure Virtual WAN includes the following components and resources:

- WAN: Represents entire network in Microsoft Azure. It contains links to all Hubs that you would like to have within this WAN. WANs are isolated from each other and cannot contain a common hub, or connections between two hubs in different WANs.
- Site: Represents your on-premises VPN device and its settings. A Site can connect to multiple hubs. By using Citrix SD-WAN, you can have a built-in solution to automatically export this information to Azure.
- Hub: Represents the core of your network in a specific region. The Hub contains various service endpoints to enable connectivity and other solutions to your on-premises network. Site-to-site connections are established between the Sites to a Hubs VPN endpoint.
- Hub virtual network connection: Hub network connects the Azure Virtual WAN Hub seamlessly to your virtual network. Currently, connectivity to virtual networks that are within the same Virtual Hub Region is available.
- Branch: The branches are the on-premises Citrix SD-WAN appliances, which exist in customer office locations. An SD-WAN controller manages the branches centrally. The connection origi-

nates from behind these branches and terminates into Azure. The SD-WAN controller is responsible for applying the required configuration to these branches and to Azure Hubs.

The following illustration describes the Virtual WAN components:



How does Microsoft Azure Virtual WAN work

- 1. The SD-WAN Center is authenticated by using service principal, principal, or role-based access functionality, which is enabled in the Azure GUI.
- 2. The SD-WAN Center obtains Azure connectivity configuration and updates the local device. This automates the configuration download, editing, and updating of the on premise device.
- 3. After the device has the correct Azure configuration, a site-to-site connection (two active IPsec tunnels) is established to the Azure WAN. Azure requires the branch device connector to support IKEv2 settings. The BGP configuration is optional.

Note: IPsec parameters for establishing IPsec tunnels are standardized.

Citrix SD-WAN Center 11.4

IPsec Property	Parameter
	456.256
Ike Encryption Algorithm	AES 256
Ike Integrity Algorithm	SHA 256
Dh Group	DH2
IPsec Encryption Algorithm	GCM AES 256
IPsec Integrity Algorithm	GCM AES 256
PFS Group	None

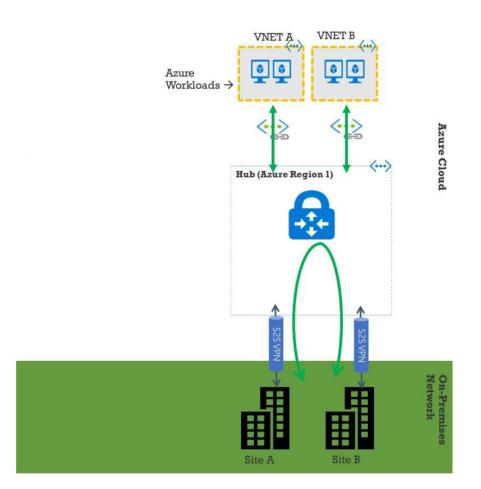
Azure Virtual WAN automates connectivity between the workload virtual network and the hub. When you create a Hub Virtual Network Connection, it sets the appropriate configuration between the provisioned hub and the workloads virtual network (VNET).

Prerequisites and requirements

Read the following requirements before proceeding with configuring Azure and SD-WAN to manage branch sites connecting to Azure hubs.

- 1. Have whitelisted Azure subscription for Virtual WAN.
- 2. Have an on premise appliance such as, an SD-WAN appliance to establish IPsec into Azure resources.
- 3. Have Internet links with public IP addresses. Though a single Internet link is sufficient to establish connectivity into Azure, you need two IPsec tunnels to use the same WAN link.
- 4. SD-WAN controller –a controller is the interface responsible for configuring SD-WAN appliances for connecting into Azure.
- 5. A VNET in Azure that has at least one workload. For instance, a VM, which is hosting a service. Consider the following points:
 - a) The virtual network must not have an Azure VPN or Express Route gateway, or a network virtual appliance.
 - b) The virtual network must not have a user-defined route, which routes traffic to a non-Virtual WAN virtual network for the workload accessed from on-premises branch.
 - c) Appropriate permissions to access the workload must be configured. For example, port 22 SSH access for a ubuntu VM.

The following diagram illustrates a network with two sites and two virtual networks in Microsoft Azure.



Set up Microsoft Azure Virtual WAN

For on premise SD-WAN branches to connect into Azure and access the resources over IPsec tunnels, the following steps need to be completed.

- 1. Configuring WAN resources.
- 2. Enabling SD-WAN branches to connect into Azure using IPsec tunnels.

Configure Azure network before configuring SD-WAN network, since the Azure resources required to connect to SD-WAN appliances must be available beforehand. However, you can configure SD-WAN configuration before configuring Azure resources, if you prefer. This topic discusses setting up the Azure Virtual WAN network first before configuring SD-WAN appliances. https://microsoft.com Azure virtual-wan.

Create a WAN resource

To use Virtual WAN features and connect the on premises branch appliance into Azure:

1. Sign in to Azure Marketplace, go to the Virtual WAN app, and select **Create WAN**.

Microsoft Azure				X
«	Home > Virtual WAN			
+ Create a resource	Virtual WAN		☆ □ ×	
E All services		rking service that provides optimized and automated brar	ich to branch	
— ★ FAVORITES ————————————————————————————————————	connectivity through Azure. V	irtual WAN lets you connect and configure branch devices	s to	
🗔 Dashboard		can be done either manually, or by using preferred provie r. Using preferred provider devices allows you ease of use		
All resources		and configuration management. The Azure WAN built-in ing insights that can help save you time, and gives you an		
😭 Resource groups	view large-scale Site-to-Site o		cusy may to	
🔇 App Services	Save for later			
🎸 Function Apps				
👼 SQL databases	PUBLISHER	Microsoft		
🧷 Azure Cosmos DB	USEFUL LINKS	Service overview Documentation		
🧕 Virtual machines		Pricing		
💠 Load balancers				
🧾 Storage accounts				
↔ Virtual networks				
Azure Active Directory				
😬 Monitor				
🧛 Advisor				
📋 Security Center	Create			
Oost Management + Billi				
P Help + support				

2. Enter a name for the WAN and select the subscription you want to use for WAN.

Citrix SD-WAN Center 11.4

Create WAN			
The virtual WAN resource overlay of your Azure net of multiple resources.			
Learn more.			
* Name			
* Subscription			_
		\sim	
* Resource group			1
Select existing		\sim	
Create new			
* Resource group location	on 🔁		_
East Asia		\sim	

Automation options

- 3. Select an existing resource group or create a fresh resource group. Resource groups are logical constructs and data exchange across resource groups is always possible.
- 4. Select the location where you want your resource group to reside. WAN is a global resource that does not have a location. However, you must enter a location for the resource group that contains metadata for WAN resource.
- 5. Click **Create**. This starts the process to validate and deploy your settings.

Create site

Create

You can create a site by using a preferred vendor. The preferred vendor sends the information about your device and site to Azure or you can decide to manage the device yourself. If you want to manage the device, you need to create the site in Azure Portal.

SD-WAN network and Microsoft Azure Virtual WAN workflow

Configure SD-WAN appliance:

- 1. Provision a Citrix SD-WAN appliance
 - Connect SD-WAN branch appliance to the MCN appliance.
- 2. Configure SD-WAN appliance
 - Configure Intranet Services for Active-Active connection.

Configure SD-WAN Center:

• Configure SD-WAN Center to connect to Microsoft Azure.

Configure Azure settings:

• Provide Tenant ID, Client ID, Secure Key, Subscriber ID, and Resource Group.

Configure branch site to WAN association:

- 1. Associate one WAN resource to a branch. Same site cannot be connected to multiple WANs.
- 2. Click **New** to configure Site-WAN association.
- 3. Select Azure Wan-resources.
- 4. Select **Services** (Intranet) for the site. Select two services for Active-Standby support.
- 5. Select **Site Names** to be associated with the Wan-resources.
- 6. Click **Deploy** to confirm the association.
- 7. Wait for the status to change to **Tunnels Deployed** to view the **IPsec tunnel** settings.
- 8. Use the SD-WAN Center Reporting view to check status of the respective IPsec tunnels.

Configure Citrix SD-WAN network

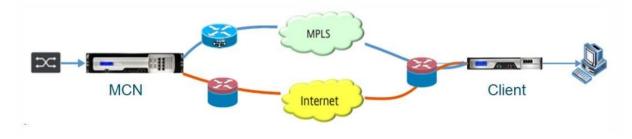
MCN:

The MCN serves as the distribution point for the initial system configuration and subsequent configuration changes. There can be only one active MCN in a Virtual WAN.

By default, appliances have the pre-assigned role of client. To establish an appliance as the MCN, you must first add and configure the site as an MCN. The network configuration GUI becomes available after a site is configured as an MCN. Upgrades and configuration changes must be performed from the MCN or SD-WAN center only.

Role of MCN:

The MCN is the central node that acts as the controller of an SD-WAN network and the central administration point for the client nodes. All configuration activities, in addition to preparation of firmware packages and their distribution to the clients, are configured on the MCN. In addition, monitoring information is available only on the MCN. The MCN can monitor the entire SD-WAN network, whereas client nodes can monitor only the local Intranets and some information for those clients, which they are connected. The primary purpose of the MCN is to establish overlay connections (virtual paths) with one or more client nodes located across the SD-WAN network for Enterprise Site-to-Site communication. An MCN can administer and have Virtual Paths to multiple client nodes. There can be more than one MCN, but only one can be active at any given time. The below figure illustrates the basic diagram of the MCN and client (branch node) appliances for a small two site network.



Configure SD-WAN appliance as MCN

To add and configure the MCN, you must first log into the Management Web Interface on the appliance you are designating as the MCN, and switch the Management Web Interface to MCN Console mode. MCN Console mode enables access to the Configuration Editor in the Management Web Interface to which you are currently connected. You can then use the Configuration Editor to add and configure the MCN site.

To switch the Management Web Interface to MCN Console mode, do the following:

- 1. Log into the SD-WAN management web interface on the appliance you want to configure as the MCN.
- 2. Click **Configuration** in the main menu bar of the Management Web Interface main screen (blue bar at the top of the page).
- 3. In the navigation tree (left pane), open the **Appliance Settings branch** and click **Administrator Interface**.
- 4. Select the Miscellaneous tab. The miscellaneous administrative settings page opens.

Administrator Interface Logging/Monitoring User Accounts RADIUS TACACS+ HTTPS Cert Miscellaneous Change Web Console Timeout SNMP Licensing Timeout: 9999 Enter the new timeout value in minutes (1-9999).	- Appliance Settings	Configuration > Appliance Settings
	 Logging/Monitoring Network Adapters Net Flow SNMP 	Change Web Console Timeout
	tem Maintenance	Switch to MCN Console

At the bottom of the **Miscellaneous** tab page is the **Switch to [Client, MCN] Console** section. This section contains the **Switch Console** button for toggling between appliance console modes.

The section heading indicates the current console mode, as follows:

- When in Client Console mode (default), the section heading is Switch to MCN Console.
- When in MCN Console mode, the section heading is Switch to Client Console.

By default, a new appliance is in the Client Console mode. MCN Console mode enables the Configuration Editor view in the navigation tree. The Configuration Editor is available on the MCN appliance, only.

Configure MCN To add and begin configuring the MCN appliance site, do the following:

1. In the SD-WAN appliance GUI, navigate to **Virtual WAN > Configuration Editor**.

- Virtual WAN			
View Configuration	VEX		View Tutorial / Citrix Support
Configuration Editor Change Management	New Open Save Save As Import		Q All * Global Actions * B 2
Change Management Settings	New Open Save Save As Import	Export.	Q All * Global Actions *
Restart/Reboot Network			
Enable/Disable/Purge Flows			
Dynamic Virtual Paths SD-WAN Center Certificates	Basic Global Sites Connections Opt	imization Provisioning	N
System Maintenance	View Mode: Step +		
	+ Sites	Sile Details Self Add	
	20	Appliance:	
	BR	Appliance (CBVPX)	
		Interfaces: 0 +	
		Interfaces: 0 +	
		Mode: Fail to Block, VLANS: 0 (17210.00.1/24)	
		- TARGE OLIVATION OF T	
		WAN Links: 0 +	
		DC Wo 1 Access Type : Public Internet	
		Rates : 130000M / 20000M IP Address : 17210.10.1/24	
		VLAN: 0 GW Address: 172.10.10.2	
		Virtual Path Mode : Primary	
		Static Routes: 0 +	

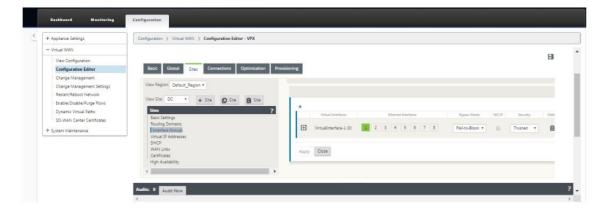
2. Click + **Sites** in the Sites bar to begin adding and configuring the MCN site. The **Add Site** dialog box is displayed.

Add		×
Site Name:		
*		
Site Location:		
Secure Key:		
2133fd5e276b6735		
Model:	Mode:	
	client	
CB1000 *		
CB1000 •	client	

- 3. Enter a site name that lets you determine the geographic location and role of the appliance (DC/secondary DC). Select the correct appliance model. Selecting the correct appliance is crucial since the hardware platforms differ from each other in terms of processing power and licensing. Since we are configuring this appliance as the primary head end appliance, choose the mode as primary MCN and click **Add**.
- 4. This adds the new site to the sites tree and the default view shows the basic settings configuration page as shown below:

	Site Name:		
ew Site: MCN-DC • + Site 🖸 Site	MCN-DC		
Sites ?	Appliance Name:	Secure Key:	
Basic Settings	Appliance	3484f4bcf5f758f5	Regenerate
Routing Domains	Model:	Mode:	
Interface Groups Virtual IP Addresses	CBVPX *		
VRRP DHCP WAN Links Certificates High Availability	Site Location: Default Direct Route 0 5	Cost	
	Gateway ARP Timer in	ns):	
	1000		
	Enable Source MA	C Learning	

- 5. Enter the basic settings such as location, site name.
- 6. Configure the appliance so that it can accept traffic from Internet/MPLS/Broadband. Define the interfaces where the links are terminated. This depends on whether the appliance is either in overlay or underlay mode.
- 7. Click Interface groups to start defining the interfaces.



8. Click + to add virtual interface groups. This adds a new virtual interface group, the number of virtual interfaces depends on the links that you want the appliance to handle. The number of links that an appliance can handle varies from appliance model to model and the maximum number of links can be up to eight.

Add Virtual Interfaces		Ethernet Inter	faces		Bypass Mode	WCCP	Security	Delete
ŧ	1 2 3	4 5	6 7	8	Fail-to-Block •		Trusted •	Û
								_

9. Click + to the right of virtual interfaces to view the screen as shown below.

Virtual Interfaces		Ethernet Interfaces		Bypass Mode	WCCP	Security	Delet
Э	1 2 3	4 5 6 7 8	Fa	il-to-Block 🔹	-	Trusted •	Û
Virtual Interfaces	+					Bridge Pairs	
	Add	Firewall Zone	VLAN ID	DHCP Client	Delete	Interfaces LS	P Delete
VirtualInterf	ace-1	Default_LAN_Zor •	0		*		

- 10. Select the **Ethernet interfaces**, which form the part of this virtual interface. Depending on the platform model, appliances have a pre-configured pair of fail-to-wire interfaces. If you want to enable fail-to-wire on appliances, then ensure that you are choosing the correct pair of interfaces and ensure that you choose fail-to-wire under the **Bypass Mode** column.
- 11. Select the security level from the drop-down list. Trusted mode is chosen, if the interface is serving MPLS links and Untrusted is chosen when Internet links are used on the respective interfaces.
- 12. Click + to the right of the label named virtual interfaces. This shows the Name, firewall zone and VLAN IDs. Enter the **Name and VLAN ID** for this virtual interface group. VLAN ID is used to identifying and marking traffic to and from the virtual interface, use 0 (zero) for native/untagged traffic.

Sites	?									
Basic Settings			Virtual Interfaces		Ethernet Interfaces		Bypass Mode	WCCP	Security	-
Routing Domains Interface Groups Virtual IP Addresses			VirtualInterface-1 (0)	1 2	3 4 5 6 7	8	Fail-to-Block		Trusted •	
DHCP WAN Links Certificates		L	Virtual Interfaces +						Bridge Pairs 🔸	
High Availability			Name		Firewall Zone	VLAN ID	DHCP Client	Delete	Interfaces LSP	De
	•		VirtualInterface-2		<default></default>	0		*		
			VirtualInterface-1		Default_LAN_Zone Internet_Zone Untrusted_Internet_	Zone 0		Û		
		-								

- 13. To configure the interfaces in fail to wire, click Bridge pairs. This adds a new bridge pair and allows for editing. Click **Apply** to confirm these settings.
- 14. To add more virtual interface groups click + to the right of the interface groups branch and proceed as above.
- 15. After the interfaces are chosen, the next step is to configure IP addresses on these interfaces. In Citrix SD-WAN terminology this is known as a VIP (Virtual IP).
- 16. Continue in the sites view and click the Virtual IP address to view the interfaces for configuring VIP.

5	D Site D Site ?	Add P Address / Prefix	Virtual Interface	Firewall Zone	Identity	Private	Security Delete	
ic Settings .ting Domains	<i>*</i>	172.10.10.1/24	VirtualInterface-1 •	Default_LAN_Zone				8
erface Groups mual IP Addresses CP N Links tificates h Availability		Apply Close						
h Availability	•							
• IP Address / Prefix	Virtual Interface	Firewall Zone	Identity Private Se	scurity Delete				
	Virtual Interface	Firewall Zone	Identity Private So		*			
IP Address / Prefix	_	Firewall Zone Default_LAN_Zone			<i>م</i>			

17. Enter the IP Address / Prefix information, and select the Virtual Interface with which the ad-

dress is associated. The Virtual IP Address must include the full host address and netmask. Select the desired settings for the Virtual IP address, such as the Firewall Zone, Identity, Private, and Security. Click **Apply**. This adds the address information to the site and includes it in the site Virtual IP Addresses table. To add more Virtual IP Addresses, click + to the right of the Virtual IP Addresses, and proceed as above.

18. Continue in the sites section to configure WAN Links for the site.

View Region: Default_Region *	+ Add Link	
View Site DC1 + Site D Site	76	
Clean Save Serbing: Receive Domain Receive Domain Interface Coupon Vincal IP Addresses OHCP VINCALID Addresses Vinga Availability	Revic Settings Note: Changing the access type of this WANN Link may cause automatically generated Paths to the init, to be added or removed. Access Type: Public Internet WANN Link Temptate: defame> // Users table Physical Rate Munic // Set Premiced From Physical Permitted Rate (key)	VILINI IS 1001 Physical Rate Maps: M Set Permitted From Physical Permitted Rate Maps:
	Tracking IP Address	Autodetect Public IP Public IP Address:
	Advanced Settings Bighality	
	Metered/Standby Link	

19. Click **Add link**, at the top of the panel on the right hand side. This opens a dialog box, which allows you to choose the type of link to be configured.

Add	^
Name:	
DC1-WL-1	
Access Type:	
Public Internet	
Public Internet	
Private Intranet	tel

- 20. Public Internet is for Internet/broadband/DSL/ADSL links, whereas private MPLS is for MPLS links. Private Intranet is also for MPLS links. The difference between private MPLS and private Intranet links is that private MPLS allows for preserving the QoS policies of MPLS links.
- 21. If you are choosing public Internet and the IPs are assigned through DHCP, choose the auto detect IP option.
- 22. Select Access Interfaces in the WAN link configuration page. This opens the Access Interfaces

VAN Link: DC1-V	WL-1 V Section:	Access Interfaces •	+ Add Link	Delete Link		
+		iace IP Address Gatew			Internet Access for All Routing Domains	Delete

view for the site. Add and configure the VIP and gateway IP for each of the links as shown below.

- 23. Click + to add an interface. This adds a blank entry to the table and opens it for editing.
- 24. Enter the name you want to assign to this Interface. You may choose to name it based on the link type and location. Keep the routing domain as default if you do not want to segregate networks and assign an IP to the Interface.
- 25. Ensure that you provide a publicly reachable gateway IP address if the link is an internet link or a private IP if the link is an MPLS link. Keep the virtual path mode as primary since you need this link to form virtual path.

Note: Enable proxy ARP as the appliance replies to ARP requests for the gateway IP address when the gateway is unreachable.

- 26. Click **Apply** to finish configuring WAN link. If you want to configure more WAN links, then repeat the steps for another link.
- 27. Configure routes for the site. Click Connections view and select routes.
- 28. Click + to add routes, this opens a dialog box as shown below.

Vetwork IP Address	Cost	Service Type		Gateway I	P Address
*	5	Local	•		*
Export Route					
Summary Route					
Eligibility Based On Path					
ath:					
<none> *</none>					
Eligibility Based On Gatew					

- 29. Enter the following information is available for the new route:
 - Network IP Address
 - Cost –Cost determines which route takes precedence over the other. Paths with lower costs take precedence over higher cost routes. The default value is five.
 - Service type –Select the service, a service can be any of the following:
 - Virtual Path
 - Intranet
 - Internet
 - Passthrough
 - Local
 - GRE Tunnel
 - LAN IPsec tunnel

30. Click Apply.

To add more routes for the site click + to the right of the routes branch and proceed as above. For more information, refer to Configure MCN.

Configure virtual path between MCN and branch sites Establish connectivity between the MCN and branch node. You can do this by configuring a virtual path between these two sites. Navigate to the **Connections** tab in the configuration tree of the configuration editor.

- 1. Click the **Connections** tab in the configuration section. This displays the connections section of configuration tree.
- 2. Select the MCN from view site drop-down menu in the connections section page.

Basic Global Sites Connections Optimization Prov	visioning
ew Region: Default_Region ew Site: MCN-DC Connections WAN-to-WAN Forwarding Virtual Paths Dynamic Virtual Paths Internet Services WAN Links GRE Tunnels IPsec Tunnels Firewall Application Routes Routes OSPF BGP Route Learning Properties Multicast Groups	Group: Default> * Enable WAN-to-WAN Forwarding (Routes Export) Enable Virtual Path-to-Virtual Path Forwarding Enable Virtual Path-to-Internet/Intranet Forwarding Enable Site as Intermediate Node Apply Close

3. Select virtual path from under the connections tab to create virtual path between the MCN and branch sites.

	-
	tual Path to Site: Section: + Add Virtual Path Delete Virtual Path
View Site: MCN-DC Connections Connection	Tracking IP Address: Default Set: <none> None> Route Cost: 5 Apply Close</none>

4. Click Add Virtual Path next to the name of the static virtual path in the virtual paths section. This opens up a dialog box as shown below. Choose the branch for which you want the Virtual path to be configured. You must configure this under the label named remote site. Select the branch node from this drop-down list, and click the check box **Reverse Also**.

Add	×	
Remote Site:		
<none></none>	* ▼	
Reverse Also If enabled, Clas both Sites for th	ses and Rules will be mi is Virtual Path.	irrored on

Traffic classification and steering are mirrored on both sites of the virtual path. After this is complete, select paths from the drop-down menu under the label named section as shown below.

w Site: MCN-5100 V + Site Site Site	+				WAN L Classe Rules				
VAN-to-WAN Forwarding Virtual Paths	From Site	From Link	To Site	To Li	Paths		1	Delete	
Dynamic Virtual Paths	BR57	2 BR572-WL-1	MCN-5100	MCN-5100	-WL-1	YES	0	台	
sternet Service	BR57	2 BR572-WL-1	MCN-5100	MCN-5100	-WL-2	YES	0	Ĥ	
ntranet Services /AN Links	BR57	2 BR572-WL-2	MCN-5100	MCN-5100	-WL-1	YES	0	Û	
RE Tunnels	BR57	2 BR572-WL-2	MCN-5100	MCN-5100	-WL-2	YES	0	Û	
Psec Tunnels	MCN-510	0 MCN-5100-WL-1	BR572	BR572-WL	-1	YES	0	Û	
rewall polication Routes	MCN-510	0 MCN-5100-WL-1	BR572	BR572-WL	-2	YES	0	自	
outes		0 MCN-5100-WL-2		BR572-WL	-1	YES	0	Û	
SPF GP		MCN-5100-WL-2		BR572-WL		YES	0	Û	
Route Learning Properties Multicast Groups Application Settings	Apply	Refresh							

5. Click **+ Add** above the paths table, which displays the add path dialog box. Specify the endpoints within which the virtual path must be configured. Now, click **Add** to create the path and click the **Reverse Also checkbox**.

Note: Citrix SD-WAN measures link quality in both directions. This means point A to point B is one path and point B to point A is another path. With the help of unidirectional measurement of link conditions, the SD-WAN is able to choose the best route to send traffic over. This is different from measures such as RTT, which is a bi-directional metric to measure latency. For example, one connection between point A and point B is displayed as two paths and for each of them the link performance metrics are calculated independently.

This setting is enough to bring the virtual paths up between the MCN and the branch, other configuration options are also available. For more information, refer to Configure virtual path service between MCN and Client sites.

Deploy MCN configuration The next step is to deploy the configuration. This involves the following two steps:

- 1. Export the SD-WAN configuration package to Change Management.
 - Before you can generate the Appliance Packages, you must first export the completed configuration package from the **Configuration Editor** to the global **Change Management** staging inbox on the MCN. Refer to the steps provided in the section, Perform change management.
- 2. Generate and stage the appliance packages.
 - After you have added the new configuration package to the Change Management inbox, you can generate and stage the Appliance Packages on the branch sites. To do this, you use the Change Management wizard in the management web interface on the MCN. Refer to the steps provided in the section, Stage Appliance Packages.

Configure intranet services to connect with Azure WAN resources

1. In the SD-WAN appliance GUI, go to the **Configuration Editor**, navigate to the **Connections** tile. Click **+ Add Service** to add an Intranet Service for that site.

Basic Global Sites Connections Optimization P	rovisioning
View Region: Default_Region *	+ Add Service
View Site: BR513 👻 🕂 Site 🔂 Site	NO OBJECTS ADDED, PLEASE CLICK THE ADD BUTTON
Connections ?	
WAN-to-WAN Forwarding	
Virtual Paths	
Dynamic Virtual Paths	
Internet Service	
Intranet Services	
WAN Links	
GRE Tunnels	
IPsec Tunnels	
Firewall	
Application Routes	
Routes	
OSPF	
BGP	
Route Learning Properties	
Multicast Groups	
Application Settings	

- 2. In the **Basic Settings** for the Intranet Service, there are several options on how you want the Intranet Service to behave during unavailability of WAN links.
 - **Enable primary reclaim** –check this box if you want the chosen primary link to take over when it comes up after failing over. If you however, choose not to check this option then the secondary link would continue to send traffic over.
 - **Ignore WAN Link status** –If this option is enabled, then packets destined for this intranet service would continue to use this service even if the constituent WAN links are unavail-

ıble.			
Intranet Service: New_Intranet_Service-2 •	Section: Basic Settings *	+ Add Service	Delete Service
Name:	Basic Settings WAN Links Rules		
New_Intranet_S			
Firewall Zone: <pre></pre>			
 Enable Primary Reclaim Default Set: <none> •</none> 			
Ignore WAN Link Status			
Apply Refresh			

3. After configuring the basic settings, the next step is to choose the constituent WAN Links for this service. At the maximum of two links are chosen for one Intranet service. To choose the WAN links please select the WAN links option from the drop-down list labeled Section. The WAN links function in primary and secondary mode and only one link are chosen as a primary WAN link.

Note: When a second intranet service is created, it must have the primary and secondary wanlink mapping.

						LAN to	WAN			WAN to LAN		
	WAN Link	Use	Mode	Tunnel Header Size (bytes)	Access Interface Failover	Tagging	Max Delay (ms)	Tagging		Matching		Grooming
I	BR513-WL-1		Prima •	0	•	None •	500	None	٠	None	٠	•
E	BR513-WL-2		Prima *	0		None *	500	None	Ŧ	None	Ŧ	1

4. Branch site specific Rules are available, enabling the capability of customization of each branch site uniquely overriding any general settings configured in the global default set. Modes include desired delivery over a specific WAN link, or as an Override Service allowing for pass through or discard of the filtered traffic. For instance, if there is some traffic, which you do not wants to be going over the intranet service, you can write a rule to discard that traffic or send it over a different service (internet or pass through).

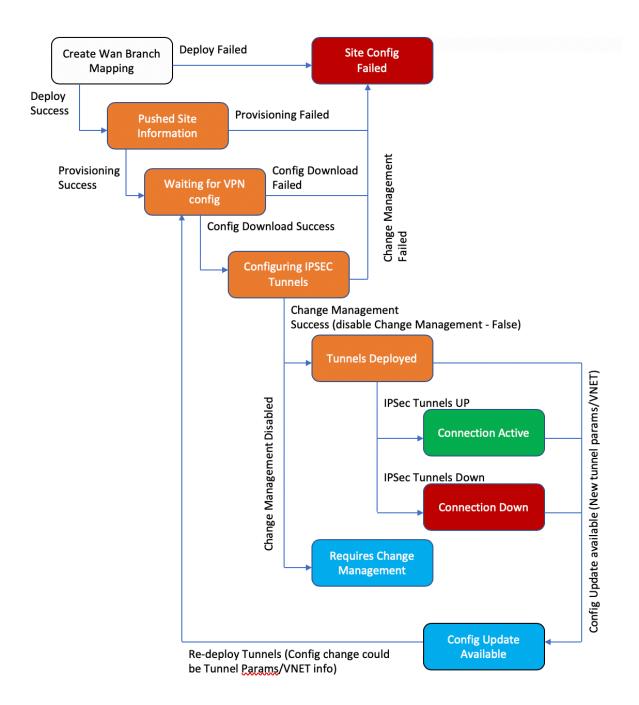
			IP Address					Port						
Order	Rule Group Name	Source	Dest=Src	Dest	Protocol	Protocol #	Source	Dest=Src	Dest	DSCP	VLAN	Rebind Flow on Change	Delete	Clo
100	<none> •</none>	x		*	Any •	0	*		*	Any •	*			đ
Verride S <pick or<="" td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></pick>														
	ne> ▼													

5. With Intranet Service enabled for a site, the **Provisioning** tile is made available to allow for the bidirectional (LAN to WAN / WAN to LAN) distribution of bandwidth for a WAN link among the various services utilizing the WAN link. The **Services** section allows you to further fine-tune bandwidth allocation. In addition, fair share can be enabled, allowing services to receive their minimum reserved bandwidth before fair distribution is enacted.

			LAN to	9 WAN			WAN	to LAN		
Name 🔥	Group	Min (kbps)	Max (kbps)	Shares of Group	Fair (kbps)	Min (kbps)	Max (kbps)	Shares of Group	Fair (kbps)	
MCN-5100	Default •	80	no limit	1000	4990	80	no limit	1000	4990	WAN to LAN
New_Intranet_Service-	2 Default 🔹	100	no limit	1000	5010	100	no limit	1000	5010	
Totals:		180) 0	2000	0 10000	0 180) (200	0 10000	

Configure SD-WAN Center

The following diagram describes the high-level workflow of SD-WAN Center and Azure Virtual WAN connection and corresponding state transitions of the deployment.



Configure Azure settings:

• Provide Azure Tenant ID, Application ID, Secret Key and Subscription ID (also known as service

principal).

Configure branch site to WAN association:

- Associate a branch site to a WAN resource. Same site cannot be connected to multiple WANs.
- Click **New** to configure Site-WAN association.
- Select Azure WAN-resources.
- Select Site Names to be associated with the WAN resources.
- Click **Deploy** to confirm the association. The WAN links to be used for Tunnel Deployment is auto-populated with the one with best link capacity.
- Wait for the status to change to 'Tunnels Deployed'to view the IPsec tunnel settings.
- Use the SD-WAN Center Reporting view to check status of the respective IPsec tunnels. The IPsec tunnel status must be GREEN for the data traffic to flow, which says the connection is active.

Provision SD-WAN Center:

SD-WAN center is the management and reporting tool for Citrix SD-WAN. The required configuration for Virtual WAN is performed in SD-WAN Center. SD-WAN center is available only as a virtual form factor (VPX) and needs to be installed on a VMware ESXi or a XenServer hypervisor. The minimum resources needed to configure an SD-WAN center appliance are 8 GB RAM and 4 CPU cores. Here are the steps to Install and configure an SD-WAN center VM.

Configure SD-WAN Center for Azure connectivity

Read create a service principal for more information.

To successfully authenticate SD-WAN center with Azure, the following parameters must be available:

- Directory(Tenant ID)
- Application(Client ID)
- Secure Key(Client Secret)
- Subscriber ID

Authenticate SD-WAN Center:

In the SD-WAN Center UI, navigate to **Configuration** > **Cloud Connectivity** > **Azure** > **Virtual WAN**. Configure Azure connection settings. Refer to the following link for more information about configuring Azure VPN connection,

Azure Resource Manager.

Citrix SD-	-WAN	Center			ł,				admin 🗸
Dashboard			Configuration	Reporting	Administration	Nitro API			
<		Configuration /	/ Cloud Connectivity / A:	zure / Virtual WAN					
Network Configuratio	n	Secure Con	nections to Azu	re Network					0
Zero Touch Deployme	ent	Active Config:							
Change Management	t	Add Add Multip	le			Subscription	Refresh WAN Pull Active Conf	ig 🌣 Settings	O365 Policy
Appliance Settings								Search:	
Mobile Broadband					WAN Links				
Licensing			Sites 🗸	Primary		Secondary	Azure WAN	Status	Details
Hosted Firewall									
Cloud Connectivity	~								
Cloud Direct		ReDeploy	Delete						
Azure	~								
Virtual WAN									
Automated Azure	Deployment								
Security	>								

With 11.1.0 release and above, the Primary and Secondary WAN link configuration for Azure Virtual WAN integration is supported. The primary reason of adding secondary WAN link is to have redundancy from the Citrix SD-WAN site.

With the previous implementation, failure of the WAN link could result in traffic disruption and connectivity loss to Azure Virtual WAN. With the current implementation, the Site to Azure Virtual WAN connectivity is kept alive even if the primary WAN link is down.

Enter the **Subscription ID**, **Tenant ID**, **Application ID** and **Secure Key**. This step is required to authenticate SD-WAN center with Azure. If the credentials entered above are not correct, then the authentication fails and further action is not allowed. Click **Apply**.

Subscription for Azure		×
Subscription ID:		
		*
Tenant ID:		
		*
Application ID:		
		*
Secret Key:		
		*
	Apply	ancel

The Storage account field refers to the storage account that you have created in Azure. If you did

not create a storage account then a new storage account is automatically created in your subscription when you click **Apply**.

Obtain Azure Virtual WAN resources:

After authentication is successful, Citrix SD-WAN polls Azure for obtaining a list of Azure virtual WAN resources, which you created in the first step after logging into Azure portal. The WAN resources represent your entire network in Azure. It contains links to all Hubs that you would like to have within this WAN. WANs are isolated from each other and cannot contain a common hub or connections between two different hubs in different WAN resources.

Citrix SD-W	AN Center					R10_1_0_133_695064 ~	admin ~
	ault. Monitoria	g Configuration	Reporting Adv				
Network Discovery	Configuration	/ Claud Connectivity					
Network Configuration Zero Touch Deployment Change Management		nections to Azure I					
Appliance Settings Mobile Broadband	Add Add Multi		it Azure portal			[Subscription] [Refresh WAN] [Aut Active Config]	O Setting
Licensing	Show 10 + 0	ntries.				Search	
Cloud Connectivity			Intrat	et Services			
	0	Stes	Tunnel1	Tunnel2	Azure WAN	Status en	Details
				No data available in tat	sie	_	
	Showing 0 to					Previou	n Ned
	Deploy 🔒	Delete					

To associate branch sites and Azure WAN resources:

A Branch site needs to be associated with Azure WAN resources to establish IPsec tunnels. One Branch can be connected to multiple Hubs within an Azure virtual WAN resource and one Azure virtual WAN resource can be connected with multiple on premise branch sites. Create single rows for each Branch to Azure Virtual WAN resource deployments.

To add multiple sites:

You can choose to add all the respective sites and associate them with the chosen single WAN resources.

1. Click Add Multiple to add all the sites that must be associated with the chosen WAN resources.

		Configuration						
Network Discovery	Configuration /	Cloud Connectivity / A	zure / Virtual WAN					
Network Configuration	Secure Con	nections to Azu	re Network					(
Zero Touch Deployment	Active Config:							
Change Management	Add Add Multip	le			Subscripti	on Refresh WAN Pull Active	Config Settings	O365 Policy
Appliance Settings	Connect n once	nultiple SD-WAN sites into	Azure at				Search:	
Mobile Broadband				WAN Links				
Licensing		Sites 🗸	Primary	Se	condary	Azure WAN	Status	Details

- 2. The Azure WAN resources drop-down list (shown below) is pre-populated with the resources belonging to your Azure account. If no WAN resources have been created then this list is empty, and you must navigate to the Azure portal to create the resources. If the list is populated with WAN resources, choose the **Azure WAN resource** to which you need the branch sites to be connected to.
- 3. Choose one or all of the branch sites to initiate the process of IPsec tunnel establishment. The Sites best capacity Public Internet WAN links are chosen automatically to establish the IPsec tunnels to the Azure VPN Gateways.

X

Configure multiple sites	s to Azure	network
Azure WAN:		
wannew5		•
Sites:		
✓Select All		
✓Branch		
✓DC		
	Deploy	Cancel

To add single site:

You can also choose to add sites one-by-one (single) and as your network grows, or if you are performing a site-by-site deployment, you can choose to add multiple sites as described above.

1. Click **Add New Entry** to select one Site Name for the Site-Wan association. Add sites in the Configure Sites to **Azure Network** dialog box.

	7.014	Center						R11	_0_3_2_808846 ~	admin
shboard F	ault	Monitoring	Configuration	Reporting	Administration	Nitro API				
rork Discovery		Configuration /	Cloud Connectivity	/ Azure / Virtual WAN	1					
ork Configuration		Secure Conn	ections Cont	figure Sites to Azure n	etwork				×	
Touch Deployment		Active Config: config_a	ug27 Add	4						
ige Management		Add			Sites	WAN Link		Azure WAN	Settin	gs 0365 P
ance Settings			No c	lata available in table						
le Broadband				-					Deploy Clear	Details
sing		No data available i								
ed Firewall		Showing 0 to 0 of 0 ReDeploy	entries Delete							
d Connectivity	~									
ud Direct										
re	~									
irtual WAN										
utomated Azure Dep	oyment >									
rity	<i></i>									
	es to A	zure network								>
onfigure Site										
onfigure Site								Δ.71	ure WAN	
			Sites			WAN Link		AL		
Add	DC		Sites	• D0	C-WL-1	WAN Link	•	wannew5		
Add			Sites		C-WL-1 anch-WL-1	WAN Link	• •			•

- 2. Select the Branch site to configure to the Azure Virtual WAN network.
- 3. Select the WAN link associated with the site(the Public Internet type links are listed in the order best physical link capacity)
- 4. Select the WAN resource to which the site must be associated to from the **Azure Virtual WANs** drop-down menu.
- 5. Click **Deploy** to confirm the association. The status ("Init Site Information "Pushed Site Information" & "Waiting for VPN configuration") is updated to notify you about the process.

The deploy process includes the following status:

- Push Site Information
- Waiting for VPN configuration
- Tunnels Deployed
- Connection Active (IPsec Tunnel is up) or Connection Down (IPsec Tunnel is down)

			Configuration								
etwork Discovery		Configuration /	Cloud Connectivity / A	zure / Virtual WAN							
etwork Configuration		Secure Conr	ections to Azu	re Network							
ro Touch Deployment		L Please confirm t	he creation of Hub on the	Azure portal for the deploy	ed sites if not already cre	nated.					
hange Management		Opployment Suc									
opliance Settings		Active Config: config_) Add Add Multipl						Subscription	Refresh WAN P	ull Active Config	O365 Poli
obile Broadband										Search	
ensing sted Firewall						WAN Links					
oud Connectivity		•	Sites 🗸		Primary	Sec	ndary	Azure	NAN	Status	Details
jud connectivity	Ť	DCA2		DC-WL-1		DC-WL-2		VirtualWANUS		Init Site Information	
oud Direct		Bran		Branch-W	a	Branch-WL-2		VirtualWANUS		Connection Active	
Virtual WAN	ř	Showing 1 to 2 of 2 ReDeploy	Delete								
Automated Azure Depl	loyment										

Associate Site Wan Resource Mappings (Azure portal):

Associate the deployed sites on the Azure portal to the Virtual Hubs created under the Azure Virtual WAN resource. One or more Virtual Hubs can associated with the Branch site. Each Virtual Hub is created in a specific region and specific workloads can be associated with the Virtual Hubs by creating Virtual Network Connections. Only after the Branch Site to Virtual Hub association is successful, the VPN configurations gets downloaded and respective IPsec tunnels are established from the Site to VPN Gateways.

Wait for the Status to change to Tunnels Deployed or Connection Active to view the **IPsec tunnel** settings. View IPsec settings associated with the selected services.

Dashboard	Fault		Configuration	Reporting	Administration	Nitro API				_
	rauit	Monitoring	comgeration	Reporting	Administration	NICOAFI				
ietwork Discovery		Configuration	/ Cloud Connectivity / /	Azure / Virtual WAN						
ietwork Configuration		Secure Con	nections to Azu	re Network						
ero Touch Deployment		Active Config: config.	_MultipleLink							
hange Management		Add Add Multip	ple					Subscription CRefresh WAN	Pull Active Config Settings	O365 Polis
ppliance Settings									Search:	
fobile Broadband						WAN Links				
icensing			Sites 🗸		Primary		Secondary	Azure WAN	Status	Details
osted Firewall		O DCA	z	DC-W		DC-WL-2		VirtualWANUS	Connection Active	
	~	Bran Showing 1 to 2 of	nchAZ	Bran	h-WL-1	Branch-WL-2		VirtualWANUS	Connection Active	
oud Connectivity	Ň		2 entries							
Cloud Direct			<u>u</u>							
zure	~									
Virtual WAN										
Automated Azure De	ployment									
curity	>									

	Monitoring	Configuration						
etwork Discovery	Configuration /	Cloud Connectivity / A	zure / Virtual WAN					
etwork Configuration	🔔 For region:Defau	It_Region SE Connect	ion Properties				×	
ero Touch Deployment	Secure Conn	ections	time : 2019-10-04 00:41: of Hubs Connected: 1	21 UTC Error Status : N/A				
hange Management	Active Config: config_au	g27 Status - T	unnel 1	State: UP	Packets Received: 5	Packets Transmitted: 5	Packets Dropped: 0	
ppliance Settings	Add	Status - T	unnel 2	State: UP 🔵	Packets Received: 4	Packets Transmitted: 4	Packets Dropped: 0	Settings O365 P
lobile Broadband		Site Infor	mation - Tunnel 1	Local IP: 192.168.100.3	LocalEndpointIP: 208.50.136.169	Peer IP: 20.44.35.203	MTU: 1500	
censing osted Firewall	DC	Site Infor	mation - Tunnel 2	Local IP: 192.168.100.3	LocalEndpointIP: 208.50.136.169	Peer IP: 20.44.35.244	MTU: 1500	Details
oud Connectivity \sim	Brance Showing 1 to 2 of 2 e		nfig	Ike Version: ikev2	DH Group: group2	Ike HASH Algorithm: sha256	Ike Integrity: sha256	•
Cloud Direct		Delete		Ike Encryption: aes256 Ipsec Integrity: sha256	Ipsec Tunnel Type: esp Ipsec Encryption: aes256gcm128	PFS Group: none Mismatch Behaviour: drop	Ipsec HASH Algorithm: sha256	
Azure Virtual WAN		Protected	d Networks	34.34.34.6/32	34.34.34.7/32			
Automated Azure Deployment		BGP Info		BGP State: Enabled	BGP PeerIP: 34.34.34.6,34.34.34.7	BGP LocalASN: 59437	BGP PeerASN: 65515	
curity >								

SD-WAN Azure settings:

- Disable SD-WAN change management –By default, the Change Management process is automated. This means that anytime a new configuration is available at Azure Virtual WAN infrastructure, SD-WAN Center obtains it and starts applying it to branches automatically. However, this behavior is controlled, if you want to control when a configuration must be applied to branches. One benefit of disabling automatic change management is that the configuration for this feature and other SD-WAN features is managed independently.
- **Disable SDWAN Polling**–Disables all SD-WAN Azure new deployments and polling on existing deployments.
- **Polling Interval** Polling interval option controls the interval of looking for configuration updates in Azure Virtual WAN infrastructure, the recommended time for polling interval is 1 hour.
- **Disable Branch-to-Branch Connection** –Disables branch-to-branch communication over Azure Virtual WAN infrastructure. By default, this option is disabled. Once you enable this, it means on-prem branches are able to communicate with each other and the resources behind the branches over IPsec through Azure's Virtual WAN Infra. This does not have any effect on branch-to-branch communication over SD-WAN virtual path, branches are able to communicate with each other and their respective resources/end points over virtual path even if this option is disabled.
- **Disable BGP** This disables BGP over IP, by default it is disabled. Once enabled the site routes are advertised over BGP.
- Debug Level Enables capturing logs to debug if there is any connectivity issues.

SDWAN Azure Settings	×
Disable SDWAN Polling:	
Disable SDWAN Change Management: 🖉	
Disable Branch to Branch Connection:	
Disable BGP:	
Polling Interval: 60 minutes	
Debug Level: Debug 🔻	
Change Management	
Apply Ca	ncel

Refresh WAN resources:

Click the **Refresh** icon to retrieve latest set of WAN Resources that you updated on the Azure Portal. A message stating, "successfully refreshed WAN resources" is displayed after the refresh process is complete.

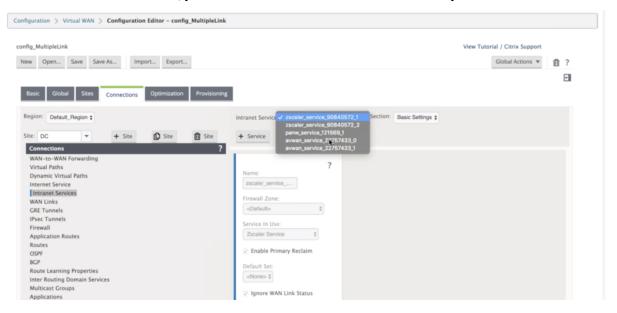
Dashbard Yaut Menitoring Configuration Reporting Administration Nitro APi Resont Discovery Network Configuration Resont Discovery Network Configuration Resont Discovery Resont Discovery Resont Discovery Network Configuration Resont Discovery Resont Dis	Citrix SD-V	VAN	Center								R11_1_0_169_832	2211 ~	admin 🔻
Network Discovery Cenfiguration / Cloud Connectivity / Astrix / Vitual WAN Network Configuration Secure Connections to Azure Network Carpe Management Aplance Settings Aplance Settings Aplance Settings Noble Broodband Image Management Locensig Aplance Settings Noble Broodband Image Management Locensig Aplance Settings Noble Broodband Image Management Locensid Image Management Autor Image Management Autor Image Management Autor Image Management Locensid Image Management Autor Image Management <t< th=""><th></th><th></th><th></th><th>Configuration</th><th>Reporting</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></t<>				Configuration	Reporting								
Cancel Control Cont			Configur	ation / Cloud Connectivity /	Azure / Virtual WAN								
Change Management Acter Coding:	Network Configuration		Secure	Connections to Azu	ire Network								0
Change Mangement Add Mad Multiple Backerstein Advise Backerstein Advise Backerstein Advise Backerstein Advise Backerstein Advise <td>Zero Touch Deployment</td> <td></td> <td>3</td>	Zero Touch Deployment												3
Applance Settings Image: Setting Settings Mobile Broadband Image: Setting Setti	Change Management									Conference and an		the formation of	0.00
Model ensemble Image: Steam of the steam	Appliance Settings		Add Add	Multiple					Subscription	C Refresh WAN	Pull Active Config	Settings	O365 Policy
Hosted Frewall Sites v Primary Secondary Arure WAN Status Primary Cloud Connectivity DOAZ DCW.1 DCW.2 Vinual WANUS Connection Active Sites v Cloud Direct Branch-XZ Branch-WL-2 Vinual WANUS Connection Active Sites v Vinual WAN Branch-WL-2 Vinual WANUS Connection Active Sites v	Mobile Broadband										Se	sarch:	
Cloud ConnetNikly Cloud ConnetNikly Cloud ConnetNikly Cloud Direct Aure Virtual WANN Automated Acure Deployment	Licensing				_		WAN Links						
Cloud Connectivity Branch-W2 Vintual/WANUS Connection Active Cloud Direct. Ature Vintual WANN	Hosted Firewall			Sites 🗸		Primary		Secondary	Azur	re WAN	Stat	us	Details
Branch-XZ Branch-WL-1 Branch-WL-2 Virtual/WANUS Connection Active Image: Connection Active Cloud Direct Rechtplow Image: Connection Active Image: Connection Active Image: Connection Active Image: Connection Active Virtual/WAN Automated Acure Deployment Image: Connection Active Image: Connection Active Image: Connection Active Image: Connection Active	Cloud Connectivity	~											
Couc Direct Anure Anure Virtual WAN Automated Azure Deployment					Branch	-WL-1	Branch-WL-2		VirtualWANUS		Connection Active	e	
Azure Virtual Vann Automated Azure Deployment													
Automated Azure Deployment		Ň											
Security >	Automated Azure De	ployment											
	Security	>											

Remove site WAN resource association Select one or multiple mappings to perform deletion. Internally, the SD-WAN appliance Change Management process is triggered and until it is successful, the Delete option is disabled to prevent from performing further deletions. Deleting mapping requires you to disassociate or delete the corresponding sites in the Azure portal. The user has to perform this

operation manually.

Citrix SD-	WAN	Center						R11_1_0_169_832211 ~	admin \vee
Dashboard			Configuration	Reporting					
Network Discovery		Configuration	/ Cloud Connectivity / /	Azure / Virtual WAN					
Network Configuration	•	Secure Cor	nnections to Azu	re Network					0
Zero Touch Deploymer	nt	Active Config: confi							
Change Management		Add Add Mult	liple				Subscription CRefresh WAN	Pull Active Config	O365 Policy
Appliance Settings						Delete ×		Search	
Mobile Broadband						Deleting mapping would trigger a change			
Licensing		0	Sites 🗸		Primary	management. Please disassociate/delete the corresponding sites on Azure portal. Are you sure	Azure WAN	Status	Details
Hosted Firewall			:AZ	DC-WL		you want to Delete this entry/entries?	VirtualWANUS	Connection Active	
Cloud Connectivity	~	Showing 1 to 2 of	anchAZ If 2 entries	Branch	-WL-1	Delete Cancel	VirtualWANUS	Connection Active	
Cloud Direct		ReDeploy	Delete						
Azure	~								
Virtual WAN									
Automated Azure I	Deployment								
Security	>								

Once the tunnels are created, you can see two intranet services created in your MCN.



Each Intranet service corresponds to IPsec tunnels that are created with Peer IPs (Azure Virtual WAN end point IPs).

							View		Citrix Suppor	
ew Open Save Save As	. Import Export							Glob	al Actions	Ĺ
	Optimization	Provisioning								
egion: Default_Region \$	► Site	🚺 Site								?
Connections		?	vice Type	Name	Firewall Zone	Local IP	Peer IP	MTU	Keepalive	
WAN-to-WAN Forwarding Virtual Paths				avwan_service_22757433_0 ‡	<default></default>	<auto></auto>	13.83.24.93	1500	2	Û
Dynamic Virtual Paths				avwan_service_22757433_1 ‡	<default></default>	<auto></auto>	13.83.24.138	1500	2	Û
Internet Service			¢	panw_service_121569_1	<default></default>	10.10.2.4 ‡	34.104.0.33	1500	$\overline{\mathbf{Z}}$	Û
Intranet Services WAN Links			\$	zscaler_service_90840572_1 \$	<default></default>	10.10.2.4 \$	104.129.202.10	1500	2	Û
GRE Tunnels			÷	zscaler_service_90840572_2 ‡	<default></default>	10.10.2.4 ‡	104.129.198.179	1500	Z	Û
IPsec Tunnels Firewall Application Routes Routes OSPF BGP Route Learning Properties Inter Routing Domain Services										

From the **Intranet Services**, if you select **WAN Links** from the **Section** drop-down list, you can see both primary and secondary WAN link that specified by you. By default the mode is set to **Auto**.

fig_MultipleLink									1	View	Tutorial / Citrix S	Suppo	ort
w Open Save Save As Import Export											Global Acti	ions	•
Basic Global Sites Connections Optimization Provi	sioning												
Basic Global Sites Connections Optimization Provi	sioning												
egion: Default_Region \$	Intranet Se	ervice:	avwa	in_service,	,22757433,	_0 \$ Se	ction:	/AN Link	•				
te: DC 👻 + Site 🛍 Site	+ Servic	e f	Ser	vice									
Connections	?	_											
WAN-to-WAN Forwarding													
Virtual Paths							LAN to	WAN			WAN to LAN		_
Virtual Paths Dynamic Virtual Paths		WAN	lise	Mode	Tunnel Header	Access		Max	Taoning				Grooming
		WAN Link	Use	Mode	Tunnel Header Size (bytes)	Access Interface Failover	LAN to		Tagging		WAN to LAN Matching		Grooming
Virtual Paths Dynamic Virtual Paths Internet Service [Intranet Services WAN Links	-	WAN Link DC-	Use	Mode	Header Size	Interface		Max Delay	Tagging				Grooming
Virtual Paths Dynamic Virtual Paths Internet Service Intranet Services WAN Links GRE Tunnels		DC-	Use		Header Size (bytes)	Interface Failover	Tagging	Max Delay (ms)			Matching		Grooming
Virtual Paths Dynamic Virtual Paths Internet Service Intranet Services WAN Links GRE Tunnels IPsec Tunnels		DC- WL-	Use	Mode Auto \$	Header Size (bytes)	Interface		Max Delay (ms)	Tagging			•	Grooming
Virtual Paths Dynamic Virtual Paths Internet Services WAN Links GRE Tunnels Firewall		DC- WL- 1	Use		Header Size (bytes)	Interface Failover	Tagging	Max Delay (ms)			Matching	•	
Virtual Paths Dynamic Virtual Paths Internet Services WAN Links GRE Tunnels IPsec Tunnels Firewall Application Routes		DC- WL-	Use		Header Size (bytes)	Interface Failover	Tagging None \$	Max Delay (ms)		0	Matching	•	
Virtual Paths Dynamic Virtual Paths Internet Services WAN Links GRE Tunnels Firewall Application Routes Routes OSPF		DC- WL- 1	Use		Header Size (bytes)	Interface Failover	Tagging	Max Delay (ms)		0	Matching	•	
Virtual Paths Dynamic Virtual Paths Internet Service Intranet Services WAN Links GRE Tunnels Firewall Application Routes Routes OSPF BCP	,	DC- WL- 1 DC-	Use	Auto \$	Header Size (bytes)	Interface Failover	Tagging None \$	Max Delay (ms)	None	0	Matching	0	٥
Virtual Paths Dynamic Virtual Paths Internet Service Intranet Services WAN Links GRE Tunnels Firewall Application Routes Routes OSPF	,	DC- WL- 1 DC- WL-	Use	Auto \$	Header Size (bytes)	Interface Failover	Tagging None \$	Max Delay (ms)	None	0	Matching	0	٥

Monitor IPsec Tunnels In the SD-WAN Center UI, navigate to **Reporting** > **IPsec** to check the status of IPsec tunnels. The tunnel status must be GREEN for the data traffic to flow.

inne. O	October 3, 2019 5:	23pm	📰 Las	t: Hour /	Day / W	eek / Month										Mode:	Relative (1	minute ago)		¢ (C
	11:30am		12:00pm	12:	:30pm	1:00pm		1:30pm	2:00pm	2	::30pm		3:00pm		3:30pm	4:00pm		4:30pm	5:00pm		
													1								
	11:30am		12:00pm	12:	:30pm	1:00pm		1:30pm	2:00pm	2	::30pm		3:00pm		3:30pm	4:00pm	KK (KK)	4:30pm ▶ >> >>1	5:00pm Interval: 1	minute	¢
iting Domain: A	ny	\$																			
plications HD	OX App QoE	MOS	Services	Classes	Sites	Virtual Paths	Paths	WAN Links	MPLS Queues	Ethernet	GRE	IPsec	Events								
		g 1 - 6 of i	rrs: + 6						az	ure										P	10*
¢ / page	Showin	g 1 - 6 of i		Servi	ice Type	In	tranet Ser	vice Type		ure ec Tunnel Wo	orst State	e 🖸	M	TU	TX Bandwid	th 🖂	RX Band	dwidth 🖂	Data	Dropped	
¢ / page Nan	Showin filtered	g 1 - 6 of 1 from 9	6	Servio	ice Type	Azure	tranet Ser	vice Type				e 🖂	M	TU 1434	TX Bandwid	th 🖂	RX Band	lwidth 🖂 0.04			
¢ / page Nan service_690152	Showin filtered me ^ 269_0	g 1 - 6 of 1 from 9	6 Site		ice Type		tranet Ser	vice Type		ec Tunnel Wo		• 🖻	M		TX Bandwid	_	RX Band		2		1 E
/ page Nanservice_690152service_690152	Showin, filtered me ^ 269_0 269_1	g 1 - 6 of 1 from 9	6 Site Branch	Intranet	ice Type	Azure	tranet Ser	vice Type		ec Tunnel Wo GOOD		e 🖂	M	1434	TX Bandwid	0.04 🗠	RX Band	0.04			1 🖂 0.00 E
/ page Nan a_service_690152 a_service_690152	Showin, filtered me ^ 269_0 269_1 269_2	g 1 - 6 of i from 9	6 Site Branch Branch	Intranet Intranet	ice Type	Azure Azure	tranet Ser	vice Type		ec Tunnel Wo GOOD GOOD		e 🖂	M	1434 1434	TX Bandwid	0.04 🗹	RX Band	0.04			0.00 E
w Bandwidth/Dat w Bandwidth/Dat page Nan n_service_690152 n_service_690152 n_service_690152 n_service_690152 n_service_690152	Showin, filtered 269_0 269_1 269_2 269_3	g 1 - 6 of 1 from 9	6 Site Branch Branch Branch	Intranet Intranet Intranet	ice Type	Azure Azure Azure	tranet Ser	vice Type		ec Tunnel Wo GOOD GOOD GOOD		e 🖾	M	1434 1434 1434	TX Bandwid	0.04 🖂 0.04 🖂 0.04 🖂	RX Band	0.04			0.00 E 0.00 E 0.00 E

Cloud Direct Service

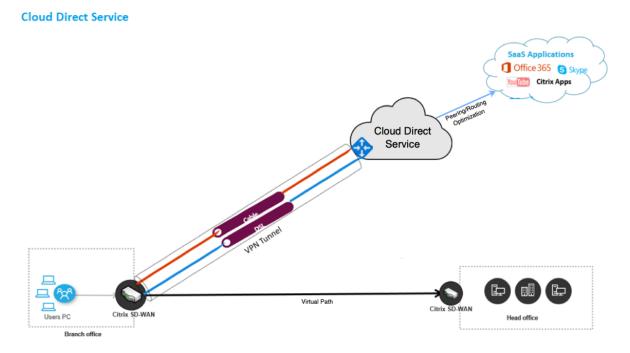
March 12, 2021

The Cloud Direct service delivers SD-WAN functionalities as a cloud service through reliable and secure delivery for all internet-bound traffic regardless of the host environment (data center, cloud, and internet). It improves network visibility and management. It enables partners to offer managed SD-WAN services for business critical SaaS applications to their end customers.

Cloud direct service offers the following advantages:

- **Redundancy** Uses multiple internet WAN links and provides seamless failover.
- Link aggregation Uses all internet WAN links at the same time.
- Intelligent load-balancing across WAN connections from different providers:
 - Measuring packet loss, jitter and throughput.
 - Custom application identification.
 - Application requirement and circuit performance matching (adapt to real-time network conditions).
- SLA-grade Dynamic QoS Capability to internet circuit:
 - Dynamically adapts to varying circuit throughput.
 - Adaption through the tunnel at ingress and egress endpoints.
- Rerouting VOIP calls between circuits without dropping the call.
- End-to-end monitoring and visibility.

Cloud direct service workflow



Before you begin deploying the Cloud Direct Service, ensure that the following steps are completed:

- 1. Have a 410-SE, 210-SE, or 1100-SE/PE edition appliance. If the factory shipped SD-WAN version of the appliance is earlier than 9.3.5, then you must follow the USB reimaging procedure to upgrade the appliance to the latest shipping base image.
- 2. Perform single step upgrade procedure to install the software version that supports Cloud Direct Service.
- 3. Configure the MCN appliance and establish the virtual paths with its branches:
 - Configure branch site. See Configure Branch for more information.
 - Create application objects for application-based routes.
 - If you intend to selectively steer the applications through the Cloud direct service, create the application objects by including the corresponding applications, see how to create Application Objects, which are routed through the Cloud direct service. To manage Internet bound traffic, the Internet service must be created from the appliance configuration editor. For more information, see Internet Service.
 - If you intend to steer all internet bound traffic through the Citrix Cloud direct service, then you can skip creating the specific application objects.

Licensing

The Cloud Direct service feature is licensed independently from the base licenses of SD-WAN. Ensure that you have installed the required licenses for the Cloud Direct service on SD-WAN Center. For more information, see Citrix SD-WAN Center as a license server.sd-wan-center-as-license-server.

The Licensing page provides details about the installed Cloud Direct service license information.

Dashboard			Configuration	Reporting	Admini	stration Nitro API		
< Network Discovery		Configuration / Licen	sing / License Details					
Network Configuration	1	Network Summary	License Detai	Is File Ma	nagement			
Zero Touch Deploymer	nt	License Server Host ID:	f2ba416af433					
Change Management		License Kind: Cloud Direct						
Appliance Settings		A deleted Cloud Direct licer	se will expire on the day	it was deleted.				
Mobile Broadband								
Licensing		Show 100 \$ entries	Search:					
		Bandwidth (Mb	ps) 🔨	Available	Used	License Ex	piry	Grace Period Remaining
Cloud Connectivity	~	10	1		0	Sun Dec 01 00:00:00 2019		
Cloud Direct		Showing 1 to 1 of 1 entries						Previous 1 Nex
Azure	>							
Security	>							

Note

There is a grace period of 30 days for the expired or deleted Cloud Direct licenses, before which you need to install the valid licenses for the deployed Cloud Direct sites to be functional. If no valid licenses are installed before the expiry of the Grace period, SD-WAN Center disables the Cloud Direct service on site using the expired license.

Configure cloud direct service in SD-WAN Center

1. In the SD-WAN Center GUI, navigate to **Configuration** > **Cloud Connectivity** > **Cloud Direct**.

Dashboard	Fault	Monitoring	Configuration	Reporting	Administration	Nitro	API
Network Discovery		Configuration / Cloud Cloud Connectivity	l Connectivity				
Zero Touch Deployment		Cloud Direct					Azure
Change Management					a cloud service through reli nost environment (data ce		Virtual WAN
Appliance Settings Mobile Broadband					nent. It enables partners to o their end customers.	offer	Azure Virtual WAN is used to upload the Branch site information into Azure portal to ensure connectivity between the Branch and Azure backbone. In order to establish the Azure connectivity, the Branch site needs to be preconfigured with the Intranet service using the required wan-links associated with the intranet service.
Licensing							Automated SD-WAN Deployment
Cloud Connectivity	~						Automated SD-WAN Deployment enables organizations to have a direct secure connection from branch environments to applications hosted in Azure in an automated manner eliminating
Cloud Direct							deployment complexity, the need for dedicated express route and backhauling cloud bound traffic through a data center. This helps in ensuring a superior user experience especially for latency
Azure	>						sensitive and bandwidth intensive applications such as the ones hosted in Citrix Virtual Apps and Desktoos service.
Security	>						Busiceps of recei

2. Log in with Citrix Cloud credentials.

• • •	Citrix Secure Sign In	
https://accounts-internal.c	cloud.com/core/login?signin=e0fa6531d8b50068bf	0 7
Citrix Cloud [™]		
Enter your Citrix credentials. (Citrix.com, My Citrix, or Citrix	Cloud)	
abc@citrix.com		
	Sign In	I
Remember me		
Eo	rgot your username or password? Contact Support	
	Don't have an account?	
	Sign up and try it free	
:	Sign in with my company credentials	
English (US)		
stablishing secure connection		

The Cloud Direct home page appears after you successfully logged into the Citrix Cloud Service.

			Configuration		Admin		litro API				
Network Discovery Network Configuration		Configuration / Cloud	Connectivity / Cloud D	irect							
Zero Touch Deployment		Site Details									
Change Management		Add Edit								Pull	Active Config
Appliance Settings		Show 100 \$ entries	Search:								
Mobile Broadband		Site Name		AN Links	Regio	n Primary POP	Secondary POP	Subscription Bandwidth (Mbps)	Service Status	Appliance Status	Details
Licensing		No sites deployed for Clo	Link Names	(kbps)	(kbps)						
Cloud Connectivity	~		elete							Previous	Next
Cloud Direct		Deploy Disable D	Pelete								
Azure	>	License Details									
Security	>	Show 100 \$ entries	Search:								
		Bandwidth (N	, .	Available	Used		icense Expiry		Grace Per	iod Remaining	
		10 Showing 1 to 1 of 1 entrie	1 s		0	Sun Dec 01 00:00:00	2019				
										Previous	1 Next

3. Click **Pull Active Config** to retrieve latest active MCN configuration.

Configuration / Cloud Conn	nectivity / Clo	ud Direct							
Site Details									
Add Edit								Pull	Active Config
Show 100 \$ entries Se	earch:								
		WAN Links				Subscription			
Site Name	Link Names	Pull Acti	ve Config		× ondary POP	Bandwidth (Mbps)	Service Status	Appliance Status	Details
No sites deployed for Cloud Dir	rect service.	deplo	ng active config will ove byed changes	erwrite any un-					
		Do ye	ou want to continue?					Previous	Next
License Details			Yes	lo					
License Details									
Show 100 🛊 entries Se	earch:								
Bandwidth (Mbps)	^	Available	Used	-	License Expiry		Grace Peri	iod Remaining	
10		1	0	Sun Dec 01 00:00:0	0 2019				
Showing 1 to 1 of 1 entries								Previous	Next

4. Click **Add a new site**. Sites that are eligible for the Cloud Direct service deployment are displayed in the menu.

Note

- The Cloud Direct service feature is supported on 210, 410, and 1100 hardware appliances.
- From 11.2 release onwards, the Cloud Direct service is supported on SD-WAN 2100, 4100, and 6100 appliances. Both SD-WAN Center and Orchestrator allow the Cloud Direct service feature to be deployed on SD-WAN 2100, 4100, and 6100 appliances. SD-WAN Center supports up to 250 Mbps subscription licenses for Cloud Direct.

nfigure	e Site to Cl	oud Direct Servi	ce						
Not	e: To add ap	plication objects, i	nternet service must be	configured on the	site.				
ite Nan site21(•	Cb2				legion: Default I	Region	
elect u	pto four WAN	N Links:*			Dormi	tted Rate		Pandwidth for Cl	oud Direct Service
Use 🔥	WAN Link	Access Type	WAN Link Type	Standby Mode	LAN to WAN(kbps)	WAN to LAN(kt		LAN to WAN(kbps)	WAN to LAN(kbps)
	site210- WL-1	public_internet	Select WAN Link 🔻	Disabled	1000000	1000000			
	site210- WL-2	public_internet	Select WAN Link 🔻	Disabled	1000000	1000000			
	site210- WL-4	public_internet	Select WAN Link 🔻	Disabled	1000000	1000000			
	site210- WL-5	public_internet	Select WAN Link 🔻	Disabled	1000000	1000000			

5. When a site is chosen, the public internet WAN links that are associated with the selected site are displayed, along with the appliance model information and the region in which the appliance is deployed.

6. Select the WAN links that you would like to use for Cloud Direct service traffic, along with the WAN Link Type, Application Objects, Subscription Bandwidth, Primary POP, and Secondary POP options.

Note

- Up to four WAN links are supported for Cloud Direct service.
- A WAN link bandwidth is no longer needed to be reserved exclusively for the Cloud Direct service. If the Cloud Direct service is not active then the other services such as virtual path, internet, or intranet services configured on that WAN link can use the bandwidth as per the configured shares.

ne:		Mode			Regio		
)	•	cb2	10		Defa	ult Region	
to four WAN	Links:					1	
				Permi	itted Rate	Bandwidth for G	Cloud Direct Service
WAN Link	Access Type	WAN Link Type	Standby Mode	LAN to WAN(kbps)	WAN to LAN(kbps)	LAN to WAN(kbps)	WAN to LAN(kbps)
site210-WL- 1	public_internet	Fiber •	Disabled	1000000	1000000	1000	1000
site210-WL- 2	public_internet	T1/T3 *	Disabled	1000000	1000000	1000	1000
site210-WL- 4	public_internet	Select WAN Link 🔻	Disabled	1000000	1000000		
site210-WL- 5	public_internet	Select WAN Link 🔻	Disabled	1000000	1000000		
nal NAT							
on Objects:				Subscription	n Bandwidth:		
ternet Traffic				10Mbps	*		
POP:				Secondary	POP:		
	Ito four WAN WAN Link site210-WL- 1 site210-WL- 2 site210-WL- 5 5 non Objects: ternet Traffic	v v	w cb2 ito four WAN Links: wan Link WAN Link Access Type WAN Link Type site210-WL- public_internet Fiber 2 public_internet T1/T3 site210-WL- public_internet T1/T3 2 public_internet Select WAN Link * site210-WL- public_internet Select WAN Link * site210-WL- public_internet Select WAN Link * no Objects: sternet Traffic sternet Traffic	v cb210 ito four WAN Links: WAN Link Access Type WAN Link Type Standby Mode site210-WL- public_internet Fiber Disabled site210-WL- public_internet T1/T3 Disabled site210-WL- public_internet Select WAN Link * Disabled a on Objects: Select WAN Link * Disabled	Image: Select WAN Link Type Image: Select WAN Link Type Standby Mode Image: LAN to WAN(kbps) WAN Link Access Type WAN Link Type Standby Mode Image: LAN to WAN(kbps) site210-WL- public_internet Fiber Image: Disabled 1000000 site210-WL- public_internet T1/T3 Image: Disabled 1000000 site210-WL- public_internet Select WAN Link * Disabled 1000000 4 public_internet Select WAN Link * Disabled 1000000 5 public_internet Select WAN Link * Disabled 1000000 5 public_internet Select WAN Link * Disabled 1000000 6 Image: Comparison of the	Image: marked base of the second s	Image: cb210 Default Region ito four WAN Links: Image: cb210 WAN Link Access Type WAN Link Fiber Disabled 1000000 1000000 1000000 1000000 1000000 site210-WL- public_internet Select WAN Link * Disabled 1000000 1000000 1000000 site210-WL- public_internet Select WAN Link * public_internet Select WAN Link * Disabled 1000000 non Objects: Subscription Bandwidth: 1000000 10Mbps *

- Site Name: Displays the sites that are eligible for the Cloud Direct feature deployment.
- **Model**: For the selected site, corresponding appliance model name is auto populated.
- **Region**: For the selected site, the appliance specific deployed region details are auto populated.
- WAN Link: For the selected site, the associated public internet WAN links are displayed.
- WAN Link Type: Select the WAN link type from the menu.
- Standby Mode: The standby mode is retrieved from the WAN link configuration.
- **Bandwidth for Cloud Direct Service**: Enter the bandwidth that the Cloud Direct Service can use exclusively. The selected bandwidth must be lesser than the configured permitted

bandwidth and would not be available for use by the Virtual Path, Internet, and Intranet services.

- **External NAT**: It is required that the public internet traffic originated from the branch LAN network is source NAT from a specific IP address. By default, this is automatically performed and taken care as part of the SD-WAN network configuration. If you would like to configure the NAT IP (LAN Network) outside the SD-WAN device (for example, in an external firewall), you can choose the External NAT option when deploying sites. The IP to which the LAN traffic has to be the source NAT is available in the **Details** page of the deployed Cloud Direct site.
- **Application objects**: You can choose specific application objects or select "All Internet Traffic"to be redirected through the Cloud Direct service. In case when the specific application objects are selected, the traffic for those applications is sent through the Cloud Direct service, and the rest of the traffic is steered using the internet service configured on the appliance.
- **Subscription bandwidth**: Subscription bandwidth is associated with the licensing for the cloud direct service.
- **Billing Mode**: When a customer plans to deploy a Cloud Direct site as part of validating proof of concept (POC), the **Billing Mode** field must set as **Demo**. For all other cases, set the billing mode as **Production**.

NOTE: The following situation occurs, if the **Billing Mode** is selected as **Demo** or **Production**:

- If a Cloud Direct site is created with **Billing Mode** as **Demo**, the settings can be edited to Production.
- If a Cloud Direct site is created with **Billing Mode** as **Production**, the setting cannot be edited to **Demo**.

The **Billing Mode** option enables the use of Cloud Direct trial/evaluation licenses, which can be provided by Citrix sales or authorized partners. Sites operating with Cloud Direct evaluation licenses must be set to the **Demo Billing Mode** option. Sites upgrading to full Cloud Direct subscription licenses must be set to the **Production Billing Mode** option.

- **Primary/Secondary POP**: Ensure that the primary and secondary POP is not the same. Select the POPs depending on the location proximity. Click **Add**.
- 7. After the sites are added, the service status is shown as **Deployment is Pending**. Select the site for which you want to deploy Cloud Direct service and click **Deploy**.

dd	Edit									Pull	Active Conf
Show	100 \$ entries	Search:									
	Site Name		WAN Links					Subscription			
	Site Name	Link Names	LAN to WAN (kbps)	WAN to LAN (kbps)	Region	Primary POP	Secondary POP	Bandwidth (Mbps)	Service Status	Appliance Status	Details
	site210	site210-WL-1	1000	1000	Default	SEA(Seattle, WA)	LAX(Los Angeles,	10Mbps	Deployment	N/A	0
•	SILEZTO	site210-WL-2	1000	1000	Region	SEA(Seattle, WA)	CA)	TOMBPS	Pending	N/A	
Deple	Disable De	elete								Previous	1 Next
ense l	Details										
	Details	Search:									
			Available	Used		Lic	ense Expiry		Grace Per	riod Remaining	

A notification stating that the deploy operation initiates a change management on the MCN appliance is displayed. You can click **Yes** or **No**.

Site Det	ails										
Add	Edit									Pull	Active Config
Show	100 🌲 entries	Search:									
	Site Name		WAN Lin	ks				Subscription			
	Site Name 🛪	Link Name	es	Deploy Sites	5		× POP	Bandwidth (Mbps)	Service Status	Appliance Status	Details
	site210	site210-WL-1 site210-WL-2			nent will initiate Ch t to continue?	ange Management. Do	(Los Angeles,	10Mbps	Deployment Pending	N/A	0
Dep	loy Disable D	elete			Yes	No				Previous	1 Next
License	Details										
Show	100 🛊 entries	Search:									
	Bandwidth (M	bps) 🔨	Avail	able	Used	Lic	ense Expiry		Grace Per	iod Remaining	
10			1		0	Sun Dec 01 00:00:00 2	2019				
Showi	ng 1 to 1 of 1 entries									Previous	1 Next

 \bigodot Ensuring appliance readiness for the Cloud Direct configuration change

Site Det	ails										
Add	Edit									Pull .	Active Config
Show	100 ¢ entries	Search:									
	Site Name		WAN Links					Subscription			
	Site Name	Link Name	LAN to WAN (kbps)	WAN to LAN (kbps)	Region	Primary POP	Secondary POP	Bandwidth (Mbps)	Service Status	Appliance Status	Details
	site210	site210-WL-1 site210-WL-2	1000	1000 1000	Default Region	SEA(Seattle, WA)	LAX(Los Angeles, CA)	10Mbps	Deployment Pending	N/A	0
Depl	oy Disable De	elete								Previous	1 Next
License	Details										
Show	100 \$ entries	Search:									
	Bandwidth (Ml	bps) 🔨	Available	Used		Lic	ense Expiry		Grace Per	iod Remaining	
10			1	0	S	Sun Dec 01 00:00:00	2019				
Showi	ng 1 to 1 of 1 entries									Previous	1 Next

Change Management Status: Verifying config file on MCN

Site Det	ails										
Add	Edit									Pull A	Active Config
Show	100 \$ entries	Search:									
	Site Name	WAN	Links		Deeler	D-1	6	Subscription	Constant Charlos	And Party Chattan	Detalla
	Site Name A	Link Names	LAN to WAN (kbps)	WAN to LAN (kbps)	Region	Primary POP	Secondary POP	Bandwidth (Mbps)	Service Status	Appliance Status	Details
	site210	site210-WL-1	1000	1000	Default	SEA(Seattle, WA)	LAX(Los Angeles,	10Mbps	Deployment	N/A	0
	SILCE TO	site210-WL-2	1000	1000	Region	Series and	CA)	10110p3	Pending	1071	•
Deple	Disable De	lete								Previous 1	Next
License	Details										

License Details

Show 100 \$ entries Search:				
Bandwidth (Mbps) 🔺	Available	Used	License Expiry	Grace Period Remaining
10	1	0	Sun Dec 01 00:00:00 2019	
Showing 1 to 1 of 1 entries				Previous 1 Next

 ${\sf C}$ Change Management Status: Preparing the change for distribution to all appliances in the network

Site Details

Add	Edit									Pull	Active Confi
Show	100 \$ entries	Search:									
	Site Name		l Links		Region	Primary POP	Secondary POP	Subscription	Service Status	Appliance Status	Details
	Site Name A	Link Names	LAN to WAN (kbps)	WAN to LAN (kbps)	Region	Primary POP	Secondary POP	Bandwidth (Mbps)	Service status	Appliance status	Details
v	site210	site210-WL-1	1000	1000	Default	SEA(Seattle, WA)	LAX(Los Angeles,	10Mbps	Deployment	N/A	0
		site210-WL-2	1000	1000	Region		CA)		Pending		Ŭ
Dep	loy Disable D	elete								Previous	Next

License Details

Show 100 \$ entries Search:				
Bandwidth (Mbps) 🔨	Available	Used	License Expiry	Grace Period Remaining
10	1	0	Sun Dec 01 00:00:00 2019	
Showing 1 to 1 of 1 entries				Previous 1 Next

igcap Change Management Status: Activating the changes in the network. Please wait.

Site Det	ails										
Add	Edit									Pu	II Active Config
Show	100 ¢ entries	Search:									
			WAN Links					Subscription			
	Site Name 🤸	Link Names	LAN to WAN (kbps)	WAN to LAN (kbps)	Region	Primary POP	Secondary POP	Bandwidth (Mbps)	Service Status	Appliance Status	Details
V	site210	site210-WL-1 site210-WL-2	1000 1000	1000 1000	Default Region	SEA(Seattle, WA)	LAX(Los Angeles, CA)	10Mbps	Deployment Pending	N/A	0
Depl	oy Disable De	lete								Previous	1 Next
License	Details										
Show	100 🛊 entries	Search:									
	Bandwidth (M	bps) 🔨	Available	Used		Lic	ense Expiry		Grace Per	iod Remaining	
10			1	0	5	Sun Dec 01 00:00:00	2019				
Showin	ng 1 to 1 of 1 entries									Previous	1 Next

	ils										
	Edit									Pull	Active Co
ow	100 ¢ entries	Search:									
	Site Name	WA	N Links				6	Subscription			
	Site Name	Link Names	LAN to WAN (kbps)	WAN to LAN (kbps)	Region	Primary POP	Secondary POP	Bandwidth (Mbps)	Service Status	Appliance Status	Details
	site210	site210-WL-1	1000	1000	Default	SEA(Seattle, WA)	LAX(Los Angeles,	10Mbps	Deployed	Enabled	0
		site210-WL-2	1000	1000	Region	55 45 66 66 7 10 9	CA)		o oprofeo	LINGING	Ŭ
Deplo	y Disable De	lete								Previous	1 Nex
nse [Details										
iow	100 \$ entries	Search:									
011	roo y entites	Search									

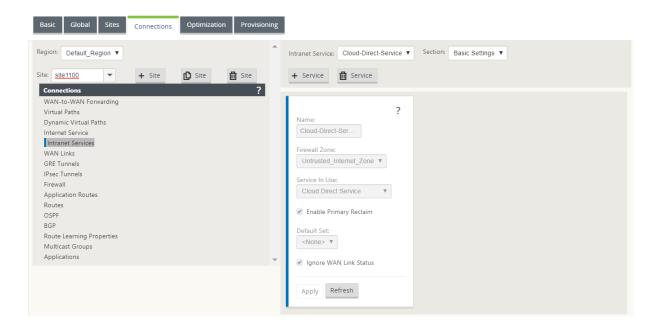
After successfully deploying the sites, the cloud direct service page displays the following:

- Service status: Deployed
- Appliance status: Enabled
- Subscription Bandwidth (Mbps): 10 Mbps
- Consumed the installed license

The above change management step auto generate and add the needed Cloud Direct service configurations to the running configuration.

Note

The auto-created **Cloud Direct Service** (intranet service) is associated with the Default_RoutingDomain.



Firewall Settings

Connections ?									
NAN-to-WAN Forwarding		+							
/irtual Paths									
Dynamic Virtual Paths		Priority	Direction	Туре	Service	Inside Zone	Inside IP Address	Outside Zone	Outside IP Addre
nternet Service					CI 1				
ntranet Services				Port	Cloud-				
NAN Links		(Auto)	Outbound		Direct-	*	198.18.101.2/32	Untrusted_Internet_Zone	
GRE Tunnels				Restricted	Service				
Psec Tunnels									
Firewall		100	Outbound	Port	Internet	*	0.0.0/0	Untrusted_Internet_Zone	
Application Routes			outoound	Restricted			0101010/0	onnaorea_nnendeone	
Routes					Cloud-				
DSPF				Port					
3GP		(Auto)	Outbound	Restricted	Direct-	*	198.18.102.2/32	Untrusted_Internet_Zone	
Route Learning Properties				Restricted	Service				
Multicast Groups					Cloud-				
Applications	-			Port					
		(Auto)	Outbound	Restricted	Direct-	*	198.18.103.2/32	Untrusted_Internet_Zone	
				Restricted	Service				
					Cloud-				
				Port					
		(Auto)	Outbound	Restricted	Direct-	*	198.18.104.2/32	Untrusted_Internet_Zone	
				Restricted	Service				
					Cloud-				
				Port	Cloud-				
		(Auto)	Outbound		Direct-	Any	*	Untrusted_Internet_Zone	209.202.233.198
				Restricted	Service				
			_						
		Apply	Refresh						

Provisioning Sites in SD-WAN application GUI

Region: Default_Region ▼	•	WAN Link: site1100-WL-6	•											
Site: site1100 V + Site D Site Site Provisioning ? Groups Services	v	Filter by Group: LAN	to WAN Permitted F	late (kbps):	100000	WAN to I	.AN Permitt	ed Rate (kb	ps): 10000	000				2 LAN to WAN
				_		LAN to WAN					WAN to LAN			
		Name 🔨	Group	Min (kbps)	Max (kbps)	Shares of Group	Fair (kbps)	Sum Remote (kbps)	Min (kbps)	Max (kbps)	Shares of Group	Fair (kbps)	Sum Remote (kbps)	
		Cloud-Direct-Service	Default V	500	500	0	500	N/A	500	500	0	500	N/A	WAN to LAN
		dc2100	Default •	80	no limit	1000	499740	10000	80	no limit	1000	499740	10000	
		 internet 	Default	100	no limit	1000	499760	N/A	100	no limit	1000	499760	N/A	
		Totals:		6	80 50	2000	100000	1	680	500	2000	100000)	
		Apply Refresh												

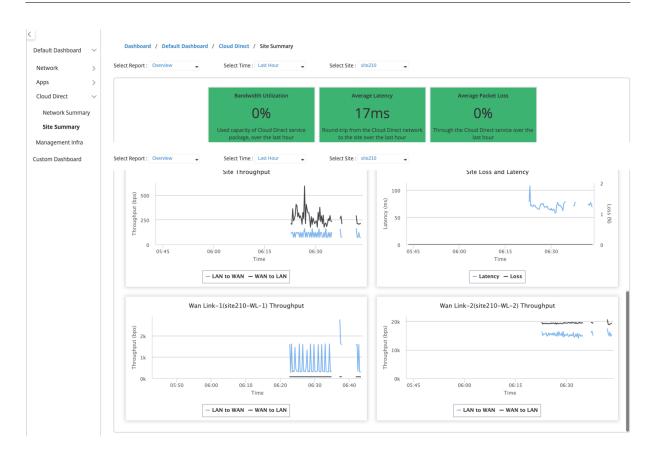
Monitoring Cloud Direct service

You can view the configured Cloud Direct service after the sites are deployed and enabled. Click the exclamation icon in the **Details** column to view the site details.

Cloud Direct Site Details			×
Site Info			
Site Name: she250 NAT: External (148.163.177.2/32) Application Object: All internet Traffic	Site Health: Site Site Site Site Site Site Site Site		Nance Status: Drubled
WAN Links			
Status Healty LAN to MAN	Status Status Healby LAN to WAN	www.3	WORKN 4
1000Mps WAN 19 LAN 1000Mps	1000Altys WAN to LAN 1000Altys		
Type Hiter Protocol Static	Tppe Tp/T3 Protocol DHCP	Unconfigured	Unconfigured
Static IP Address 17214.28 Subnet Mask 205.255.255.0	Static IP Address N/A Subnet Mask N/A		
Gateway IP Address 17236-21	Gabeway IP Address N/A		
Standby Mode Disabled	Standby Mode Disabled		

You can view the site summary graphs by navigating to **Dashboard** > **Cloud Direct** > **Network Summary** and **Site Summary**.

Dashboard		Monitoring	Configuration I	Reporting Administ	ration Nitro API		
C Default Dashboard Network	~	Dashboard / Default Dash Cloud Direct: Summary	board / Cloud Direct / Ne	twork Summary			
Apps Cloud Direct Network Sumn Site Summary Management Infra		1 Total Sites	O Offline	1 Wan Link Issues	O Healthy	6 POPs	 Site is offline and all WAN Links are down. Site is up and running, but one or more WAN Links have performance issues. Site is up and running without any issues.
Custom Dashboard		Show 10 ¢ entries site210 Showing 1 to 1 of 1 entries	Search: Site Name		Subscription	n Bandwidth	Status Wan Link Issues Previous 1 Next



Editing site in SD-WAN Center

You can choose to edit the sites to modify bandwidth and wan link type.

Note

POP selections cannot be edited.

id E	dit									Pull	Active Con
how	100 🛊 entries	Search:									
			WAN Links					Subscription			
	Site Name 🧥	Link Names	LAN to WAN (kbps)	WAN to LAN (kbps)	Region	Primary POP	Secondary POP	Bandwidth (Mbps)	Service Status	Appliance Status	Details
	site210	site210-WL-1	1000	1000	Default	SEA(Seattle, WA)	LAX(Los Angeles,	10Mbps	Deployed	Enabled	0
	SILEZ TO	site210-WL-2	1000	1000	Region	SEA(Seattle, WA)	CA)	TOWDPS	Deployed	Enabled	•
Deplo	y Disable De	lete								Previous	1 Next
ense [
	100 ¢ entries	Search:									
	100 🛊 entries Bandwidth (MB		Available	Used		Lic	ense Expiry		Grace Per	iod Remaining	

A													
No No		lication objects,	nternet service	e must be Mod	-	on the	site.		Regior				
ite21		Ŧ			210					It Region			
										0			
lect i	ipto four WAN	LINKS:						Permitted Ra	t		Dan duridah fa	Cloud Direct Co	redee
								Permitted Ka			bandwidth it	or Cloud Direct Se	rvice
se 🔨	WAN Link	Access Type	WAN Link	Туре	Standby	/ Mode	LAN to WAN(k	(bps) WAN	to LAN(kbps)	LAN t	o WAN(kbps)	WAN to LA	AN(kbps)
	site210- WL-1	public_internet	Fiber	Ŧ	Disable	ed	1000000	1000	000	1000		1000	
2	site210- WL-2	public_internet	T1/T3	Ŧ	Disable	ed	1000000	1000	000	1000		1000	
	site210- WL-4	public_internet	Select WAN L		Disable	ed	1000000	1000	000				
	site210- WL-5	public_internet	Select WAN L	.ink 🔻	Disable	ed	1000000	1000	000				
	rnal NAT tion Objects:						Subscr	iption Bandw	dth:				
	nternet Traffic						10Mb		*				
	/ POP: eattle, WA)	v						dary POP: Los Angeles, C	A) v				
		¥							A) v				Арр
EA(S Site	eattie, WA) edited for Clouc								A) *			Pull	
Site	eattle, WA) edited for Cloud								A) *			Pull	
Site	edited for Cloud ails Edit	d Direct service.	WAN Links									Pull	
Site Det	edited for Cloud ails Edit	d Direct service.	LAN		/AN to LAN (kbps)	Region			Suberrin		Service Status	Pull Appliance Status	Active C
Site Det	edited for Cloud ails Edit	d Direct service.	nes LAN (i	to WAN W	(kbps)	Region		.os Angeles, C	p Subscrip Bandwidth	(Mbps)	Service Status Redeployment Pending		Active C
Site Det d	edited for Cloud ails Edit 100 ¢ entries Site Name	Direct service. Search: Link Nar site210-WL-1 site210-WL-2	nes LAN (i	to WAN W kbps)	(kbps)	Default	Primary POP	LAX(Los Angel	P Subscript Bandwidth	(Mbps)	Redeployment	Appliance Status	Active C Details
EA(S Site Det d Depl	edited for Cloud ails Edit Site Name site210	Direct service. Search: Link Nar site210-WL-1 site210-WL-2	nes LAN (i	to WAN W kbps)	(kbps)	Default	Primary POP	LAX(Los Angel	P Subscript Bandwidth	(Mbps)	Redeployment	Appliance Status	Active C Details
Site Det d Depl	edited for Cloud ails Edit 100 ¢ entries Site Name site210 oy Disable	Direct service. Search: Link Nar site210-WL-1 site210-WL-2	nes LAN (i	to WAN W kbps)	(kbps)	Default	Primary POP	LAX(Los Angel	P Subscript Bandwidth	(Mbps)	Redeployment	Appliance Status	Active Co Details
Site Det d Depl	edited for Cloud ails Edit 100 ¢ entries Site Name site210 Details	I Direct service. Search: Link Nar site210-WL-1 site210-WL-2 Delete Search:	nes LAN (i	to WAN W kbps) 2000	(kbps)	Default	Primary POP SEA(Seattle, WA)	LAX(Los Angel	P Subscript Bandwidth	(Mbps)	Redeployment Pending	Appliance Status	

The service status displays as redeployment pending. Deploy the site. The deployment process is completed for the edited site.

Site Details								
Add Edit							Pull	Active Config
Show 100 \$ entries	Search:							
Site Name		WAN Links		ondary POP	Subscription	Service Status	Appliance Status	Details
	Link Name	Deploy Sites	×		Bandwidth (Mbps)	Service Status	Appliance status	Details
site210	site210-WL-1 site210-WL-2	Deployment will you want to con	ll initiate Change Management. Do ntinue?	(Los Angeles,	10Mbps	Redeployment Pending	Enabled	0
Deploy Disable	Delete		Yes No				Previous	1 Next
License Details								
Show 100 \$ entries	Search:							
Bandwidth (Mbps) 🔨	Available Us	sed Licer	se Expiry		Grace Per	iod Remaining	
10		0 1	Sun Dec 01 00:00:00 20	19				
Showing 1 to 1 of 1 entrie	25						Previous	1 Next
 Cloud Direct configur 	ation change comple	ted successfully						

Site Details

					1						
	Site Name	WA	N Links					Subscription			
	Site Name	Link Names	LAN to WAN (kbps)	WAN to LAN (kbps)	Region	Primary POP	Secondary POP	Bandwidth (Mbps)	Service Status	Appliance Status	Details
	site210	site210-WL-1 site210-WL-2	1000 3000	1000 3000	Default Region	SEA(Seattle, WA)	LAX(Los Angeles, CA)	10Mbps	Deployed	Enabled	0
eploy	Disable De	lete								Previous	1 Nex
	etails										
ise D											
	00 🛊 entries	Search:									
	00 ¢ entries Bandwidth (Mi		Available	Used		Lic	ense Expiry		Grace Per	iod Remaining	

Enable and Disable Site

You can enable a deployed site that has an appliance status shown as disabled. To enable a site, click **Enable**.

											II Anti-un C
Ec	dit									Pu	ll Active C
v 1	00 🛊 entries	Search:									
	Site Name		WAN Links		Region	Primary POP	Secondary POP	Subscription	Service Status	Appliance Status	Details
	Site Name X	Link Names	LAN to WAN (kbps)	WAN to LAN (kbps)	Region	Primary POP	Secondary POP	Bandwidth (Mbps)	Service Status	Appnance status	Details
	site210	site210-WL-1 site210-WL-2	1000 3000	1000 3000	Default Region	SEA(Seattle, WA)	LAX(Los Angeles, CA)	10Mbps	Deployed	Disabled	0
oloy	Enable Dis	able Delete								Previous	1 Ne
e D	etails										
1	00 \$ entries	Search:									
	Bandwidth (Mb	ops) 🔨	Available	Used		Lie	cense Expiry		Grace Pe	riod Remaining	
			0	1	S	un Dec 01 00:00:00	2019				
										Previous	1 Ne
lou	d Direct Service en	abled successfully.									
eta		abled successfully.								Pull	Active Co
eta	ils	abled successfully.								Pull	Active Co
eta	ils		WAN Links s LAN to WAY (kbps)	WAN to LAN (kbps)	Region	Primary POP	Secondary POP	Subscription Bandwidth (Mbps)	Service Status	Pull Appliance Status	Active Co Details
eta	ils idit	Search:	LAN to WA		Region	Primary POP SEA(Seattle, WA)	Secondary POP LAX(Los Angeles, CA)		Service Status Deployed		
eta	ils dit 100 entries Site Name A site210	Search: Link Name site210-WL-1	s LAN to WAN (kbps) 1000	(kbps) 1000	Default		LAX(Los Angeles,	Bandwidth (Mbps)		Appliance Status	Details
eta w	ils dit 100 entries Site Name A site210	Search: Link Name site210-WL-1 site210-WL-2	s LAN to WAN (kbps) 1000	(kbps) 1000	Default		LAX(Los Angeles,	Bandwidth (Mbps)		Appliance Status	Details
w (************************************	ils dit 100 • entries Site Name A site210 y Enable Dis	Search: Link Name site210-WL-1 site210-WL-2	s LAN to WAN (kbps) 1000	(kbps) 1000	Default		LAX(Los Angeles,	Bandwidth (Mbps)		Appliance Status	Details
eplor se C	ils dit 100 • entries Site Name ~ site210 y Enable Dis Details	Search: Link Name site210-WL-1 site210-WL-2 able Delete Search:	s LAN to WAN (kbps) 1000	(kbps) 1000	Default	SEA(Seattle, WA)	LAX(Los Angeles,	Bandwidth (Mbps)	Deployed	Appliance Status	0

Click **Disable** to disable a deployed site. Disabling site would no longer use cloud direct service to steer the internet traffic. All traffic is redirected through the internet service, if configured on the appliance.

Site Details

Edit									ru	ll Active Co
w 100 \$ entries	Search:			-						
Site Name	W	AN Links		Region	Primary POP	Secondary POP	Subscription	Service Status	Appliance Status	Details
	Link Names	LAN to WAN (kbps)	WAN to LAN (kbps)		,		Bandwidth (Mbps)			
site210	site210-WL-1 site210-WL-2	1000 3000	1000 3000	Default Region	SEA(Seattle, WA)	LAX(Los Angeles, CA)	10Mbps	Deployed	Enabled	0
eploy Disable D	elete								Previous	1 Nex
e Details										
Bandwidth (N	Search:	As an Hank La	lied			energy Revelues		6	and the second states of	
Bandwidth (w	0	Available	Used		Li Sun Dec 01 00:00:00	cense Expiry		Grace Pe	eriod Remaining	
Cloud Direct Service di	sabled successfully.									×
Details									Pull /	× Active Confi
Details	Search								Pull /	× Active Confi
Details	Search	AN Links (AN to WAN (Khos)	WAN to LAN	Region	Primary POP	Secondary POP	Subscription Bandwidth (Mbps)	Service Status	Pull <i>i</i> Appliance Status	Active Confi
Details Edit w 100 \$ entries Site Name A	Search W/		WAN to LAN (kbps) 1000 3000	Region Default Region	Primary POP SEA(Seattle, WA)	Secondary POP LAX(Los Angeles, CA)		Service Status Deployed		
Details Edit w 100 € entries Site Name ∧ site210	Search W/ Link Names site210-WL-1	LAN to WAN (kbps) 1000	WAN to LAN (kbps) 1000	Default		LAX(Los Angeles,	Bandwidth (Mbps)		Appliance Status	Details
Details Edit 100 \$ entries Site Name \$ site210 eploy Disable D	Search W/ Link Names site210-WL-1 site210-WL-2	LAN to WAN (kbps) 1000	WAN to LAN (kbps) 1000	Default		LAX(Los Angeles,	Bandwidth (Mbps)		Appliance Status	Details
Details Edit w 100 ÷ entries Site Name A site210 leploy Disable D use Details	Search W/ Link Names site210-WL-1 site210-WL-2	LAN to WAN (kbps) 1000	WAN to LAN (kbps) 1000	Default		LAX(Los Angeles,	Bandwidth (Mbps)		Appliance Status	Details
site210	Search Link Names site210-WL-1 site210-WL-2 elete	LAN to WAN (kbps) 1000	WAN to LAN (kbps) 1000	Default	SEA(Seattle, WA)	LAX(Los Angeles,	Bandwidth (Mbps)	Deployed	Appliance Status	Details

Site Deletion

You can choose to delete the sites that no longer require Cloud Direct connectivity. To delete sites, select the site and click **Delete**. A confirmation message to delete sites is displayed. All cloud direct service configuration is removed through the change management process.

Site Details

Add Ed	dit									Pull Activ	ve Config
Show 1	00 \$ entries	Search:									
		WAN Links						Subscription			
	Site Name 🧥	Link Names	LAN to WAN (kbps)	WAN to LAN (kbps)	Region	Primary POP	Secondary POP	Bandwidth (Mbps)	Service Status	Appliance Status	Details
	site210	site210-WL-1 site210-WL-2	1000 3000	1000 3000	Default Region	SEA(Seattle, WA)	LAX(Los Angeles, CA)	10Mbps	Deployed	Enabled	0
Deploy Disable Delete								Next			
icense D	etails										
Show 1	00 \$ entries	Search:									
Bandwidth (Mbps) 🔥 Available Used						License Expiry Grace Period Remaining					
10 0 1 Su						Sun Dec 01 00:00:00 2019					
Showing	1 to 1 of 1 entries										

Site Detai	ls									
Add Ec	lit								Pull Acti	ve Config
Show 1	00 🛊 entries	Search:								
			WAN Links			Secondary POP	Subscription		Appliance Status	Details
	Site Maine A	Link Name	es Delete Sites		×		Bandwidth (Mbps)	Service Status	Appliance status	Details
	site210	site210-WL-1 site210-WL-2	Deleting Are you s Service fo	sites will initiate Cha sure you want to del or the selected site(s	ange Management. lete the Cloud Direct s)?	LAX(Los Angeles, CA)	10Mbps	Deployed	Enabled	0
Deploy Disable Delete			_	Yes	0				Previous 1	Next
License D	etails									
Show 1	00 🛊 entries	Search:								
Bandwidth (Mbps) 🔺 🛛 A		Available	Available Used		ense Expiry		Grace Period Remaining			
10 0			0	1	Sun Dec 01 00:00:00 20	019				
Showing	1 to 1 of 1 entries								Previous 1	Next

 \bigcirc Ensuring appliance readiness for the Cloud Direct configuration change

Site De	tails	5										
Add	Edi	t									Pull Activ	ve Config
Show	10	0 🛊 entries	Search:									
		Cite Manage	WAN Links						Subscription			
		Site Name 🤸	Link Name	LAN to WAN (kbps)	WAN to LAN (kbps)	Region	Primary POP	Secondary POP	Bandwidth (Mbps)	Service Status	Appliance Status	Details
		site210	site210-WL-1 site210-WL-2	1000 3000	1000 3000	Default Region	SEA(Seattle, WA)	LAX(Los Angeles, CA)	10Mbps	Deletion in Progress	N/A	0
Dep	oloy	Disable Del	ete								Previous 1	Next
License	e De	tails										
Show	10	0 🛊 entries	Search:									
	Bandwidth (Mbps) Available Use		Used		License Expiry			Grace Period Remaining				
10	10 0 1			Sur	Sun Dec 01 00:00:00 2019							
Showi	ing 1	to 1 of 1 entries									Previous 1	Next

Previous 1 Next

Cloud Direct configu	ation change complet	ed successfully								
Details										
d Edit									Pull Activ	ve C
now 100 🛊 entries	Search:									
Site Name		WAN Links					Subscription			Deta
Site Name	Link Name	LAN to WAN (kbps)	WAN to LAN (kbps)	Region	Primary POP Se	Secondary POP	Bandwidth (Mbps)	Service Status	Appliance Status	De
No sites deployed for C	oud Direct service.									
Deploy Disable	Delete								Previous	Ne
o is a second										
nse Details										
now 100 🛊 entries	Search:									
Bandwidth (Mbps)		Available	Used		Lice	nse Expiry		Grace Peri	od Remaining	_
10 1		1	0	Sur	n Dec 01 00:00:00 20					
10										

Cloud Direct Service status on Citrix SD-WAN

You can verify the Cloud Direct service status on a local SD-WAN appliance.

Go to the Citrix SD-WAN GUI, navigate to **Configuration** > expand the **Appliance Settings** > select **Cloud Direct Service**.

Dashboard Monitoring	Configuration
- Appliance Settings - Administrator Interface - Logging/Monitoring	Configuration > Appliance Settings > Cloud Direct Service Cloud Direct Service
– Network Adapters – Net Flow – App Flow/IPFIX	Cloud Direct service has been configured and running currently.
- SNMP - NITRO API - Licensing	
Cloud Direct Service + Virtual WAN	
+ System Maintenance	

Click **Disable** option to disable the Cloud Direct service.

Dashboard Monitoring	Configuration
- Appliance Settings	Configuration > Appliance Settings > Cloud Direct Service
- Administrator Interface - Logging/Monitoring	Cloud Direct Service
 Network Adapters Net Flow App Flow/IPFIX 	Cloud Direct service has been configured but disabled currently. Please re-enable from the SDWAN Center.
SNMP	
- NITRO API	
+ Virtual WAN	
+ System Maintenance	

Troubleshooting

The most common error messages that might occur on SD-WAN Center when deploying Cloud Direct service are as follows.

Error/status messages are displayed on SDW-AN Center under **Configuration** > **Cloud Connectivity** > **Cloud Direct**.

'Cloud Direct License error! Please upload additional license for {bandwidth} Mbps bandwidth'

 Upload a valid Cloud Direct license on SD-WAN Center by navigating to Configuration > Licensing > File Management option and then proceed with deploying this feature

'Cloud Direct configuration HA due to Citrix Cloud Workspace login issue'

 Reenter credentials for Citrix Cloud Workspace login on SD-WAN Center by navigating to Configuration > Cloud Connectivity option.

'Cloud Direct configuration processing error! Site: {site_name}(IP: {mgmt_ip}) is not reachable or is missing Cloud Direct support'

• Check if SD-WAN appliance or appliances (in case of HA deployment) are reachable on the management port.

'Cloud Direct configuration HA Config Check error for site: {site_name}'

• Check for connectivity of both appliances in HA pair corresponding to site being deployed.

'Both the HA Pair Appliances have to be reachable to perform Cloud Direct Configuration'

• When deploying Cloud Direct service on SD-WAN appliances in HA pair, both secondary and primary appliances must be reachable on the management port.

'Cloud Direct configuration processing error! Site: {site_name}(IP: {mgmt_ip}) has SSO Login Issue'

• Check if SD-WAN appliance is up/running and reachable on the management port. This error is displayed when SD-WAN Center is unable to perform single sign-on to the SD-WAN appliance.

'Internal error encountered during Cloud Direct configuration processing'

• This might occur due to multiple error conditions while carrying out configuration check or rest of the processing. A user might need to review the logs and perform the operation again.

'Cloud Direct configuration processing canceled! MCN is not ready for change management'

• Check if MCN is accessible and up and running and that its change management state is "network_staging."

'Cloud Direct configuration processing error! Site: {site_name}(IP: {mgmt_ip}) does not have Cloud Direct support. Please do single step upgrade to have a Cloud Direct support'

 Perform single step software upgrade on the SD-WAN appliance through MCN > Change Management. After this procedure, reattempt deploying Cloud Direct service for this site.

'Cloud Direct configuration processing error! SD WAN change management operation failed'

• Change management operation somehow did not succeed. Check SD-WAN Center logs for details.

'Cloud Direct configuration processing error! Enabling service at site: {site_name} failed'

• Unable to enable Cloud Direct service on SD-WAN appliance. Check for connectivity of specific appliance or for those in HA pair or for any issue when performing single sign-on. Check logs on SD-WAN Center and appliance for details.

'Cloud Direct configuration processing error! Disabling service at site: {site_name} failed'

• Unable to disable Cloud Direct service on SD-WAN appliance. Check for connectivity of specific appliance or those in HA pair or for any issue when performing single sign-on. Check logs on SD-WAN Center and appliance for details.

'Cloud Direct configuration processing error! Config image push to site: {site_name} failed'

• Unable to upload service-specific image on appliance via REST api or not able to access both appliances in HA pair.

'Cloud Direct Service encountered an error during configuration processing. Audit errors found in the SD WAN config!'

• Audit errors found when attempting to compile the SD-WAN config. Check SD-WAN Center logs for details.

'Cloud Direct configuration processing error! Create Site failed for Site: {site_name}'

• Service-side error when attempting to create a site for the corresponding SD-WAN appliance. Review SD-WAN Center logs for additional details.

'Cloud Direct configuration processing error! Update Site failed for Site: {site_name}'

• Service-side error when attempting to modify site related settings for the corresponding SD-WAN appliance. Review SD-WAN Center logs for additional details.

Error messages seen in logs (SDWAN_common.log)

Here are few scenarios where Cloud Direct service is deployed on SD-WAN appliance, but might not function as expected. You can download and review the logs on the local SD-WAN appliance using the SDWAN_common.log for more details.

Scenario 1

"Detected Cloud Direct VM is not responding ...Disabling Cloud Direct Service now!""Cloud Direct service has been disabled." Underlying KVM running on local SD-WAN appliance is not functioning in expected manner. In such case, Cloud Direct service functionality is disabled on the appliance.

Scenario 2

"No tunneled packets seen for past 5 mins ...Disabling Cloud Direct Service now!" "Cloud Direct service has been disabled." There is no tunnel established between SD-WAN appliance and tunnel endpoint in-use for Cloud Direct service. This might be due to misconfiguration of wan-link, lack of internet connectivity over configured wan-link, incompatible or invalid data/config image pushed to appliance or any firewall rule that might be dropping UDP tunnel packets when received over wan-link. In such case, Cloud Direct service functionality is disabled on the appliance.

When you activate a configuration on MCN with different Cloud Direct configuration (For example: NAT configuration is changed for Cloud Direct) and it might lead to the permanent interruption of traffic. To overcome this block, you can follow either one of the following steps to select the different routes present on the appliance:

 In the SD-WAN Center GUI, navigate to Configuration > Cloud Connectivity > Cloud Direct. Select the cloud direct appliance and click Disable option to disable the cloud direct service.

Dashboard	Fault	: Мо	onitoring	Configuration	Reporting) Ad	Iministra	ation Ni	tro API				
Ketwork Discovery		Config	uration / Cloud	Connectivity / Cloud D	irect								
Network Configuration													
Zero Touch Deploymen	nt	Site Deta	ils										
Change Management		Add Ed	dit Billing Mode	e: Demo 🔻	X							Pull Act	ive Config
Appliance Settings		Show	100 • entries	Search:									
Mobile Broadband			Site Name 🔺	v	/AN Links		Region	Primary POP	Secondary POP	Subscription Bandwidth (Mbps)	Service Status	Appliance Status	Details
Licensing				Link Names	LAN to WAN (kbps)	WAN to LAN (kbps)				bandwidth (wbps)			
Cloud Connectivity	~		br-RCN	WL	5000	5000	RCN1	XIRX1(Citrix, Santa Clara, CA)	XIRX2(Citrix, Santa Clara, CA)	10Mbps	A Redeployment Required	Enabled	0
Cloud Direct		Deploy	Disable Del	ata								Previous 1	Next
Azure	>	ocpio <u>i</u>		d Direct service on sele	rted sites								
Security	>	License D	_	a an est ser fice on sete									,
		cicense b	como										
		Show	100 🔻 entries	Search:									
			Bandwidth (M	bps) 🔨	Available	Used		Li	cense Expiry		Grace Peri	od Remaining	

 Navigate to Configuration > Cloud Connectivity > Cloud Direct and pull active config to get the clean-up notification. You can click the Cleanup Missing Sites notification button shown for the affected cloud direct appliance. This operation disables Cloud Direct service running on the appliance.

Dashboard	Fault	Mo	onitoring	Configuration	Reporting	Ad	ministra	ation Ni	tro API				
Network Discovery		Config	uration / Cloud	Connectivity / Cloud Dir	ect								
Network Configuration	n	A Sites:	site210, br-RCN(d	uplicate) where Cloud Dir	ect Service were p	reviously cre	ated are r	now missing in the	active SD WAN conf	figuration. Cleanup Mi	ssing Sites		×
Zero Touch Deploymer	nt			uplicate) where Cloud Dir vice settings and sd wan c		reviously cre	ated are r	now missing in the	active SD WAN conf	figuration.Sites br-RCN	l require redeploy	ment due to config	uration ×
Change Management													
Appliance Settings		Site Detai	ils										
Mobile Broadband		Add Ec	Billing Mode	e: Demo 🔻	×							Pu	II Active Config
Cloud Connectivity	~	Show	100 🔻 entries	Search:							1		
Cloud Direct			Site Name 🔺	Link Names	LAN to WAN	WAN to LAN	Region	Primary POP	Secondary POP	Subscription Bandwidth (Mbps)	Service Status	Appliance Status	Details
Azure	>			Link Names	(kbps)	(kbps)							
Security	>		br-RCN	WL	5000	5000	RCN1	XIRX1(Citrix, Santa Clara, CA)	XIRX2(Citrix, Santa Clara, CA)	10Mbps	A Redeployment Required	Enabled	0
		Deploy	Disable Dele	ete								Previous	1 Next
		4											F
		License D	etails										
		Show	100 v entries	Search:									

3. Redeploy the Cloud Direct service on SD-WAN Center to use the Cloud Direct service for affected appliances.

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

March 12, 2021

Citrix SD-WAN and Zscaler help enterprises transform their WAN for cloud migration by providing secure local breakouts to applications and resources hosted on the Internet. New WAN infrastructure technologies such as SD-WAN increase network agility and scale while lowering cost and complexity for an improved user experience in distributed organizations.

SD-WAN solutions simplify routing by allowing traffic destined for the cloud to breakout to the Internet locally. SD-WAN provides flexibility for routing traffic to the Internet (remove central DC environment) by using application steering features. However, exposing the network to the Internet poses significant security risks. A centralized approach to securing local breakout through a cloud service eliminates the overhead of maintaining security infrastructure in the branches. All traffic is reliably and securely routed to Zscaler (cloud-based security platform) with Citrix SD-WAN in the branch network. You can eliminate costly infrastructure and protect your network from threats and vulnerabilities.

Citrix SD-WAN

Citrix SD-WAN helps enterprises move to the cloud by securely enabling local branch-to-Internet breakouts with a built-in stateful firewall for creating policies that can allow or deny Internet access directly from the branch. Citrix SD-WAN identifies applications through a combination of an integrated database of over 4,000 applications, including individual SaaS applications, and uses deep packet inspection technology for real-time discovery and classification of applications. It uses this application knowledge to steer traffic from the branch to the Internet, cloud or SaaS.

Zscaler

Zscaler is the leading cloud-based security platform, which delivers superior security without the need for on-premises hardware, appliances, or software. Zscaler puts a perimeter around the Internet, so that enterprises do not need to put a security perimeter around every office. The Zscaler Cloud Security Platform acts as a series of security check posts in more than 100 data centers around the world. By redirecting internet traffic to Zscaler, enterprises can instantly secure stores, branches, and remote locations. Zscaler connects users and the Internet, inspecting every byte of traffic—even if it is encrypted or compressed—so that users are secure and all hidden threats are identified before they can infiltrate the enterprise network.

Citrix SD-WAN allows creating policies that enable direct Internet breakout from the branch and Zscaler's Cloud Security Platform ensures security for IT by inspecting all internet-bound traffic in a cloud service close to where users connect.

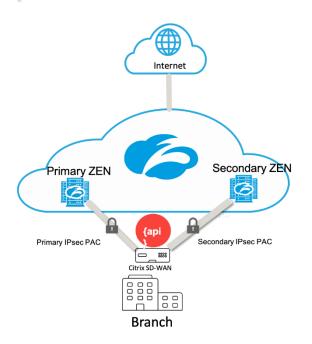
Zscaler enforcement nodes (ZENs)

Citrix SD-WAN supports Zscaler APIs for automating creation of IPsec tunnels between Citrix SD-WAN and Zscaler Enforcement Nodes (ZENs) in Zscaler's cloud network. ZENs are full-featured, inline Internet security gateways that inspect all Internet traffic bi-directionally for malware, and enforce security and compliance policies.

The Zscaler API provides the two closest data center locations to each branch, allowing SD-WAN to steer traffic effectively. Organizations can allow Zscaler to automatically pick the closest ZEN to the branch by having ZEN look at IP addresses of WAN links configured on Citrix SD-WAN or can manually select the **ZENs**.

NOTE

Both the routes always be in active mode if the tunnel is UP. If any tunnel goes down the corresponding route becomes unreachable and the other route stay UP in that case.



Benefits

The benefits of integrating Citrix SD-WAN and Zscaler include:

- Faster adoption of SaaS and cloud in a distributed enterprise.
 - Centralizing security as a cloud service eliminates the need to have it in each branch.
 - Eliminating the need to backhaul internet-destined traffic allowing local Internet breakout at the branch.

- Simplified IT management with automated connectivity to a Secure Web Gateway.
 - API support automates configuration of secure tunnels to Zscaler
- Improved user experience by reducing latency from backhauling SaaS traffic.
 - Eliminates hub-and-spoke model dependency for security purposes
- Elimination of costly security stacks at branches
 - Reduce the overhead of having to deploy and manage firewalls at the branches.
- Assurance that internet-bound traffic is always secure.
 - Security policies do not tie users to a physical location.
 - Provides sandboxing, inspection of all ports and protocols, including SSL, URL filtering, advanced threat protection, and more to protect against zero-day attacks.

Supported functionality

A Zscaler deployment using SD-WAN appliances supports the following functionality:

- Forwarding user-defined Internet traffic to Zscaler, thereby enabling direct Internet breakout.
- Direct internet access (DIA) using Zscaler on a per customer site basis.
 - On some sites, you might want to provide DIA with on-premises security equipment and not use Zscaler.
 - On some sites, you might choose to backhaul the traffic another customer site for internet access.
- Virtual routing and forwarding deployments.
- One WAN link as part of internet services.

Zscaler is a cloud service. You must set it up as a service and define the underlying WAN links:

- Configure a trusted Public internet wan link at the data center and the branch sites.
- Auto configure IPsec Tunnels for intranet services.

Deploying Zscaler in Citrix SD-WAN Center workflow

The following are the high-level steps that define the workflow to deploy Zscaler in SD-WAN Center.

- 1. Configure Zscaler subscription to SD-WAN Center (onetime). Log into the Zscaler site to obtain subscription information.
- 2. Select **Deploy** in Citrix SD-WAN Center GUI.

- Deploy configuration for site using internet wan-link and preconfigured application object.
- Establish Connectivity.
- Get/Update of IPsec status.

Zscaler subscription

Before you proceed with configuring Zscaler in SD-WAN Center, you need to log into the Zscaler portal.

1. Log into the Zscaler site to obtain subscription information. The Dashboard page opens.

Web Overview		24 Hours ~			№ С
CLOUD APPLICATION CLASSES	Bytes TC	DP URL CATEGORIES	Transactions	TOP USERS	Transactions
No data for selected t	ime range	No data for selected	time range	No data for selected time range	
SOCIAL NETWORKING APPLICATIONS	Transactions ST	REAMING MEDIA APPLICATIONS	Bytes	TOP ADVANCED THREATS	Transactio
No data for selected t	ime range	No data for selected	time range	No data for selected time range	

2. Click Administration > Partner Integrations.

 Settings 			24 Hours 🗸			o 🔥 C
ACCOUNT MANAGEMENT My Profile Company Profile Akrts Print All Policios	CLOUD CONFIGURATION Advanced Bettings Plantner Integrations NUW	Dytes	TOP URL CATEGORIES	Transactions	TOP USERS	Transactions
Authentication Authentication Counsultation Authentication Settings User Management	Achieves this tool occurring a second		No data for selected time range		No data for selected time range	
Control Contro	ACCESS CONTROL URL Categories Bandwitch Classos Time Induser Notifications	Transactions	STREAMING MEDIA APPLICATIONS	Bytes	TOP ADVANCED THREATS	Transactions
DATA LOSS PREVENTION DLP Dictionarios & Engines DLP Notification Templates	Standard for principal lines of ege		No data for selected time range		No data for selected time range	

3. Select **SD-WAN** on the **Partner Integrations** page. Click **Add Partner Key**.

← →	e c	https://admin.zscalerbeta.net/#admini	istration/partner-integration			ର୍ 🕁 ତ	Θ:
\$	Partner	Integrations					
Deshtroard	MICROSO	OFT CLOUD APP SECURITY SD-WAN					
جما	O Add F	Partner Key					
Analytics	No.	Partner Name	Көу	Last Modified By	Last Modified On		E
Poley	1	Riverbed SteelConnect	wpxgZq0LSHyh	System	November 20, 2018 08:34 PM	/ c	* ^
Policy	2	Cisco Viptela	3b6D0sLbre0R RAdM9V[ZURC2	System	November 20, 2018 08:34 PM November 20, 2018 08:34 PM	/ c	×
CC Accession	3	Silver Peak HPE Aruba	RAdM9VjZURC2 R5B82L0mtRxR	System	November 20, 2018 08:34 PM November 20, 2018 08:34 PM	/ 0	×
	Ľ.,						• •
(1) Activation							
Q Bearch							
0							R
•)							
Copyright00	2007-2018 Zscaler I	Inc. All rights reserved. Version 5.6 Potents			Weblog Time: 11/21/0018 1	19062 PM - Last Updated: 11/2	21/2018 1:00:00 PM
r		Partner Key			Vesting Time: 11/21/5018 4	10000 PM - Lond Updater 110	25.2018 1:00:03 PM
Ľ	Add F				Webling Towe 11/21/6/08 1		25.2018 1:00:03 PM
		NER		Name	Webing Tone 11/01/0018		25.2018 1:00:03 PM
	PARTN Type	NER e			Webking Towe 11/07/06/8	×	25.2018 1:00:03 PM
r	PARTN Type	NER		Name NONE	Velog Toe 11/31/0018		25.2018 1:00:03 PM
r	PARTN Type	NER e			Velog Toe 11/31/001	×	21/2018 1:00:00 PM
	PARTN Type	NER e			Velog Tore 11/31/0014	×	
	PARTN Type	NER e		NONE	Velog Tore 11/31/001	×	25.2018 1:00:03 PM
	PARTI Type SD-\	NER e WAN		NONE		×	
	PARTI Type SD-\	NER e		NONE Search VMware Vel	loCloud	×	
	PARTI Type SD-\	NER e WAN		NONE	loCloud	×	
	PARTI Type SD-\	NER e WAN		NONE Search VMware Vel Cisco Viptel	loCloud	×	
	PARTI Type SD-\	NER e WAN		NONE Search VMware Vel Cisco Viptel Silver Peak	loCloud	×	
	PARTI Type SD-\	NER e WAN		NONE Search VMware Vel Cisco Viptel	loCloud	×	
	PARTI Type SD-\	NER e WAN		NONE Search VMware Vel Cisco Viptel Silver Peak	loCloud	×	

4. Choose **Citrix SDWAN** for the partner key and click **Generate**. Store the key.

Configure Zscaler in Citrix SD-WAN Center

- In the Citrix SD-WAN Center GUI, navigate to the Configuration > Security page. The Zscaler Configured Sites page opens.
- Click Subscription. Enter the Zscaler API (partner key) which created in the preceding steps. Provide your Zscaler Username and Password. Select the Zscaler Cloud Name, Zscaler Log Level, and click Apply.

Subscription for Zscale API Key:		
WzFb7qcelvCW		
Username:		
abc@zscaler.com		
Password:		
XXXXXXXX		
Zscaler Cloud Name:		
zscalerthree.net		
Zscaler Log Level:		
Debug	•	
	Apply	Cancel

3. Zens provides the list of available VPN endpoints for this Zscaler cloud subscription.

C Zscaler Enforce	ment Node(ZE	N) VIPs					
Show 10 🔻 en	tries Search	h:					
Location 🔺	. Ge	eo Region	VPN Host	Name	VP	N End Point IP	
No data available	in table						
Showing 0 to 0 of (0 entries					Close	ousNext
Add Show 10 + ent	Zscaler Enforcer	-	-		×	ZENS Su	bscription
	Location 🔺	Geo Region	VPN Host Name	VPN End Point I	P		
Site Name	Frankfurt IV	Europe	fra4-vpn.zscalerbeta.net	165.225.72.39	_	Deployment Status	Details
Sanjose	San Francisco IV	US & Canada	sunnyvale1-vpn.zscalerbeta.ne	et 199.168.148.132	ta.net 🔻	Tunnels Deployed	÷
Showing 1 to 1 of 1 Re-deploy De	Washington DC Showing 1 to 3 of 3	US & Canada entries	was1-vpn.zscalerbeta.net	104.129.194.39 Previous 1 Close	Next	Previous	1 Next

4. After entering the Zscaler subscription and ZEN details, you can start adding sites to Zscaler. Click **Add**.

			g Configuration	Reporting					
Network Discovery		Configuration /							
Network Configuration Zero Touch Deployment			gured Sites	dd separate disk to store stat	stics from SD-WAN when p	olling SD-WANS. Click here to na	wgate to Administration->stora	ge Maintenance.	1
Change Management	Ad	śd						ZENs	Subscription (
Appliance Settings	s	show 10 V er	ntries Search:						
Mobile Broadband						Z	N		
			Site Name 🔺	WAN Link	Application Objects	Primary	Secondary	Deployment Status	Details
Licensing									
		0	Branch	Branch-WL-1	zscalerappobject *	sjc4-vpn.zscalerthree.net *	sea1-vpn.zscalerthree.net *	Connection Active	0
Licensing Cloud Connectivity Security			DC	Branch-WL-1 DC-WL-1	zscalerappobject *	sjc4-vpn.zscalerthree.net *	sea1-vpn.zscalerthree.net *	Connection Active	0

5. In the **Configure Sites to Zscaler** dialog box, add **Site, WAN Link,** and **Application Objects**. By default, the **Auto assign ZEN** option is selected.

dd Multiple					Auto assign ZEN	
					Auto assign ZEN Manually Select 2	
Site		WAN Link		Application Object	ts	Action
Select Site	*	Select WAN Link	-*	Select Application Objects	*	Đ

You can **Manually Select ZEN**. However, the following message appears notifying that unsaved changes are lost.

Note: Deploying sites will initiat	e Change Manageme	ent			Manually Select	▼ ✓
Site		WAN Link		Application Objects		Action
Select Site	*	Select WAN Link	*	Select Application Objects	-*	
owing 1 to 1 of 1 entries						
					Dep	loy Cance

 Select required sites and click **Deploy**. You can choose to add multiple sites by selecting **Add Multiple**. The selected sites are deployed and the configuration page is displayed.

Note: Depi	loying sites will initiat	e enange managem					
Add Multiple						Manua	ally Select 🔻 🗸
	Site		WAT	N Link	Ар	plication Objects	Action
DC		~	DC-WL-1	•	zscalerappobject		• İİ
Branch		•	Branch-WL-1	*	zscalerappobject	1	· 🗓
onfiguration /	Security	-					Deploy Cano Deploy
	security gured Sites						
aler Config	-						
aler Config	gured Sites						Deploy
aler Config	gured Sites			Z	EN		Deploy
aler Config	gured Sites	WAN Link	Application Objects	Primary	EN Secondary	Deployment Status	Deploy
ow 10 v ent	gured Sites	WAN Link Branch-WL-1	Application Objects zscalerappobject *			Deployment Status Connection Active	Deploy

Observe that the primary and secondary ZEN IP addresses are populated and the deployment status is **Connection Active**.

7. Click **Re-Deploy**, if you make changes to the configured site's VPN endpoints or application objects. Any changes to the configured sites in the SD-WAN Center trigger a **Change Management** process on the appliances configured at the branch sites and DC sites.

	×						
te Change	Configuratio	n Reporting	Administration	Nitro API			
•	ecurity						
A For region:De	fault_Region SD-WAN Cente	r, add separate disk to store st	tatistics from SD-WAN when po	lling SD-WANs. Click here to na	avigate to Administration->Stora	ge Maintenance.	×
Zscaler Confi	gured Sites						
Add						ZENs	Subscription
Show 10 T	ntries Search:						
					EN		
	Site Name 🔺	WAN Link	Application Objects	Primary	Secondary	Deployment Status	Details
8	Branch	Branch-WL-1	zscalerappobject1 *	sjc4-vpn.zscalerthree.net *	sea1-vpn.zscalerthree.net *	Connection Active	0
	DC	DC-WL-1	zscalerappobject1 *	sjc4-vpn.zscalerthree.net *	sea1-vpn.zscalerthree.net *	Connection Active	0
_						Pro	vious 1 Next
	Change For region.Dec Zscaler Confi Add Show 10 * e Showing 1 to 2 of	Configuratio currly for region/Default, Region SD WAN Center Cscaler Configured Sites Add Show 10 entries Search Branch Dc Showing 1 to 2 of 2 entries	Configuration Reporting curity Configuration Reporting curity Configuration Reporting curity Configured Sites Add Store entries Search Site Name A WAN Link Configured Sites C	Configuration Reporting Administration Configuration Reporting Administration Configuration Reporting Administration Configuration Report of the second sec	Configuration Reporting Administration Nitro API curity Configuration Reporting Administration Nitro API curity Configuration SD WAN Center, add separate disk to store statistics from SD WAN when polling 5D WAAs. Click here to n Zscaler Configured Sites Add Show 10 entries Sarch Site Name WAN Link Application Objects Primary Branch Branch Branch WAN Link Application Objects Primary Branch Branch Branch COC.WL-1 StateRappoDject1 Site Application Primary Showing 1 to 2 of 2 entries	Configuration Reporting Administration Nitro API Configuration Reporting Administration Nitro API curity Cardingured Sites Example Cardingured Sites Example Site Name A WAN Link Application Objects Primary Secondary Site Name A WAN Link Application Objects Primary Site Name A WAN Link Application Objects Site Name A WAN Lin	RLD _2_0_404_715626 Configuration Reporting Administration Nitro APi Image: Configuration Image: Co

Deleting sites also triggers the change management process.

Delete Sites		×						
Deleting sites will initiate Do you want to continue	e Change Management. 67	Configuratio	on Reporting					
Yes (No	ecurity						
etwork Configuration	For region:De	efault_Region SD-WAN Cente	er, add separate disk to store s	statistics from SD-WAN when p	olling SD-WANs. Click here to na	wigate to Administration->Store	ige Maintenance.	
ro Touch Deployment	Zscaler Conf	igured Sites						
		0						
lange Management	Add						ZENs	Subscription
nange Management opliance Settings	Add Show 10 *	entries Search:					ZEN:	Subscription
		entries Search				EN	ZENs	Subscription
obile Broadband		entries Search	WAN Link	Application Objects	Z. Primary	EN	ZENs Deployment Status	Subscription
pliance Settings obile Broadband ensing	Show 10 V		WAN Link Branch-WL-1	Application Objects zscalerappobject1 *			Deployment Status	
pliance Settings oblie Broadband ensing oud Connectivity	Show 10 T	Site Name 🔺			Primary	Secondary	Deployment Status Connection Active	Details
pliance Settings	Show 10 V	Site Name 🖍 Branch DC	Branch-WL-1	zscalerappobject1 *	Primary sjc4-vpn.zscalerthree.net *	Secondary sea1-vpn.zscalerthree.net *	Deployment Status Connection Active Connection Active	Details

Monitoring and troubleshooting

Select configured sites to view more information about Application Objects and Primary/Secondary IP addresses. You can click the **Details** icon to view complete information about the configured sites.

Dashboard			Configuration						
		Zscaler Site D	etails						
		Application Object	:t						
	Zso	Application Object	Name: zscalerappobject						
	t Ad	Match Criteria							
Change Management	S		Match Type		Application		Application Family	Protocol	
Appliance Settings			application		Salesforce(salesforc	2)			
Mobile Broadband		IPsec Tunnels							
Licensing		iPsec lunnels							
Cloud Connectivity		Local IP:	2	scaler_service_1331170 Peer IP:	17_1	_	zscale Local IP:	_service_13311707_2 Peer IP:	
Security	SI	192.168.100	2	104.129.2			192.168.100.2	165.225.50.22	
		MTU: 1500		Firewall 2	lone:		MTU: 1500	Firewall Zone:	
		IKE Version: ikev2		DH Group group2	:		IKE Version: ikev2	DH Group: group2	
		IKE Hash Al sha256	gorithm:	IKE Integ sha256	rity:		IKE Hash Algorithm: sha256	IKE Integrity: sha256	
		IKE Encrypt aes256	ion:	IKE Ident user_fqdr			IKE Encryption: aes256	IKE Identity: user_fqdn	
		Identity Dat branch1331	ta: 1707@citrix.com	IPsec Tun esp_null	nel Type:		Identity Data: branch13311707@citrix.com	IPsec Tunnel Type: esp_null	
		PFS Group: none		IPsec Has md5	h Algorithm:		PFS Group: none	IPsec Hash Algorithm: md5	
		IPsec Mismo drop	atch Behaviour:				IPsec Mismatch Behaviour: drop		

You can view and download the Zscaler logs that can be used to troubleshoot issues in the Citrix SD-WAN Center.

To view Zscaler log files:

1. In the Citrix SD-WAN Center web interface, click the **Monitoring** tab > **Diagnostics**.

Citrix SD-	WAN	Center				R11_2_1_47_864113 ~	admin
		Monitoring			Administration		
Network Map		Monitoring / Diagnostic	55				
Statistics Diagnostics System Information	Lo	og Files og File: SDWANCENTER_access.I	og v View	Download			0
	D	iagnostic Packages					0
		server) by clicking on Uplo			ard to Citrix Support Represen	ntatives. They may be downloaded directly through the browser or uploaded to Citrix	(or another
		Create Package Include Workspaces For : admin Package Name:	✓ Create	Diagn	age Packages ostic Package: VANCENTER_2020-5-15-14-14	4-26-diagnost v	

- 2. From the Log File drop-down list, select the Zscaler log file you want to view. Click View.
- 3. If you want to download the log files to your computer, click **Download**.

IPsec tunnel configuration

The Details page in SD-WAN Center GUI provides information about the IPsec tunnel configuration to Primary and Secondary endpoints. The Peer IP is obtained from Zscaler. Verify IPsec tunnel configuration in the SD-WAN appliance GUI configuration editor.

	Service Type	Intranet Service Type	Name	Firewall Zone		Local IP		Peer IP	MTU	Keepalive	Delet
+	Intranet \$	ZScaler	zscaler_service_44472088_1	\$ <default> \$</default>	1	0.9.2.4	¢	199.168.148.132	1500		Ū
÷	Intranet \$	ZScaler	zscaler_service_44472088_2	\$ <default> \$</default>	1	0.9.2.4	¢	104.129.194.39	1500	•	Ū

IKE settings

The following IKE/IPSec settings are chosen for IPsec tunnel configuration in the SD-WAN appliance. For more information about configuring IPsec tunnel –IKE settings, see; How to configure IPsec tunnel between SD-WAN and third-party devices topic.

- IKE version IKEv2
- IKE Identity –User FQDN
- Hash Algorithm SHA-256
- Integrity Algorithm SHA-256
- Encryption Mode AES 256 Bits

- IPsec Tunnel Mode
- IPsec Encryption Null

Service Type	Intranet Service Type	Name		Firewall Zone	Local IP	•	Peer IP	MTU	Keepaliv
Intranet \$	ZScaler	zscaler_service_44472088_	1 \$	<default> +</default>	10.9.2.4	¢	199.168.148.132	1500	
									?
IKE Set	-								f
IKE	v2 \$								
Ident		Identity Data:	1	Authentication:	Pro	e-Sl	hared Key: 💿		
Use	r FQDN \$	sanjose4447208		Pre-Shared Key 💲					
Peer	Authentication:								
Mirr	ored \$			Validate Peer Identity	/				
DH G	roup:	Hash Algorith	m:	Integrity Al	gorithm:		Encryption	Mode:	
Gro	up 2 (MODP1024)	\$ SHA-256	¢	SHA-256	\$		AES 256-	Bit ‡	
Lifeti	me (s):	Lifetime (s) Ma	x:		DPD) Tir	meout (s):		
3600	D	86400			300	D			
IPsec S	Settings								?
			_			_			

IPsec settings

For more information about configuring IPsec tunnel settings, see How to configure IPsec tunnel between SD-WAN and third-party devices topic.

	Service Type	Intranet Service Type	Name	Firewall Zone	Local IP	Peer IP	MTU	Keepalive	Del
Ξ	Intranet \$	ZScaler \$	zscaler_service_44472088_1 \$	<default> +</default>	10.9.2.4 ‡	199.168.148.132	1500		ť
								_	
	IKE Se	ttings						?	
	IPsec S	Settings						?	
	Tunn	iel Type:	PFS Grou	ib:					
	ESF	P+NULL \$	<none:< td=""><td>*</td><td></td><td></td><td></td><td></td><td></td></none:<>	*					
	Hash	Algorithm:							
	MD	-							
	THE .	.							
	Lifeti	me (s):		Lifetime (s) Max:					
	288	86		86400					
	Lifeti	me (KB):		Lifetime (KB) Max:					
	0			0					
	Netw	ork Mismatch Behavior:							
	Dro								

Application objects

Ensure that application objects are configured. For more information about configuring application routes, see Application classification topic.

					Search			
Order	Application Object	Cost	Service Type	Service Name	Gateway IP Address	Info	Edit	Delete
1	zscalerobject	4	Intranet	zscaler_service_44472088_1		0	0	Ū
3	zscalerobject	4	Intranet	zscaler_service_44472088_2		0	1	۵
					144	<	1	> >>

Note

The GRE tunnel configuration is not supported as part of the automated workflow. However, the manual configuration is still allowed. For more information, see Zscaler Integration by using GRE tunnels and IPsec tunnels.

Monitoring

March 12, 2021

The Citrix SD-WAN Center Dashboard allows you to view the SD-WAN network statistics and graphs on a single pane. For more information, see Dashboard.

You can also view the SD-WAN network Events and Reports in Citrix SD-WAN Center.

Monitoring related articles:

Diagnostic Packages Event Notifications

Log Files

Memory Dumps

Polling Interval

Statistics

System Information

Dashboard

April 22, 2021

The Citrix SD-WAN Center Dashboard displays a subset of the common statistics at a glance. For a single-region deployment, the statistics are obtained from the MCN that is discovered in Citrix SD-WAN Center. For a multi-region deployment, the statistics are obtained from all the regional Citrix SD-WAN Center collectors for the selected time interval. You can view the following statistics:

- Network Summary
- Network QoE
- Top Sites
- Inventory
- Events and Alarms
- Top Apps
- HDX QoE
- Management Infra

For a single-region deployment, the default region statistics are displayed on the dashboard. For a multi-region deployment, you can choose to view the multi-region dashboard or the regional dashboard. To view the multi-region dashboard, in the **Region** menu select **All**. However, you cannot view the multi-region summary dashboard when more than 300 sites are configured.

Dashboard				Reporting					
< Default Dashboard	~	Dashboard / Default	Dashboard / Network					_	Region: All
Network Apps	> >	Network Summary							region1 region2 Default_Region
Management Infra Custom Dashboard	>	Time: September 20, 20	18 10:40am 🔳 Last: Hour /	Day / Week / Mo	onth			Mode: Relative (33 seconds	Schematic View
		22. Aug 24. Aug	26. Aug 28. Aug	30. Aug 1.	Sep 3. Sep	5. Sep 7. Sep	9. Sep 11. Sep		ep 19. Sep Interval: 1 minute V
		Routing Domain: Any		iguration: Config_	_				
		Atleast one Virtua		Il Virtual Paths UP, t ongestion or memb		All Virtual Pati links UP	hs and associated member	Polling in progress	
			2		2		0 Fair	0	
			Total Sites		Poor		Fair	Good	

You can view the MCN Connection status on each region tile. The MCN Connection status is the health status of the virtual path between an RCN and the MCN.

Note

For a multi-region deployment, the default region statistics include statistics of all the sites managed by the MCN. It might also include RCN statistics since the RCNs have virtual paths to the MCN.

The **Region** drop-down menu is not available in Citrix SD-WAN Center Collectors.

Dashboard	Fault	Monitor	ing Co	nfiguration	Reportin	g Admi	nistration	Nitro API			
Default Dashboard Network	~	Dashboard /	Default Dashboa	d / Network	/ Network Summa	У				Region: All	Region:
Network Summ		Current Netwo	rk Health: Mul	i-Region Sum	mary						
Network QoE											Network view
Site QoE		Atleast one Vir	rtual Path DOWN	A	ill Virtual Paths UP, t	out at least one co	ngested	All Virtual	Paths UP and healthy	Fet to be discovered	
Top Sites Inventory Events & Alarms		Default_Regi	ion			APAC SITES		MCN	Connection: GOOD		
Apps Management Infra Custom Dashboard	>	7 Total	2 Poor	1 • Fair	4 Good	4 Total	0 Poor	0 ● Fair	4 © Good		
00101100010		EMEA	Failed to re		Connection: DEAD	ANZ SITES		MCN	Connection: GOOD		
		- Total	- Poor	- Fair	- Good	4 Total	0 Poor	0 • Fair	4 Good		

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

Network summary

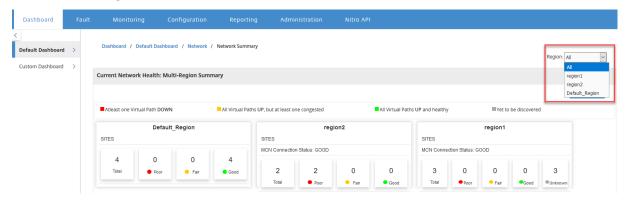
For a multi-region deployment, the **Network Summary** widget provides an overview of the network health at all the various regions. A region card for every region in the network is displayed with the following information:

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

To view multi-region network summary, navigate to **Dashboard > Default Dashboard > Network > Network Summary** and in the **Region** drop-down menu, select **All**.

Dashboard								
Contract Contract	~	Dashboard / Default D	ashboard / Network /	Network Summary				
Network	~							Region: All
Network Summ	nary	Current Network Healt	h: Multi-Region Summa	ary				
Network QoE								Regionwise view
Top Sites								
Inventory					Network (Across r	egions)		
Events & Alarms	5	Atleast one \	rintual Path DOWN	All Virtual Paths UP, but	at least one congested	All Virtual Paths UP and healthy	Yet to be discovered	
Apps	>							
Management Infra	3		-	4	0		0	
Custom Dashboard	>		(1	0	4	2	
		Tota	Sites	Poor	E Fair	Good	Unknown	

By default the screen appears in **Network view**. You can see the current network health of the multiregion network summary by clicking the **Region wise view**. You can also see the MCN Connection status on each region tile.



Click a region card to drill down into the regional dashboard.

For an individual region, the **Network Summary** widget provides an overview of the network health of the selected region.

To view regional network summary, navigate to **Dashboard** > **Default Dashboard** > **Network** > **Network Summary** and in the **Region** drop-down menu, select **a region**.

You can view the regional network summary in either the tile view or the schematic view.

You can use the timeline control to view the network status summary for a selected period. You can also play or pause the network status over a time range.

Mode helps to see the time as a relative or an absolute concept.

For more information on Timeline and mode see Timeline controls.

Tile view

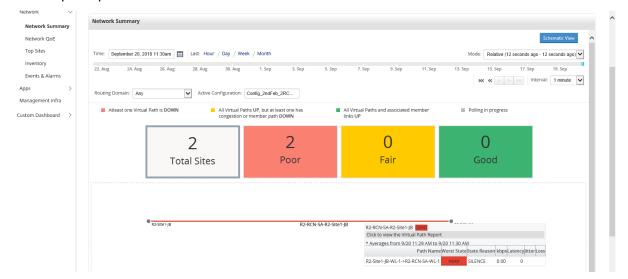
The tile view provides the following information:

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

To view a graphical representation of a path between two sites, select the path and click **Visualize**.

Dashboard Fau								
afault Dashboard V	Dashboard / Default Da	ishboard / Network / I	Vetwork Summary					Region: Default_Region 🗸
Network Summary	Network Summary							
Network QoE								Schematic View
Top Sites	Time: September 20, 2018	11:17am 🗮 Last: Ho	ur / Day / Week / M	Month			Mode: Relative (16 seconds	ago - 16 seconds ago) 🗸
Inventory Events & Alarms	22. Aug 24. Aug	26. Aug 28. Aug	30. Aug	1. Sep 3. Sep	5. Sep 7. Sep	9. Sep 11. Sep	13. Sep 15. Sep 17. S	ep 19. Sep Interval: 1 minute
ps >	Routing Domain: Any	✓ Active	Configuration: Config	g_2ndFeb_2RC				
stom Dashboard >	Atleast one Virtual P.	ath is DOWN	All Virtual Paths UP congestion or mem		 All Virtual Pa links UP 	ths and associated member	Polling in progress	_
		2		2		0	0	
		Total Site	s	Poor		Fair	Good	
			Please click on the \	/isualize Button in the ta	ble below to get the Virti	ual Path details between the sele	cted Sites.	
	Show 10 v entries		Searc	h				^
	D3 Site1 ID	Origin Site		D2 DCN SA	Connecter	d Sites		
	R2-Site1-JB			R2-RCN-SA			✓ Visualize	

Hover the mouse cursor over the sites or the path to view more details. Click the sites to view and select report options.



Schematic view

The schematic view provides a graphical view of the SD-WAN network. The information displayed in this section is updated depending on the selected configuration and routing domain. To view a network map here, you must import the network configuration and Network maps from the Master Controller Node (MCN). For more information, see Import MCN configuration.

Hover the mouse cursor over the sites or the path to view more details. Click the sites to view report options.

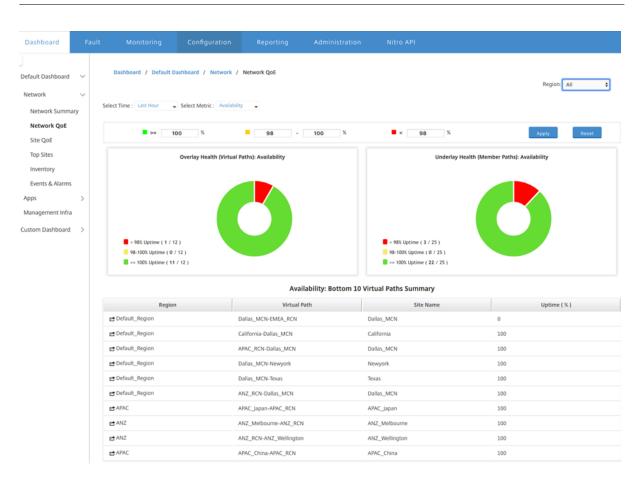
Dashboard			
Default Dashboard Network	~	Dashboard / Default Dashboard / Network / Network Summary Region: Default_Region	
Network Summa	ry	Network Summary	
Network QoE		The Vi	w
Top Sites		Time: September 20, 2018 11:44am 🛅 Last: Hour / Day / Week / Month Mode: Relative (8 accords ago)	\checkmark
Inventory		22. Aug 24. Aug 26. Aug 28. Aug 28. Aug 30. Aug 1. Sep 3. Sep 5. Sep 7. Sep 9. Sep 11. Sep 13. Sep 15. Sep 17. Sep 19. Sep	
Events & Alarms		lec ex box the the termination of termination of t	×
Apps Management Infra	>	Routing Domain: Any Configuration: C	
Custom Dashboard	>	Sto Filter	• /
		R2-RCN-SA-1 R2-RCN-SA-R2-Site 1-JB DEAD	
		Click to view the Virtual Path Report * Averages from 9/20 11:36 AM to 9/20 11:37 AM	
		* Averages from 9/20 11:36 AM to 9/20 11:37 AM Path NameWorst StateState Reason kbpsLatencyJitterLoss	>
		R2-Site1-J8-WL-1->R2-RCN-SA-WL-1 DEAD SILENCE 0.00 0	

Network QoE

The **Network QoE** widget provides a graphical representation of the availability, loss, latency, and jitter parameters of a virtual path. It provides the statistics for both overlay virtual path and the underlay member paths.

For a multi-region deployment, you can view a list of the bottom 10 virtual paths depending on the selected metric. The virtual path data is collected from all the regional collectors for the selected time interval. You can view the bandwidth, jitter, loss, and congestion details of the virtual paths that need your attention the most.

To view multi-region virtual path health, navigate to **Dashboard** > **Default Dashboard** > **Network** > **Network QoE** and in the **Region** drop-down menu select **All.**



For an individual region, you can view a list of the bottom 10 virtual paths depending on the selected metric. The statistics are collected for the selected time interval. You can view the bandwidth, jitter, loss, and congestion details of the virtual paths that need your attention the most.

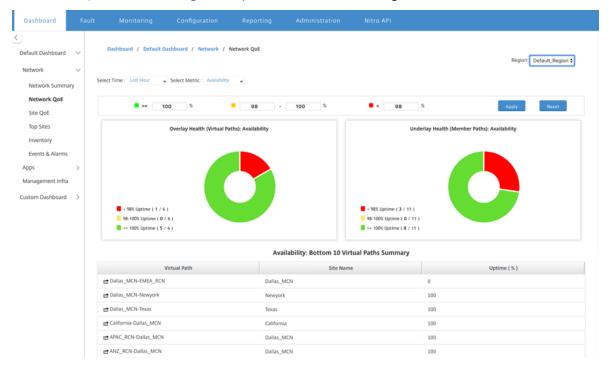
You can compare the overlay and underlay paths for the selected metric (availability, loss, jitter, latency) over the selected time interval. You can also set custom thresholds for the metrics and save them on click **Apply**. Click **Reset** to store the default thresholds.

The user can also drill down to any virtual path in the table by using on the **drill down** button on the left of each row. A **Site QoE** appears with the detailed comparison between the conduit and its underlying member paths.

Network 🗸	S	ite QoE									×
Network Summary	Select Time : Last Hour Select	t Time : Last Hou	Select Site :	APAC_RCN	 Select Virtua 	I Path : APAC_RC	N-Dallas_MCN	Select Metric : Avail	ability 🖕		Plot
Network QoE											
Site QoE			WA	AN TO LAN				LA	N TO WAN		
Top Sites		State \$ Vi	irtual Path: APAC_	_RCN-Dallas_MC	CN		State \$	Virtual Path: APAC	_RCN-Dallas_M	CN	
Inventory		GOOD					GOOD				
Events & Alarms		DEAD					DEAD				
Apps >		UNKNOWN	12:45pm	1:00pm	1:15pm	1:30pm	UNKNOWN	12:45pm	1:00pm	1:15pm	1:30pm
Management Infra											
Custom Dashboard >		State \$ Pa	ath: Dallas_MCN-o	queue1->APAC_	RCN-queue1		State \$	Path: APAC_RCN-q	ueue1->Dallas	MCN-queue1	
	98% Uptime (0	GOOD BAD					GOOD BAD				
	98-100% Uptime (DEAD DISABLED UNKNOWN					DEAD DISABLED UNKNOWN				
			12:45pm	1:00pm	1:15pm	1:30pm		12:45pm	1:00pm	1:15pm	1:30pm

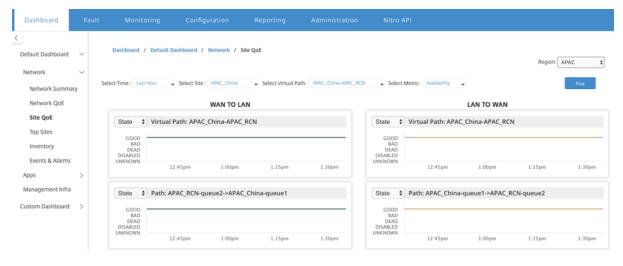
In the slider, the site name and virtual path are selected by default depending on the row that you clicked and it will be disabled. However the user can select a different time range and metric and click **Plot** option to plot the new graphs.

To view regional virtual path health statistics, navigate to **Dashboard > Default Dashboard > Network > Network QoE** and in the **Region** drop-down menu select a region.



Site QoE

You can use Site QoE as a tool to compare the virtual path and it's underlying member paths. You need to select a site and any virtual path from this site and metric. Click **Plot**.



In the first section, it plots the virtual paths statistics in both **WAN to LAN** and **LAN to WAN** direction. Below section plots all the underlying member paths graphs. Both these things are present at both region and network level.

Top sites

For a multi-region deployment, the **Top Sites** widget lists the top 10 sites across all the regions, which have the highest bandwidth usage, in the selected time interval.

To view the top sites across all regions, navigate to **Dashboard** > **Default Dashboard** > **Network** > **Top Sites** and in the **Region** drop-down menu select **All.**

Dashboard	Fau									
Default Dashboard	H ~	Dashboard / Default D	ashboard / Network / 1	Top Sites					Region: All	~
Network	~	Top sites in Network								
Network Summ	nary									
Network QoE							Select Time:			~
Top Sites							_	Last 1 Hour		
Inventory								Last 24 Hours Last Week		
Events & Alarms	15							Last Week		
Apps	>									
Management Infra	ra									
Management Infra Custom Dashboard										
					MCN-NY (41.62%) 📕 R1-1 R2-RCN-SA (14.57%) 📕 D					
		Bandwidth Usage: Top :	10 Sites Summary							
		Bandwidth Usage: Top : Show Bandwidth/Data in [Select Time: Last 1 Hou	11 🗸
									Select Time: Last 1 Hour	
		Show Bandwidth/Data in								14
		Show Bandwidth/Data in			R2-RCN-SA (14.57%) ■ D	ref-Site1-SC (13.54%)	Total Available Bandwidth	Total Pe		
		Show Bandwidth/Data in Filters: +	Kbps/KB	•,	LAN to WAN Bandwidth	ef-Site1-SC (13.54%) WAN to LAN	Total Available Bandwidth 99,000.00			1÷
		Show Bandwidth/Data in Filters: + Region	Kbps/KB v	∎ r Total Bandwidth ↓	LAN to WAN Bandwidth 3 40.30 (2)	WAN to LANBandwidth		• 🖻	rmitted Bandwidth	1 ċ ♥
		Show Bandwidth/Data in [Filters: + Region Pefault_Region	Kbps/KB V Name MCN-NY	Total Bandwidth ↓ 95.50 E	LAN to WAN Bandwidth 3 40.30 2 33.38 2	WAN to LAN Bandwidth 55.20 🔁	99,000.00	0 2	mitted Bandwidth 98,997.40 E	

Click a site or metric to view detailed reports and statistics.

For an individual region, the Top Sites widget displays the bandwidth usage statistics for all the sites in the region. The statistics are collected for the selected time interval. You can filter the sites based on the routing domain.

_								
Dashboard								
Default Dashboard	~	Dashboard / D	efault Dashboard / Network / Top Si	ites			Region: De	fault_Region V
Network Network Summa	~	Top sites						
Network QoE							Select Time: Last 1 Hour	٢
Top Sites								
Events & Alarms								
Apps Management Infra	>							
Custom Dashboard								
					EN-NY (41.61%) 📕 R1-RCN-MU			
				R2	-RCN-SA (14.41%) 📕 Def-Site1-	GC (13.72%)		
		Bandwidth Usag	e: Top 10 Sites Summary					
		Routing Domain:	Any Y Show Band	dwidth/Data in Kbps/KB 🗸			Select Time: L	ast 1 Hour 🗸
		Filters: +	Showing 1 - 1 of 1		Search			ᆔᄚᆂ
		10 V page	showing 1 - 1 of 1		Search			
		Name	Total Bandwidth 🖂 🗸	LAN to WAN Bandwidth 🛃	WAN to LAN Bandwidth 🖂	Total Available Bandwidth 🖂	Total Permitted Bandwidth 🖃	0

Inventory

Every 30 minutes, the Inventory manager gathers the hardware information from all the Citrix SD-WAN appliances that are discovered on Citrix SD-WAN Center.

To view the multi-region inventory statistics, navigate to **Dashboard > Default Dashboard > Network** > **Inventory** and in the **Region** drop-down menu select.

To view inventory statistics of a specific region, in the **Region** drop-down menu select the region.

You can view the following inventory statistics:

- **Site**: Name of the site found in the configuration running in the MCN. If the appliance is a secondary MCN, "(secondary)"appears next to the name. You can click the name to access the appliance web console.
- **Connection Status**: Connectivity state to the appliance. A red icon appears when the connection is not reachable or not authenticated.
- **Management IP**: Management IP address of the appliance. You can click the IP address to access the appliance web console.
- **BIOS Version**: BIOS version of the appliance.
- **Model**: Hardware model of the appliance.
- Serial Number: Serial Number of the appliance.
- **Software**; SD-WAN software version number.
- **Days Since Memory Dump**: Time since last system-error memory dump. If the appliance dumped its memory in the past four days, an error icon appears next to the time. If the memory dump occurred between 5 and 10 days ago, a warning icon appears. N/A appears if no dump is available. Clicking the time opens the log page of the SD-WAN.

- Active OS: The OS currently running on the appliance.
- RAM Size (GB): Amount of RAM currently installed on the appliance in GB.
- **Drive Type**: Type of data-storage drive installed on the appliance. The value can be SSD (Solid State Drive) or HDD (Hard Disk Drive).
- Drive Size (GB): Size of the data-storage drive currently installed on the appliance in GB.

Dashboard																
Default Darhboard			Dashboard	/ Default Dashboa	ed / Network /	inventory								Regis	n All	~
Network	Ÿ	1.12	nventory ch	art												
Network Summa	нy	1.1	menony co	art.												
Network QoE																
Top Sites																
Inventory																
Events & Alarms																
Apps	>															
Management Infra																
Custom Dashboard	->															
								B +ges (100%)								
			nventory													
			ies View 0	pena Seve Se Any	ve As											0
			1865 + 18 ¥/p	nga Sho	uning t - 4 of 4				Seath						C 🗅	÷
			Ster A	Connection State	Management IP	8IO5 Version	Model	Serial Number		Software	Days Since Memory Dump	Active OS	RAM Size (GB)	Orive Type	Drive Size (G8)	0
		Ð	ef Stell SC	Stats in Sync	10.102.72.53	41.5	vpx	92235110-8506-5647-6910	239791642+49	#10,2,0,50,710125	N	L 4.5	i i	a nua	41	
			ION-NY	Stats in Sync	10.105.37.49	3.0#	2000		2110127125	R10,2,0,50,710125	N	i. 45		1 110	85	
			1-RCN-MUM		10.102.72.108	415		6c9315d4-81e0-63dF6134						4 N/A	41	
		*	2-RCN-SA	Stats in Sync	10.102.72.61	415	vpx	15490784-0106-0719-0544	(37291733o6a	R10,2,0,50,710125	N	4. 4.I		e nua	41	

Note

You can arrange the columns for the inventory statistics table by using the **Show/Hide Columns** option.

Inventory											
New View O		× As									0
Filters: +		ring 1 - 4 of 4			Search					2	Site Image: Connection State Management IP BIOS Version
Site	Connection State 🔨	Management IP	BIOS Version	Model	Serial Number	Software	Days Since Memory Dump		RAM Size (GB)	_	🕈 Model 🍡 🎽
Def-Site1-SC	Stats in Sync	10.102.72.53	4.1.5	vpx	9223fcc0-850b-5647-69c0-239f9b6a2e49	R10_2_0_50_710125	N/A	4.6	4		Seria Show/Hide Columns
MCN-NY	Stats in Sync	10.106.37.49	3.0a	2000	21VA127X2F	R10_2_0_50_710125	N/A	4.5	8	- 22	Software Days Since Memory Dui
R1-RCN-MUM	Stats in Sync	10.102.72.103	4.1.5	vpx	6c9315d4-81e0-63df-6134-f9039bd69e12	R10_2_0_50_710125	183	4.6	4		
R2-RCN-SA	Stats in Sync	10.102.72.61	4.1.5	vpx	15a9b78a-0166-6f19-b544-f37291733c6a	R10_2_0_50_710125	N/A	4.6	4	N	
											Apply

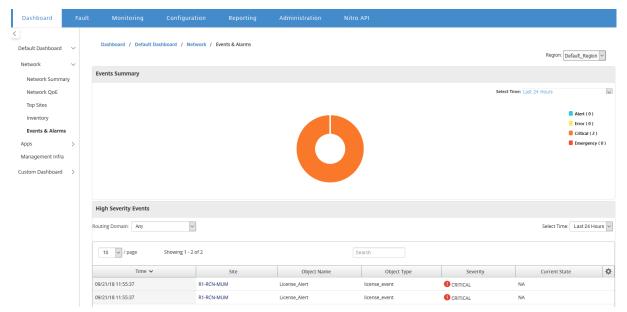
Events and alarms

For a multi-region deployment, you can view the events and alarms of all the regions in the network. This information is collected for the selected time interval. To view multi-region events and statistics, navigate to **Dashboard > Default Dashboard > Network > Events & Alarms** and in the **Region** dropdown menu select **All**.

You can also view all the events and alarms of an individual region. This information is collected for the selected time interval. To view events and alarm statistics, navigate to **Dashboard** > **Default Dashboard** > **Network** > **Events & Alarms** and in the **Region** drop-down menu select a region.

The **Event Summary** section gives a graphical overview of the event type and quantity of events. You can click the graph to view the events on the **Fault** page. The display also outlines how many events are in each category. Alarm triggers can be configured on the individual SD-WAN Appliances. For more information see, Event notifications.

The **High Severity Events** section displays a list of the severe events. You can filter the events based on the routing domain. The information displayed in this section is gathered from the **Fault** tab. For more information, see Events.



Apps

Top apps

Deep packet inspection (DPI) allows the SD-WAN appliance to parse the traffic passing through it and identify the application and application family types. For a multi-region deployment, you can view the top applications and top application families across all the regions in the network. This information is collected for the selected time interval.

To view top application statistics across all the regions in the network, navigate to **Dashboard** > **De-fault Dashboard** > **Apps** > **Top Apps**, and in the **Region** drop-down menu select **All**.

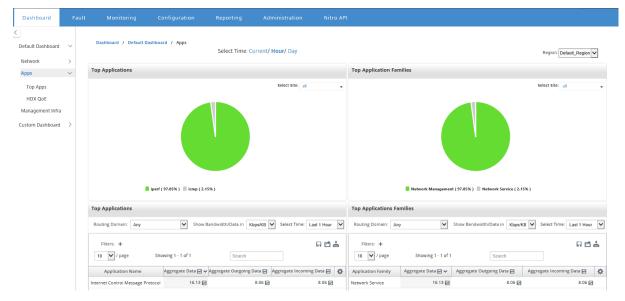
Dashboard											
C Default Dashboard Network	~	Dashboard / Default I	Dashboard / Apps	Select Time: Curr	rent / Hour/ Day					Region: All	
Apps	\sim	Top Applications					Top Application Far	nilies			
Top Apps HDX QoE Management Infra Custom Dashboard	>			D	select site: all all Def-site1-5 MCN-NY R1-RCN-ML R2-RCN-5A	ЛМ				all I I Def-SiteL-SC MCH-NY R1-BCN-MUM R2-RCN-SA	
			iperf (97.85%) 📗 icmp (2.1	5%)				Network Management	t (97.85%) 📗 Network Service (2.	15%)	
		Top Applications					Top Applications Fa	milies			
		Routing Domain: Any	Show B	andwidth/Data in Kbps	KB V Select Time: La	st 1 Hour 🗸	Routing Domain: An	y 🗸	Show Bandwidth/Data in Kbps/	KB Select Time: Last 1 Hour	~
		Filters: + 10 V page	Showing 1 - 1 of 1	Search		유변출	Filters: + 10 / page	Showing 1 - 1 of 1	Search	R 12 ÷	2
		Application Name	Aggregate Data 🕁 🗸	Aggregate Outgoing Dat	a 🛃 Aggregate Incoming	Data 🖸 🔅	Application Family	Aggregate Data 🛃 🗸	Aggregate Outgoing Data 🛃	Aggregate Incoming Data 🛃	¢
		Internet Control Message P	rotocol 137.09 🖻	68.	54 🖬	68.54 🛃	Network Service	137.09 🖬	68.54 🗠	68.54 🛃	

You can view the searchable drop-down list for site selection for both **Top Application** and **Top Application Families**.

You can also view the top applications and top application families of a particular region.

To view the application statistics of a region, navigate to **Dashboard** > **Default Dashboard** > **Apps** > **Top Apps** and in the **Region** drop-down menu select a region.

You can select the site and time interval as last 24 hours, last 1 hour, or current.



HDX QoE

Quality of Experience (QoE) is a calculated index that helps you understand your ICA quality of experience. This index is calculated for all ICA application traffic traversed from WAN to the site. Statistics of

packet drop, jitter, and latency are used in the QoE calculation. The QoE is an integer between [0, 100], the higher the number, the better the user experience. The jitter, latency, and packet drop statistics are tracked on data paths during packet processing.

Sites in the entire network are categorized as good, fair, poor, or no HDX traffic based on the QoE of HDX traffic. For more information, see HDX QoE.

To view HDX QoE, of sites, across all the regions in the network, navigate to **Dashboard** > **Default Dashboard** > **Apps** > **HDX QoE**, and in the **Region** drop-down menu select **All**.

Dashboard												
C Default Dashboard	~	Dashboard / Default Das	hboard / Apps / HDX	QoE						Re	egion: All	~
Network Apps	>	Network HDX										
Top Apps										Select	Time: Last 1 Hour	× ^
HDX QoE Management Infra		Filters: +									🗎 🖆 d	÷
Custom Dashboard	>					QoE Across SI	tes	1				¢
		Name	Total	Sites 🗸	Poor	Fair	Good	No HDX Traffic	Users		Sessions	
		Default_Region		4	0	0	0		4	0	0	
		region2		1	0	0	0		1	0	0	
		region1		0	0	0	0		0	0	0	
		Data from 20/20/18 2-11 ore to	00/00/18 2-11 ans (Asia W	silvata Tiene)								*
		Data from 09/20/18 2-11pm to	09/20/18 3·11nm (Asia/Ko	olkata Time)								

You can view the following HDX QoE metrics for the individual regions.

- Network HDX: Quality Summary
- Network HDX: Users and Sessions
- Network HDX: Bottom five Sites (Quality)
- Site HDX: Users
- Site HDX: Sessions
- Site HDX: Quality of Experience

To view HDX QoE statistics, navigate to **Dashboard** > **Default Dashboard** > **Apps** > **HDX QoE** and in the **Region** drop-down menu select a region.

Dashboard	Fault	Monitoring	Configuration	Reporting	Administration	Nitro API		
C Default Dashboard	~ >	Dashboard /	Default Dashboard / Apps	/ HDX QoE				napric (brhad, Ragion V
Apps	Ĵ	Network HDX :	Quality Summary					Network HDX : Users and Sessions
Top Apps HDX QoE Management Infra Custom Dashboard				$\left(\right)$			Good: Quel R0-100 (2) an: Quel St-84 (0) Prove: Quel S-54 (0) Prove: Quel S-54 (0) RestOCTable: (1)	2 Number of Users 2 Number of Sessions
		Network HDX :	Bottom 5 Sites (Quality)	1				Site HDX : Users
					Site Name QoE CE2K-BRANCH1 97 MCN-SITE 99			4 see sec (30:690001) ¥ 9 1 sec sec (30:69001) ¥ 0 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 1 0 1 1 1 2 2 2 2 3 1 3 4 4 5 Time
		Site HDX : Sessi	ons					Site HDX: QoE
		SSI MSI					Select Size: CB2C4RAVIEH1 ¥ Select Time: Laz 1 Hour ¥	Lo less the (BK-6940CH) V less the List 1960 V

Note

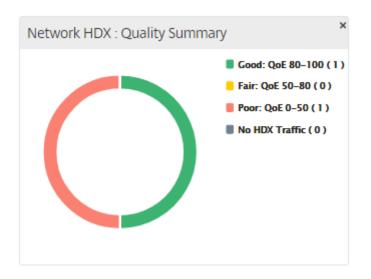
Sometimes, the HDX dashboard data and HDX reports from different sites might not seem to be in-sync because each site statistic is polled independently.

On HDX dashboard widgets, you might see a site with no HDX traffic, but there might be a nonzero number of HDX sessions and users. It happens when the HDX sessions remain idle for that polling period and still stay in open state.

Network HDX: Quality summary

The HDX traffic is classified into the following quality categories:

Quality	QoE Range
Good	80–100
Fair	50–80
Poor	0–50
No HDX Traffic	N/A



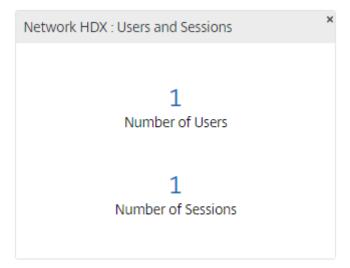
You can click the chart to view HDX reports per site. For more information, see How to View HDX Reports.

Network HDX: Users and Sessions

This widget provides information on the number of active HDX users and sessions. The number of sessions is the total number of active Single Session ICA (SSI) and Multi-Session ICA (MSI) sessions.

Note

In the current release, the number of users is not based on distinct user names. That is, two sessions started by a single user on two different machines is counted as two users.



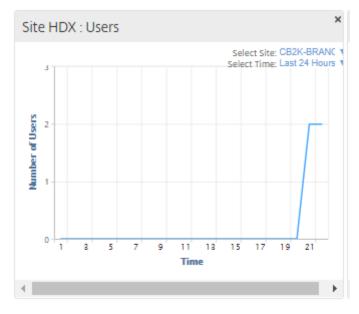
Network HDX: Bottom 5 Sites (Quality)

This widget provides a list of the bottom 5 sites that have the least QoE score. It helps drive better end-user experience initiatives.

Network HDX : Bottom	1 5 Sites (Quali	ity)
	Site Name	QOE
	CB2K-BRANCH1	100
	MCN-SITE	100
	Site1Region1	100

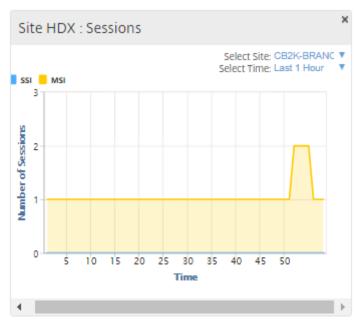
Site HDX: Users

This widget provides a graphical representation of the number of users that were active at a particular site for the selected time interval. You can select the site and the time interval as last 24 hours, last 1 hour, or last 5 minutes.



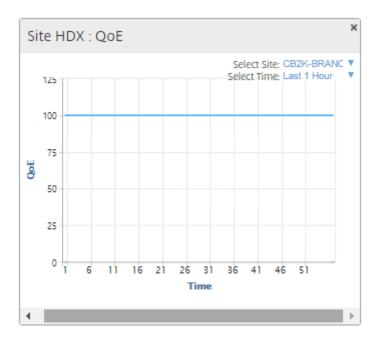
Site HDX: Sessions

This widget provides a graphical representation of the number of MSI and SSI sessions that are active at a particular site for the selected time interval. You can select the site and the time interval as last 24 hours, last 1 hour, or last 5 minutes.



Site HDX: Quality of experience

This widget provides a graphical representation of the overall QoE at a particular site for the selected time interval. You can select the site and the time interval as last 24 hours, last 1 hour, or last 5 minutes.



Application QoE

Application QoE is a measure of Quality of Experience for an application. The Application QoE score range is 0–10, where 10 represents excellent quality and 0 represents poor quality. For more information, see Application QoE. You can view application QoE score for real-time and interactive traffic.

Dashboard Fault		
Default Dashboard 🗸 🗸 🗸	Disbloard / Default Dashboard / App 3/ App QoE	Region: Default_Region *
ketwork >	Select Site: All Select App: All Select Code: All	Solert Time Last Morth
Top Apps HDX QoE	Good (QoE 8-10) Fair (QoE 4-8)	Poor (QsE 0-4)
App QoE Management Infra	QoE for Realtime Apps	QoE for interactive Apps
exergitering and	To a construction of the second secon	B Contractions

You can filter the application QoE statistics by site, application, or QoE type.

Management infra

The Management Infra page allows you to view the Citrix SD-WAN Center database usage and storage statistics.

For a multi-region deployment, you can view the database usage of all the collectors in the network. To view multi-region database statistics, navigate to **Dashboard > Default Dashboard > Management Infra** and in the **Region** drop-down menu select **All**.

Citrix SD	-WA	N	Center					R10_1_0_132_695064 ~	admin 🗸
Dashboard									
C Default Dashboard	~		Dashboard / Default I	Dashboard / Managemen	t infra			Region: All	¥
Apps	~		Database Usage (GB) ir	n Collectors					
Top Apps HDX QoE Management Inf Custom Dashboard	ra					ſ	Jatabase Total Size : 59.06 Usage		
							3.23		

To view Citrix SD-WAN Center database statistics for a particular region, navigate to **Dashboard** > **De-fault Dashboard** > **Management Infra**, and in the **Region** drop-down menu select a region.

The **Database Usage** section displays a graphical overview of the database resource usage and the thresholds for sending notifications, or halting the collection of data. You can click the graph to view the details on the Database Maintenance page.

- Usage: Database capacity currently being used, in GB.
- Notification: Threshold for generating a database usage notification. The threshold is a percentage of the maximum size of the database. If an email alert is configured, an email notification is sent when the size of the database exceeds this threshold. For more information, see Event notifications.
- **Stop Polling**: Threshold for halting statistics polling. The threshold is a percentage of the maximum size of the database. Polling stops when the size of the database exceeds this threshold. For more information, Manage database.

Citrix SD-WAN Center R10_1_0_132_695064 ~										
Dashboard										
C Default Dashboard Network	~	Dashboard / Default	Dashboard / Managemen	t Infra				Region: De	fault_Region ▼	
Apps	ý	SD-WAN Center: Data	base Usage (GB)							
Top Apps HDX QoE Management Inf Custom Dashboard	ra				Usage	Database Total Size : 2 Notification (%)	Stop Polling (%)			
					2.53	45%	50%			

Custom dashboard

You can customize the Citrix SD-WAN Center dashboard and choose the statistics that you want to view on the dashboard based on your analytical needs. Create a custom dashboard of regional details or a global summary. You can also customize an existing report.

Note

You can now pin a report as widget to your custom dashboard, by using the **Add to Dashboard** option on the Reports page.

Dashboard	Fa	ult	Monit	oring	Configuration	R	eporting	Administ	ration	Nit	tro API							
oportir	20																	
leportir	iy																	
egion: Default_	Region ~	⁄ 0																
New View Oper	n Sav	Save	e As															
Time	Septer	mber 25, :	2018 11:14	📰 Last:	Hour / Day / Week	/ Month	1							Mode: Re	lative (5 seconds ago)	~	C	
<	28. Au	119	30. Aug	1. Sep	3. Sep	5. Sep	7. Sep	9. Sep	11. S	en	13. Sep	15. Sep	17. Sep	19. Sep	21. Sep	23. Sep 2	5. Sep	
	20. AU	uБ	JU. Aug	i. sep	5. 5ch	J. Jep	7. 3ep	s. sep	11.3	cp	13. Sep	is. sep	17. 3ep	rs. sep	21. 3ep	20. 3ep 2	J. Jep	
	28. Au	ug	30. Aug	1. Sep	3. Sep	5. Sep	7. Sep	9. Sep	11.5	ер	13. Sep	15. Sep	17. Sep	19. Sep	21. Sep	23. Sep 2	5. Sep	
														A K	< 🕨 🚿 🕅 Int	erval: 1 minute	\sim	
5how Bandwidth 10 🗸 / pag			wing 1 - 10 of	162						Sea	rch						1 th	
Site 🔨		١	Virtual Servic	ce	N	ame		Тур	96		Walt Time (ms)		Sent Bandwidth		Data Pending 🛃		o (%) 🛃	
f-Site1-SC			C-MCN-NY		control_class			control_class				0.00		17.81 🛃		0.00 🛃	0.0	0 🖂
f-Site1-SC			C-MCN-NY		bulk_unused_class			bulk_class				0.00		0.00 🛃		0.00 🖂		
f-Site1-SC			C-MCN-NY		bulk_background_cla			bulk_class				0.00		0.00 🖬		0.00 🖂		
f-Site1-SC			C-MCN-NY		interactive_very_low			interactive_cla				0.00		0.00		0.00		
ef-Site1-SC			C-MCN-NY		interactive_medium			interactive_cla				0.00		0.00		0.00 🖂		
f-Site1-SC			C-MCN-NY		interactive_high_clas			interactive_cla				0.00		0.00 🖂		0.00		
	De	ef-Site1-S	C-MCN-NY		realtime_class			realtime_class				0.00		0.00 🛃	l	0.00 🛃		
			C-MCN-NY		class_9			bulk_class				0.00		0.00 🛃		0.00 🛃		
ef-Site1-SC	De	ef-Site1-S																
Def-Site1-SC Def-Site1-SC Def-Site1-SC			C-MCN-NY		class_8			bulk_class				0.00		0.00 🛃		0.00 🛃		

Enter the report name and select the custom dashboard.

Add to Custom		×
Dashboard Name:	regional Dashboard 1 🗸	
	regional Dashboard 1	
	region_2_dashboard	Add
	RegionalDB1	Add
	test	

For Regional Details custom dashboard, you can choose from the following region level widgets:

- Site Summary
- Virtual Path
- Region Events
- Region Alarm Summary
- Inventory Manager (Per Region)
- Top Sites Per Region
- Paths
- MPLS Queues
- Ethernet
- LAN GRE Tunnels
- IPsec Tunnels
- Service Summary
- Classes
- Site Events
- Top Applications Per Region
- Top Application Family Per Region
- Site HDX: Users
- Site HDX: Sessions
- Site HDX: QoE
- MOS Applications
- Database Usage

For a Global Summary custom dashboard, you can choose from the following network level widgets:

- Multi-region Summary
- Virtual Path Health in Network
- Events

- Alarm Summary
- Inventory Manager
- Top Sites in Network
- Network HDX
- Database Usage in Collectors
- Top Applications
- Top Application Families

To create a custom dashboard:

1. Navigate to **Dashboard > Custom Dashboard** and click **Create Dashboard**.

Dashboard						Nitro API
C Default Dashboard	>	Dashboard / Custom D	Dashboard			
Custom Dashboard	~	Welcome to				
Global Dashboard	>	Creating your	own Custom D	ashboard		
Regions Dashboar	d >	This View will help you cr	eate your own dashboard an	id add desirable widge	ts into the dashboard.Choo	se from an exhaustive list of widgets available on SD-WAN Center.
		To create your own Dash	board, click the "Create Da	shboard" button show	vn below.	
		To import from an existi	ng JSON file, click on " Impo r	t Dashboard" button	shown below.	
		Create Dashboard	Import Dashboard			

Note

You can also import an existing dashboard in JSON format by clicking Import Dashboard.

- 2. In the **Name** field, enter a name for the custom dashboard.
- 3. Select the widget type. Select **Global Summary** to view network level widgets, select **Regional Details** to view regional level widgets.

Create a Cu		ouru
ame*		
Regional DB1		
Vidget Type) Regional Details () G	Johal Summary	
	iobal Summary	
Region Level Widgets	B	
Configured (0)	Remove All	
Noncems		
		💠 Add
Jsers to Share Configured (0)	Remove All	
No items		
NOTETIS		🐴 Add

4. Click **Add** and select the required widgets.

The widgets are categorized into three levels: Network, Apps, and Management Infrastructure.

Dashboard	Fault	Monitoring	c	onfiguration	Reporting	Admir
[•] Create	a Custo	om Dashl	boai	ď		
Name* RegionalDB1 Widget Type Regional Deta Region Level Widg	ails 🔿 Global S	ummary				
Available (3) Search + Network + Apps		Select All	•	Configured (0)		Remove All

Note

In single-region deployment, only the **Region Level Widgets** are available.

ashboard	Fault N	Aonitoring	(Configuration	Reporting	Administration	Nitro API	
Create	a Custom	n Dashl	boa	rd				
me*								
idget Type								
	ils 🔘 Global Summa	ary						
egion Level Widge	ts							
Available (3)		Select All		Configured (3)		Remove All		
Search				Site Summary Region Alarm Summ	30/			
– 🗌 Networ	<			Top Sites Per Region	i i i i i i i i i i i i i i i i i i i			
	GRE Tunnels							
IPSe	c Tunnels							
Serv	ice Summary							
Clas	ses		•					
🔲 Site	Events		•					
Ethe	rnet							
Uirt	al Path							
🔲 Reg	on Events							
🗌 Inve	ntory Manager(Per Re	gion)						
🔲 Pati	IS	~						
	COLOLIOF							
sers to Share								
Available (7)		Select All		Configured (1)		Remove All		
radSuperuser		++	_	JohnDoe		-		
root shishir		++	•					
guest_user1 tac_tb1		++	4					
tac_tb2		+						

You can also share the custom dashboard with multiple users. For more information on users, see User accounts.

5. Click **Create**. The newly created custom dashboard is listed under **Custom Dashboard**.

Dashboard	Fault	Monitoring	Configuration	Reporting	Administration	Nitro API				
Default Dashboard	>	Dashboard / Custom	Dashboard / Regions Dash	board			Region: Default_Region 🗸	Share Edit D	elete Export	
alobal Dashboard	、 、	Network Summary								
Regions Dashboard	~								Schematic View	
regional Dashboa	rd 1	Time: September 20, 20	018 3:43pm 🛅 Last: Ho	ur / Day / Week / I	Month			Mode: Relative (1 secon	nd ago - 1 second ago) 🗸	
region_2_dashbo RegionalDB1	ard	22. Aug 24. Aug	26. Aug 28. Aug	30. Aug 1	. Sep 3. Sep	5. Sep 7. Sep	9. Sep 11. Sep	13. Sep 15. Sep 17. Se	ep 19. Sep Interval: 1 minute 🗸	
	_	Routing Domain: Any	~ Activ	ve Configuration: Configuration	fig_2ndFeb_2R					
		Atleast one Virtua	Path is DOWN	 All Virtual Paths UP congestion or mem 		 All Virtual Pa links UP 	iths and associated member	ns and associated member 🔲 Polling in progress		
			4		0		0	4		
			Total Site	s	Poor		Fair	Good		

You can edit or delete the custom dashboard.

Diagnostic packages

March 12, 2021

A diagnostic package consists of all of the system log files, system information, and other necessary details that will assist the Citrix SD-WAN Support team in diagnosing and resolving issues with your system.

After creating the package you can download it to your computer and then mail the diagnostic package to Citrix Customer Support or you can directly upload it to the Citrix Customer Support sever (or another server).

Note

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

To create a diagnostic package:

- 1. In the Citrix SD-WAN Center web interface, click the **Monitoring** tab and then click **Diagnostics**.
- In the Diagnostics Packages section, under Create Package, from the Include Workspaces
 For drop-down list select a user whose workspaces will be copied into the diagnostics.

Note

The diagnostics package will include the five configurations most recently modified by the selected user.

These packages contain important real-time system in Citrix (or another server) by clicking on Upload to FTP.	formation you can forward to Citrix Support Representatives. They may be downloaded directly through the browser or uploaded to
Only 5 diagnostics packages can exist on the system a	
Create Package	Manage Packages
Include Workspaces For : admin	Diagnostic Package: Download Upload to FTP_ Delete
Package Name: DiagnosticPackage1 Create	

- 3. In the **Package Name** field, enter a name for the diagnostic package.
- 4. Click Create. This runs a system diagnostics and generates a diagnostic package.

To download a diagnostic package:

1. In the **Diagnostics Packages** section, under **Manage Package**, from the **Diagnostic Packages** drop-down list select the package that you want to download.

	n information you can forward to Citrix Support Representatives. They may be downloaded directly through the brows	ser or uploaded to
Citrix (or another server) by clicking on Upload to F Only 5 diagnostics packages can exist on the syster		
Create Package	Manage Packages	
Include Workspaces For :	Diagnostic Package:	
admin 🗸	DiagnosticPackage1.tar.gz	
Package Name:		

2. Click **Download**. The diagnostic package is downloaded to your local computer.

To upload a diagnostic package to an FTP server:

- 1. In the **Diagnostics Packages** section, under **Manage Package**, from the **Diagnostic Packages** drop-down list select a package that you want to upload.
- Click Upload to FTP. This opens the Upload to FTP Server dialog box for specifying your FTP authentication information and uploading the package to the Citrix Customer Support FTP server, or to another FTP host.

Upload to FTP	() ×
Customer Name:	
John	
FTP Host:	
10.102.29.220	
Username:	
admin	
Password:	
•••••	
	Upload Cancel

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

A directory with this name will be created on the Citrix FTP server, and your files will be uploaded to that location.

- 4. In the **FTP Host** field, enter the IP address or host name (if DNS is configured) of the FTP server.
- 5. In the **Username** field, enter a user name to be used to log onto the FTP server.

6. In the **Password** field, enter the password associated with the user name.

7. Click Upload.

Note

It is recommended to periodically delete old diagnostic packages, to prevent exceeding the limit for the maximum allowable packages. To delete an existing diagnostic package, select a diagnostic package from the **Diagnostic Package** drop-down list, and then click **Delete**.

Events

March 12, 2021

Citrix SD-WAN Center collects event information from all the discovered appliances in the network. This event information can be filtered and viewed in the **Event Viewer** page.

The event details include the following information.

- **Time:** The time the event was generated.
- Site: The name of the site on which the event originated.
- **Appliance ID:** Shows whether the appliance from which the event originated is a primary (**0**) or secondary (**1**) appliance.

Note

The Appliance ID column is hidden by default. To display the column, click **Show/Hide** (gear icon) and select the **Appliance ID** checkbox from the drop-down menu

- Object Name: The name of the object generating the event.
- **Object Type:** The type of object generating the event.
- Severity: The severity level of the event.
- **Previous State:** The state of the object before the event. The state will be listed as **unknown** if not applicable.
- Current State: The state of the object at the time of the event.
- **Description:** A text description of the event.

Viewing events

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

To access the event viewer page.

In the Citrix SD-WAN Center web interface, click the Fault tab.

The Event Viewer page appears by default.

Dashboard	Fault	Moni		Configuration	Reporting		Administratio								
Event Viewer		Fault / E	vent Viewer												
Notification Settings		New View	Open Save	Save As											0
Severity Settings	R	<	26. Aug 3:00am	er 23, 2016 2:14am E 28. Aug 30. Aug 6:00am	Last: Hour / 1.Sep 3.Sep 9:00am	Day / Wee	7. Sep 9.	Sep 11.Sep	Mode: F 13. Sep 6:00pm		ours ago - { 17. Sep 00pm ► 3> 3>4	19. Sep 23	21. Sep Sep 1 minute	€ Sep	
		Filters: + $\begin{bmatrix} 25 \\ 1 \end{bmatrix}$	Severity greater	r than info 😠									Search		÷
		Time 🗸	Site	Object Name	Object Type	Severity	Previous State	Current State			Descr	iption			\$
		09/23/16 1:32:53	DC2-201	BR2-139-WL-1->DC2- 201-WL-2	wan_to_lan_path	NOTICE	BAD	GOOD		of wan_to_la -201 has cha			->DC2-201-W OD	/L-2.for	
		09/23/16 1:32:53	DC2-201	BR2-139-DC2-201	virtual path	NOTICE	BAD	GOOD	The state to GOOD		th: BR2-13	9-DC2-201	has changed	from BAD	>
		09/23/16 1:32:53	DC2-201	BR2-139-WL-1->DC2- 201-WL-1	wan_to_lan_path	NOTICE	BAD	GOOD		of wan_to_la -201 has cha			->DC2-201-W OD	/L-1 for	

You can select and view reports of a particular period by using the timeline controls. For more information, see, Timeline controls.

Note

You can view the events data of last 30 days. Any data beyond this period is automatically removed from the SD-WAN Center collector and the respective regional collectors.

You can also create, save and open report views. For more information, see, Manage views.

Using Filters

You can create custom filters for narrowing the Events table results.

To create and apply a filter:

- 1. Click + icon to the right of the Filters section label.
- 2. Select a category form the drop-down menu.

The options available are:

- Size
- Object Name
- Object Type
- Severity
- Previous State
- Current State
- 3. Select an operator from the middle drop-down menu.

The options are as follows:

- is
- is not
- is one of
- contains
- does not contain
- less than
- less than or equal to
- greater than
- greater than or equal to
- 4. Enter the string or value by which to delimit the filter.

Note

This field is case sensitive.

Filters: 🕂					
	Severity	\sim	is	V WARNING Add	
25 ~ /	-	0			

Note

You can create and apply multiple filters.

For Multi-region network, you can select specific regions to view event.

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

Citrix SD-WAN Center 11.4

shboard	E-ula N		C	Desertions	A	nistration	Allere A DI		
snboard	Fault M	onitoring	Configuration	Reporting	Admi	nistration	Nitro API		
nt Viewer	Fault	/ Event Viewer	_						
fication Settings		efault_Region V Default_Region	0						
erity Settings	New	ANZ APAC EMEA	Save As						
	_	Time: Febru	ary 13, 2018 12:47am	Last: Hour / Day	/ Week / 1	Month	Mode	e: Relative (15 hours ago - 8 hours from now) 🔻	
		4 16. Jar	n 18. Jan 20. Jan	22. Jan 24. Jan	26. Jan 28	i. Jan 30. Jan	1. Feb 3.	Feb 5. Feb 7. Feb 9. Feb 11. Feb 13. Feb	
		3:	00am 6:00am	9:00am	12:	:00pm	3:00pm	6:00pm 9:00pm 13. Feb	
								Interval: 1 minute ▼	
	Routing Do	main: Any	¥					L Interval: 1 minute ▼	
	Routing Do		▼ ater than info					K Interval: 1 minute ▼	0+
	Filters:			0		Searc		Interval: 1 minute ▼	÷O
	Filters:	+ Severity gre ▼ / page	ater than info 🗙	0 Object Type	Severity	Searc Previous State		Description	
	Filters:	+ Severity gre ▼ / page	ater than info X Showing 1 - 25 of 2,680		Severity		ch		
	Filters: 25 Time ↓ 02/12/18	+ Severity gre / page Site	ater than info X Snowing 1 - 25 of 2,680 Object Name ANZ_RCN-queue1	Object Type	-	Previous State	ch Current State	Description	¢
	Filters: 25 Time ~ 02/12/18 23:36:14 02/12/18	 Severity gre / page Site ANZ_RCN 	ater than info X Snowing 1 - 25 of 2,680 Object Name ANZ_RCN-queue1	Object Type wanlink	NOTICE	Previous State DEAD	ch Current State GOOD	Description WAN Link ANZ_RCN-queue1 has changed to UP	

Note

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

To download the events table as a CSV file:

Click the Download icon at the upper right corner of the events table.

For more information on event statistics, see Event report.

You can configure Citrix SD-WAN Center to send external event notifications for different event types as email, SNMP traps or syslog messages. For more information, see Event notifications.

Event notifications

March 12, 2021

You can configure Citrix SD-WAN Center to send event notifications for different event types as email, SNMP traps or syslog messages. Once you have configured the email, SNMP and syslog notification settings you can select the severity for different event types and select the mode (email, SNMP, syslog) to send event notifications. Notifications are generated for events equal to or above the specified severity level for the event type.

The available severity levels are as follows, in descending order of severity:

- EMERGENCY
- ALERT
- CRITICAL
- ERROR
- WARNING
- NOTICE
- INFORMATIONAL
- DEBUG

You can configure notification settings to receive event alerts by email, SNMP traps or Syslog messages on both Citrix SD-WAN Center and the individual Citrix SD-WAN appliances in your network.

However, enabling notifications on Citrix SD-WAN Center allows you to receive event notifications for the entire Citrix SD-WAN network (i.e., MCN and all the sites). While, enabling notifications on the Citrix SD-WAN appliances allows you to receive notifications from the individual appliances only.

It is advised to enable notifications on the Citrix SD-WAN Center only, to avoid redundant notifications from the other Citrix SD-WAN appliances in your network.

Configuring email notification settings

To configure email notification settings:

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

Dashboard	Fault	Monitoring	Configuration	Reporting	Administration	
Event Viewer		Fault / Notification	Settings / Email Alerts			
Notification Setting	js	Email Alerts	SNMP Traps	Syslog		
Severity Settings		Email Settings Enable Event Ema Destination Email Ad johndoe@clirk.com Source Email Address sd-wan-alert@clirk.co SMTP Authenticatio Enable SMTP Auth User Name johndoe01 Apply Send Test Mee	Aress(es): Host 208.123. c m n eentication Password:	79.32	Port: 25	Ø

2. Select Enable Event Emails.

3. In the **Destination Email Address (es)** field, enter the email address to which alert notifications are to be sent.

Note

You can enter multiple email addresses separated by semicolons.

- 4. In the **Host** field, enter the IP Address or hostname of an external SMTP server to relay email messages to the internet.
- 5. In the **Port** field, enter the port number to be used for the SMTP connection. The default port is 25.
- 6. In the **Source Email Address** field, enter the email address from which email alerts are sent.
- 7. Select Enable SMTP Authentication.
- 8. In the **User Name** field, enter a user name for the SMTP server used for authentication.
- 9. In the **Password** field, enter the password associated with the user name for the SMTP server used for authentication.

Note

Click **Send Test Message**, to send a sample email alert to the configured recipients.

10. Click Apply.

Configuring SNMP trap notification settings

To configure SNMP trap notification settings:

- In the Citrix SD-WAN Center web management interface, navigate to Fault > Notification Settings > SNMP Traps.
- 2. Select Enable Event SNMP Traps.

Dashboard	Fault	Monitoring	Configuration	Reporting	Administration	
Event Viewer		Fault / Notification	Settings / SNMP Traps			
Notification Settin	gs	Email Alerts	SNMP Traps	Syslog		
Severity Settings		SNMP Traps Snable Event SNI Host(s): 10.102.29.20 Apply Send Test Tra	UDP Port:			٢

3. In the **Host(s)** field, enter the IP address or the host name of an external SNMP system. This host will receive the events as SNMP traps.

Note

You can enter multiple IP addresses or hostnames separated by semicolons.

- 4. In the **UDP Port** field, enter the UDP port to be used to send the SNMP traps. By default, the UDP port is set to 162.
- 5. Click **Apply** to apply the SNMP traps notification settings.

Note

Alternately, click **Send Test Trap** to verify whether the system is able to send an SNMP trap to the configured destination.

Configuring syslog notification settings

To configure Syslog notification settings:

- In the Citrix SD-WAN Center web management interface, navigate to Fault > Notification Settings > Syslog.
- 2. Select Enable Event Syslog Messages.

Dashboard	Fault	Monitoring	Configuration	Reporting	Administration
Event Viewer		Fault / Notificatio	n Settings / Syslog		
Notification Setting	js	Email Alerts	SNMP Traps	Syslog	
Severity Settings		Syslog Enable Event Sy: Host: 10.102.29.230 Apply Send Test M			٢

- 3. In the **Host** field, enter the IP address or the host name of an external syslog server, which will be used to receive events as syslog messages.
- 4. Click **Apply** to apply the syslog notification settings.

Note

Alternately, click **Send Test Message** to verify whether the system can send a syslog message to the configured host.

Configuring event notifications

To configure event notifications:

- 1. In the Citrix SD-WAN Center web management interface, navigate to **Fault** > **Severity Settings**.
- 2. In the **Alert if Sate Persists** field, select the time duration after which if the event still persists a notification will be sent.

Dashboard	Fault	Monitoring	Configuration	Reporting		Administration						
Event Viewer		Fault / Severity Settings										
Notification Settings												0
Severity Settings						Email	_		Syslog		SNMP	_
		Event Type	Alert i	if State Persists								
		service	2 Seconds	•		CRITICAL	۳	1	CRITICAL		CRITICAL	٣
		virtual_path	10 Seconds	3 v]	WARNING	۳		WARNING		WARNING	۳
		wanlink	600 Second	is 🔻	•	ERROR	٣		WARNING		WARNING	٣
		path	Alert Imme	diately 🔻		CRITICAL	٣		WARNING	•	WARNING	¥
		dynamic_virtual_path	Alert Imme	diately 🔻		CRITICAL	۳		WARNING		WARNING	Ŧ
		wan_link_congestion	Alert Imme	diately •	•	DEBUG	۲		WARNING	•	WARNING	۳
		usage_congestion	Alert Imme	diately v		WARNING	۳	•	WARNING	V	WARNING	٣
		hard_disk			*	EMERGENCY	۳	•	WARNING		WARNING	٣
		virtual_wan				WARNING	۳		WARNING V		WARNING	T

3. For each event type select the notification option and select the severity.

Note

The Email, Syslog and SNMP notification options will be enabled only after configuring the respective notification settings.

4. Click Apply.

Configuring alarms

You can also configure alarms in Citrix SD-WAN Center and push it to individual appliances.

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

Alarm Configuration +

Event Type	Trigger State	Trigger Duration	Clear State	Clear Duration	Severity	Email Syslog	SNMP
PATH v	DEAD 🔻	0	GOOD 🔻	0	EMERGENCY •		
WANLINK v	DEAD 🔻	0	GOOD 🔻	0	ERROR •] [0 D

Select or enter values for the following fields:

- Event Type: The Citrix SD-WAN appliance can trigger alarms for particular subsystems or objects in the network, these are called event types. The available event types are SER-VICE, VIRTUAL_PATH, WANLINK, PATH, DYNAMIC_VIRTUAL_PATH, WAN_LINK_CONGESTION, USAGE_CONGESTION, FAN, POWER_SUPPLY, PROXY_ARP, ETHERNET, DISCOVERED_MTU, GRE_TUNNEL, and IPSEC_TUNNEL.
- **Trigger State:** The event state that triggers an alarm for an Event Type. The available Trigger State options depend on the chosen event type.
- **Trigger Duration**: The duration in seconds, this determines how quickly the appliance triggers an alarm. Enter '0'to receive immediate alerts or enter a value between 15-7200 seconds. Alarms are not triggered, if additional events occur on the same object within the Trigger Duration period. Additional alarms are triggered only if an event persists longer than the Trigger Duration period.
- **Clear State**: The event state that clears an alarm for an Event Type after the alarm is triggered. The available Clear State options depend on the chosen Trigger State.
- **Clear Duration:** The duration in seconds, this determines how long to wait before clearing an alarm. Enter '0'to immediately clear the alarm or enter a value between 15-7200 seconds. The alarm is not cleared, if another clear state event occurs on the same object within the specified time.
- **Severity**: A user-defined field that determines how urgent an alarm is. The severity is displayed in the alerts sent when the alarm is triggered or cleared and in the triggered alarm summary.
- **Email**: Alarm trigger and clear alerts for the Event Type is sent via email.
- **Syslog**: Alarm trigger and clear alerts for the Event Type is sent via Syslog.
- **SNMP**: Alarm trigger and clear alerts for the Event Type is sent via SNMP trap.

Memory dumps

March 12, 2021

A memory dump is generated when a process crashes. All memory dumps currently on the system can be downloaded in one combined package, and uploaded to an FTP server for examination by the Citrix support team. However, you can delete individual memory dumps.

To download memory dumps:

- 1. In the Citrix SD-WAN Center web interface, click the **Monitoring** tab and then click **Diagnostics**.
- 2. In the **Memory Dumps** section, from the **Memory Dump Package** drop-down list select a memory dump package.

Memory Dumps	0
These packages contain saved memory dumps (caused by system error events) you can forward to Citrix Support Representatives. They may be downloaded directly through the browser or uploaded to Citrix (or another server) by clicking Upload All to FTP.	r
Memory Dump Package:	
Download All Upload All to FTP	

3. Click **Download All**. Save the memory dump package on your local computer.

To upload a memory dump package to an FTP server:

- 1. In the **Memory Dumps** section, from the **Memory Dump Package** drop-down list select a memory dump package.
- 2. Click **Upload to FTP Server**. This opens the **Upload All to FTP** dialog box for specifying your FTP authentication information and uploading the package to the Citrix Customer Support FTP server, or to another FTP host.

Upload to FTP		(?) ×
Customer Name:		
John		
FTP Host: 10.102.29.220		
Username: admin		
Password:		
	Upload	Cancel

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

A directory with this name will be created on the Citrix FTP server, and your files will be uploaded to that location.

- 4. In the **FTP Host** field, enter the IP address or host name (if DNS is configured) of the FTP server.
- 5. In the **Username** field, enter a user name to be used to log onto the FTP server.
- 6. In the **Password** field, enter the password associated with the user name.

7. Click Upload.

Log files

March 12, 2021

The Log files collect information related to the web console, user interface exceptions, internal crashes and so on. These logs can be used to troubleshoot issues in the Citrix SD-WAN Center.

To view log files:

- 1. In the Citrix SD-WAN Center web interface, click the **Monitoring** tab.
- 2. Click **Diagnostics**.
- 3. From the **Log File** drop-down list, select the log file you want to view.

Dashboard		Monitoring	Configuration	Reporting	Administration	
Network Map	M	fonitoring / Diagnos	tics			
Statistics	Lo	g Files				0
Diagnostics		; File: WC_access.log				
System Information			View Download			

4. Click **View**. The log file content is displayed.

Dashboard	Fault Moni	toring Configuratio	on Reporting	Administration	
Network Map	Monitoring	/ Diagnostics			
Statistics	VWC_	access.log			
Diagnostics	Refresh				
System Information	0000:059 R5ec:Sec 0000:000 0000:100 0000:180 0000:280 0000:280 0000:000 0000:000 0000:000 0000:000 0000:195 0000:195 0000:195 0000:120 0000:100 0000000000	1990:946 INFO 1951 u5 INFO Log file 1021:749 INFO min8auti 1004:950 INFO 1004:350 INFO 1003:774 INFO 1003:714 INFO 1003:193 INFO 1003:193 INFO 1003:614 INFO 1012:218 INFO min8auti 1009:914 INFO 1127:189 INFO 1127:189 INFO	Current tim opened at Thu Sep Ad.et740 Dee Current tim Current tim	main socket opened, listening for connections me is:Thm 3ep 1 18:49:51 2016 me is:Thm 3ep 1 18:50:51 2016 me is:Thm 3ep 1 18:52:51 2016 me is:Thm 3ep 1 18:52:51 2016 me is:Thm 3ep 1 18:55:51 2016 1 18:54:47 2016 main socket opened, listening for connections me is:Thm 3ep 1 18:55:47 2016 19 Thread 3: Request auth_req for user admin	

5. If you want to download the log files to your computer, click **Download**.

Polling interval

March 12, 2021

Polling refers to the process of collecting statistics from the discovered appliance. You can configure the interval and bandwidth limit for polling operations after discovering the appliances. For information on discovering the appliance, see Single-region network deployment or Multi-region network deployment.

To perform polling configuration:

1. In the Citrix SD-WAN Center web interface, navigate to **Configuration** > **Network Discovery** > **Discovery Settings**.

Dashboard	Fault	Monitoring	Configuration	Reporting A	
Network Discovery		Configuration / Netw	vork Discovery / Discove	y Settings	
Network Configuration	n	SSL Certificate	Discovery Setting	Inventory And St	atus
Zero Touch Deployme	nt				
Change Management		Master Control Node MG 10.105.187.111	FIP Address: est		
Appliance Settings		Rediscover			
		Polling Configuration			0
		Polling Interval (min):	Bandwidth Limit 1000	kbps):	0
		Apply			

- 2. In the **Polling Interval** field, enter the polling frequency in minutes. The range is 2–60 minutes. The default value is 5 minutes.
- 3. In the **Bandwidth Limit** field, enter the polling bandwidth limit in kbps. The MCN will limit bandwidth to the specified value when transferring polling statistics from the appliance to the Citrix SD-WAN Center. The range is 100 Kbp –1 Gbps. The default value is 1 Mbps.
- 4. Click **Apply**.

Statistics

March 12, 2021

You can view the statistics collected by Citrix SD-WAN Center as graphs. These graphs are plotted as timeline versus usage, allowing you to understand the usage trends of various network object properties. You can view graphs for network-wide application statistics. For every site in the SD-WAN network, you can view graphs for the following network parameters:

- Bandwidth
- QoS
- Virtual Path
- Internet Services
- Intranet Services
- Pass-through Services
- WAN Links
- Ethernet Interfaces
- GRE Tunnels
- IPsec Tunnels
- Applications
- Application Families

You can create views as per your requirement, save it and open existing views.

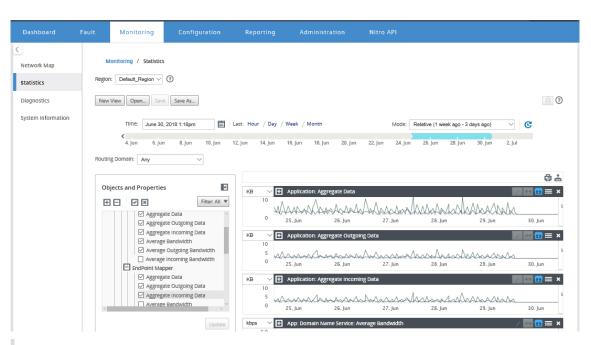
To view statistical graphs:

- 1. In Citrix SD-WAN Center web UI, navigate to **Monitoring** > **Statistics**.
- 2. Select a region and a routing domain.
- 3. From the **Objects and Properties** hierarchical tree, find and select the properties of interest.

Тір

You can also use the **Filter** drop-down menu and **Presets Menu** to simplify the process of finding and selecting properties.

4. Click **Update** to display graphs for the selected properties.



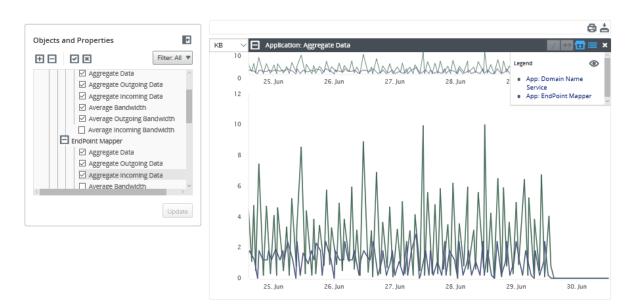
Deselect a property and click **Update** to remove the graph for that property from the Graphs Display area.

5. Select a period for the current view. For more information, see Timeline Controls

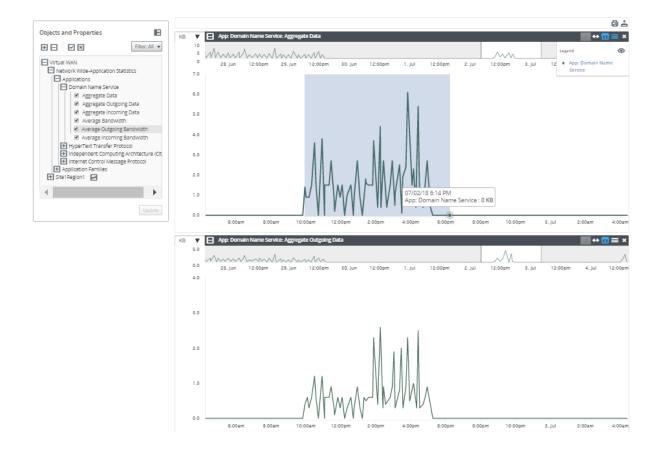
The graphs are displayed based on the selected properties.

Тір

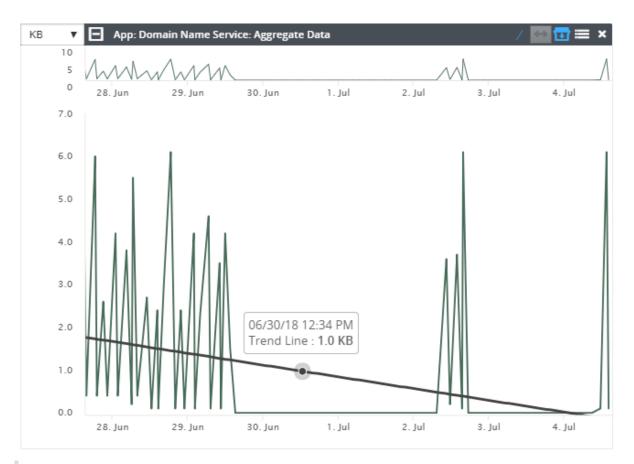
If you select more than one property, the graphs display in **Trend View** mode to save vertical space. Click on a graph heading to show and hide the fully expanded graph. You can also show and hide the trend view and legends on the graphs.



To zoom a graph, click and drag the graph plot area. Zooming on one graph zooms all graphs, to the selected time, to maintain a consistent view. Click the reset icon (↔) to reset the zoom.



You can show and hide the trend line by clicking the (/) icon.



Note

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

System information

March 12, 2021

The following information is displayed on the system information page:

- **Citrix SD-WAN Center Software Version**: The Citrix SD-WAN Center software version currently installed and running on this virtual machine.
- **Configuration Plugin Version**: The version of the Configuration Editor Plugin currently installed and running in this Citrix SD-WAN Center virtual machine.

- Hard Disk Usage: The amount of hard disk space used by the operating system and data partitions.
- **Logged-in Users**: The user name, IP Address, and logon type for each user currently logged into this Citrix SD-WAN Center virtual machine.

To display the system information:

In the Citrix SD-WAN Center web interface, click the **Monitoring** tab and then click **System Informa-tion**.

Dashboard		Monitoring	Configuration	Reporting	Administration			
Network Map Statistics		Monitoring / System	information					0
Diagnostics		SD-WAN Center Softwar	e Version: R9_1_0_81_537	013 (built 2016-08-23)			Hard Disk Usage	
System Information		Configuration Plugi	n Version: R9-1-0-81-5370	13			Partition	Usage
5,510.11.10.11.11.10.11							Active OS	37%
		.ogged-in Users						
		Usern	ame		IP Address		Login Type	
	ac	min		10.252.243.20		web		

Reporting

March 12, 2021

Citrix SD-WAN Center provides the following reports:

- **Applications:** Displays details about incoming traffic, outgoing traffic and total traffic of the top applications, sites, and application families.
- HDX: Displays detailed HDX data for every site.
- **Sites:** Displays site level statistics for every site in the Virtual WAN. Sites rows expand to show the **Services** table filtered for the Site.
- **Service:** Displays summary statistics by service type (Virtual Path, Internet, Intranet and Passthrough) for every site in the Virtual WAN. Services rows expand to show the individual Services for the Service type.
- **Virtual Paths:** Displays Virtual Path level statistics for every Virtual Path in the SD-WAN. Virtual Paths rows expand to show the Paths contained within the Virtual Path.

Note

Virtual Path data is recorded from the perspective of both endpoints, as such, each Virtual Path

may have two rows identified by the Site that recorded the statistics.

- Paths: Displays Path level statistics for every Path in the Virtual WAN.
- WAN Links: Displays WAN Link level statistics for every WAN Link at each Site in the Virtual WAN. WAN Links rows expand to show a Usage Summary for each Service type for that WAN Link. Each Service type row will then expand to show usages for each Service of that type. If the WAN Link is a Private MPLS link, a second table will be shown showing the MPLS Queues for the WAN Link.
- **MPLS Queues:** The MPLS Queues rows expand to show a usage summary for each Service type for that Queue. Each Service type row will then expand to show usages for each Service of that type.
- Classes: Displays Class level statistics for every Class for each Virtual Path in the Virtual WAN.
- **MOS Score**: The mean opinion score (MOS) provides a numerical measure of the quality of the experience that an application delivers to end users.
- **Ethernet Interfaces:** Displays Ethernet Interface level statistics for every Interface at each Site in the Virtual WAN.
- **GRE Tunnels:** Displays statistics of every LAN GRE tunnel at each site in the WAN.
- **IPsec Tunnels:** Displays statistics of every IP security tunnel at each site in the WAN.
- **Events:** Displays summary counts of events occurring at each Site in the Virtual WAN. **Events** rows expand to show summary counts by Object Type for that Site. Each Object Type will then expand to show summary counts for each Object of that type.

On the **Reporting** tab of the Citrix SD-WAN Center web interface, you can view all reports or selected reports. You can also download reports.

ashboard	Fault	Monito	oring Co	onfiguration	Reporting	Administ	ration	Nitro API						
eportin														
gion: Default_R	tegion 🗸 🕐													
ew View Open	Save Sav	e As												
Time:	September 25,	2018 2:04pm	🛗 Last: Hou	r / Day / Week	/ Month						Mode: Relative (1	week ago - 35 seco	inds ago) 🖌 🕑	
<	28. Aug	30. Aug	1. Sep	3. Sep	5. Sep 7. Sep	9. Sep	11. Sep	13. Sep	15. Sep	17. Sep	19. Sep 2	1. Sep 23. 5	Sep 25. Sep	
		- E											. I.	
	19. Sep	12:00pm	20. Sep	12:00pm	21. Sep	12:00pm	22. Sep	12:00pm	23. Sep	12:00pm			Sep 12:00pm	
											25 251 A	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	val: 1 minute 🗸	
outing Domain:	Any	~												
Applications	HDX MOS	Services	Classes Sites	Virtual Paths	Paths WAN Links	MPLS Queues	Ethernet GF	E IPsec	Events					
eport Type:	Top Applications	~	Select Site:		-									
	Data in Kbps/		rs: +										🗎 🖒	. + 4
10 V / page	e Sho	wing 1 - 2 of 2					Search							
Applica	tion Name	A	ggregate Data 🛃 🤉	 Aggregate 	Outgoing Data 🛃	Aggregate Inc	coming Data 🛃	Averag	e Bandwidth 🛃	Average O	utgoing Bandwidth 🛃	Average Ir	ncoming Bandwidth 🛃	
rf			18,747.79		9,373.90 🛃	l	9,373.90	3	416.62	3	208.3		208.3	.31 🖂
ernet Control M	essage Protocol		411.60		205.80 🖻	I	205.80	3	1.19 🛛	9	0.6	Ð	0.6	.60 🛃
	8 2:04pm to 09/2	5/18 2:05pm (/	sia (Kolkata Timo)											

You can select and view reports of a particular time frame by using the timeline controls. For more

information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.

For Multi-region network, you can select specific regions to view statistic reports.

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

Dashboard	Fault	Monitoring	Configuration	Reporting	Administration	Nitro API			
Region: Default_R region1 New Vi region2 Default_Re	tegion 🗸 🖓 Savi	e As							0
Time:	September 25, 28. Aug 19. Sep	30. Aug 1. Sep	st: Hour / Day / Week 3. Sep 0. Sep 12.00pm	/ Month 5. Sep 7. Sep 21. Sep	9. Sep 11. Se 12:00pm 22. Sep	p 13. Sep 15. Sep 12:00pm 23. Sep	17. Sep 19. Sep 21. Se 12:00pm 24. Sep 12:00p		
Routing Domain:	Any HDX MOS	Services Classes	Sites Virtual Paths	Paths WAN Links	MPLS Queues Ethernet	GRE IPsec Events			
Report Type: Show Bandwidthu 10 v / page		Select Site B Filters: + Wing 1 - 2 of 2	2:	~	Search			日 岱。	≟ ⊕
Applica	tion Name	Aggregate D	ata 🖂 🗸 🛛 Aggregate (Outgoing Data 🛃	Aggregate Incoming Data	Average Bandwidth	Average Outgoing Bandwidth 🖃	Average Incoming Bandwidth 🖂	¢.

Note

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

For more details on viewing different reports, see the following topics:

Application report Bandwidth report Class report Ethernet interface report Event report GRE tunnel report HDX report IPsec tunnel report Link performance report MOS for applications MPLS queues report

Application report

March 12, 2021

Deep packet inspection (DPI) enables the SD-WAN appliance to parse the traffic passing through it and identify the application and application family types. Citrix SD-WAN appliance records the number of bytes and bandwidth of incoming and outgoing traffic of every application. SD-WAN Center polls the SD-WAN appliance at the defined polling interval, obtains this data, and displays it on the dashboard and as reports.

You can view top applications, top sites, and top application family reports. These reports provide details about the total, incoming, and outgoing data and bandwidth.

To view application reports in Citrix SD-WAN Center:

- 1. In Citrix SD-WAN Center web UI, navigate to **Reporting** > **Applications**.
- 2. In the time-line control, select the time interval. For more information, see Timeline controls.
- 3. Select the unit to display the data. You can choose to view report data in units of Kbps, Mbps, or Gbps.
- 4. From the **Report Type** drop-down list, select one of the following report types:
 - **Top Applications**: The top applications used in the network for the selected time interval. You can filter top application by site name. By default, the top applications for all the sites are displayed.
 - **Top Application Families**: Top application families used in the network. You can filter top application families by site name. By default, the top application families for all the sites is displayed.
 - **Top Sites**: Traffic at the top sites for the selected time interval. You can filter top sites by application or application family name.

r: Default_Region w View Open_ Save Time: Septemt 28 Aug 19 Se	Save As hber 25, 2018 2:04pm 30, Aug	1. Sep		/ Month 5.5ep 7.5ep 21.5ep	9. Sep 12.00pm	11. Sep 22. Sep	13. Seg	0 15. Sep 23. Sep	17. Sep	19. Sep 21. Sep		25. Sep	
View Open Save	Save As hber 25, 2018 2:04pm 30, Aug	1. Sep	3. Sep 1	5. Sep 7. Sep						19. Sep 21. Sep	p 23. Sep	25. Sep	
Time: Septemb	nber 25, 2018 2:04pm 30. Aug	1. Sep	3. Sep 1	5. Sep 7. Sep						19. Sep 21. Sep	p 23. Sep	25. Sep	
< 28. Aug	30. Aug	1. Sep	3. Sep 1	5. Sep 7. Sep						19. Sep 21. Sep	p 23. Sep	25. Sep	
										19. Sep 21. Sep			
19. Se	iep 12:00pn	n 20. Sep	12:00pm	21. Sep	12:00pm	22. Sep	12:00pm	23. Sep	12.00am				
									12.500	24. Sep 12:00pn		12:00pm minute	
uting Domain: Any	~]											
pplications HDX N	MOS Services	Classes Sites	Virtual Paths	Paths WAN Links	MPLS Queues	Ethernet	GRE IPsec	Events					
port Type: Top Applic		Select Site:		-								8 C	÷ (
10 🗸 / page	Showing 1 - 2 of 2	2				Search							
Application Name	ie -	Aggregate Data 🛃 🗸	Aggregate (Outgoing Data 🛃	Aggregate Inc	oming Data 🛃	Averag	ge Bandwidth 🛃	Average Out	going Bandwidth 🖂	Average Incomin	g Bandwidth 🛃	
f		18,747.79		9,373.90 🛃		9,373.9		416.62		208.31 🛃		208.3	
rnet Control Message Pro	otocol	411.60	2	205.80 🛃		205.8	30 🛃	1.19	3	0.60 🛃		0.6	60 🛃

For each report type, you can view the following data:

- Aggregated Incoming Data: Application data coming into the site from the WAN.
- Aggregated Outgoing Data: Application data sent from the site to the WAN.
- Aggregated Data: Sum of incoming and outgoing traffic.
- Average Incoming Bandwidth: Bandwidth of incoming application traffic.
- Average Outgoing Bandwidth: Bandwidth of outgoing application traffic.
- **Average Bandwidth**: Total bandwidth consumed by incoming and outgoing application traffic.

Тір

For every value, you can hover the mouse cursor over the graph icon to view a mini-graph, or click to open graph view in another window. For more information, see **Statistics**.

Application QoE report

March 12, 2021

Application QoE is a measure of Quality of Experience for an application. The Application QoE score range is 0–10, where 10 represents excellent quality and 0 represents poor quality. For more information, see **Application QoE** section.

To view Application QoE report:

In Citrix SD-WAN Center, navigate to **Reporting > App QoE**, and in the timeline control select a time period.

You can select and view reports of a particular period by using the timeline controls. For more information, see, Timeline controls.

You can also create, save, and open report views. For more information, see, Manage views.

gion: Default_Region														
	• 🕜													
iew View Open	Save As													
Time: Dec	ember 5, 2018 11:03am	Last: Hour / Day / V	veek / Month									Mode: Relative (1 month ag	go - 17 hours from now) 🔻 🕓	
6. Nov	7. Nov B. Nov	9. Nov 10. Nov 11. Nov	12 New 11	3. Nov 14. Nov	15. Nov 16. Nov 17.	ine 18 New 11	0 New 20 New	21 New 22 New 21	New 24 New	25 New 26 New	27. Nov 28. Nov 29. Nov	30. Nov 1. Dec 2. Dec	3.Dec 4.Dec 5.Dec	
6. Nov				3. Nov 14. Nov				dint.m.t					3. Dec 4. Dec 5. Dec	
												A	394 Interval: 1 minute 🔻	
Applications HDX		Services Classes Sites	Virtual Patris	Patris View Links	s MPLS Queues Ethe	net GRE IPsec	Bients						8	±
Applications HDK	App Qoe MOS	rs: +	Virtual Paths	Petro VIVIN Links	s MPLS Queues Ethe	et GRE IPsec								54
Applications HDX now Bandwidtry/Data	App QoE MOS	rs: +		Petrs VIVIN Links	5 MPLS Queues Ethe	Search		Realtome Loss (%)	Realt	sme jitter(rns) 🕞	Interactive Latency(ms) 🛃	Interactive Loss (H) 🛃	Interactive jitter(ms) @	
Applications HDX how Bandwidth/Data 10 T / page Application A	App QoE MOS n Happ KB V Fitte Showing 1 - 8 of 8	n: +				Search			Reality	Sime jitter(rm) 🖯 194 🖯	interactive Latercy(rms) 🔒	_	interactive jitter(ms)	3
Applications HDX how Bandwidth/Data I 10	App QoE MOS App QoE MOS In HapsNB • Pitto Showing 1 - 8 of 8 MOH-Sitte MOH-Sitte CB2X-8RANCH1	IS: + Vitual Service. CB2X-BRANCH1-MCN-SITE CB2X-BRANCH1-MCN-SITE		Realtime Qot (2) NA (2) NA (2)	Interactive Qot 🛃	Search	tency(ms) (2 NA (2 NA (2		×8	NA 🖻	81.7 82.1	1 E 0.99	interactive jitter(ms) @	3 3.23 (3.64 (
Applications HDX now Bandwidtr/Data I 10 V / Page Application A Background Background Buik/Transfer	App Qot MOS App Qot MOS App Qot MOS App Qot MOS App Qot App Qo	INS:		Realtime Qot (; NA (;) NA (;) NA (;)	Interactive Qot 🛃	Search	tency(ms) () NA () NA () NA ()				81.7 82.1 81.7	1 2 0.99 9 2 0.00 4 2 0.75	interactive jitter(ms) (;	3.23 (3.64 (3.96 (
Applications HDX how Bandwicthrybara I 10 / page Application A Background Background Buik-Transfer Buik-Transfer	App Qot MOS N Reserve Filter Showing 1 - 8 of 8 MOS MON-STE CBD/-88A/CH1 MOH-STE CBD/-88A/CH1			Realtime Qot 😅 NA 🗟 NA 🗟 NA 🗟 NA 🗟	Interactive QoE 🛃 Colors To de El Ente El	Search	tency(ms) () NA () NA () NA () NA ()		*8		01.7 82.1 81.7 82.2	1 E 0,99 9 E 0,00 4 E 0,75 8 E 0,00	interactive jitter(ms) g	3.23 (3.64 (3.96 (4.74 (
Applications HDX how Bandwidth/Cata I to	App QoE MOS n klaps-KB V PRE Snowing 1 - 8 of 8 MO4-SITE CB3X-BANCH1 MO4-SITE CB3X-BANCH1 MO4-SITE			Realtime Cot 2 NA 23 NA 23 NA 23 NA 23 NA 23	Interactive Qof E 100 (1) 100 (2) 100 Search	tency/ms) () NA () NA () NA () NA () NA ()				01.7 82.1 81.7 82.1 83.5	1 2 0.99 9 2 0.00 4 2 0.75 8 2 0.00 7 2 1.57	interactive jitter(ms) g	3.23 E 3.64 E 3.96 E 4.74 E 2.00 E	
outing Domain: Any Applications HDX now Bandwictry/Data I 10 V / page Application A Background Background Buil-Transfer Linteractive Linteractive Linteractive Backtrove	App Qot MOS N Reserve Filter Showing 1 - 8 of 8 MOS MON-STE CBD/-88A/CH1 MOH-STE CBD/-88A/CH1			Realtime Qot 😅 NA 🗟 NA 🗟 NA 🗟 NA 🗟	Interactive QoE 🛃 Colors To de El Ente El Ente El	Search	tency(ms) () NA () NA () NA () NA ()		*8		81.7 81.1 81.7 82.1 83.5 82.1 83.5 86.0	1 E 0,99 9 E 0,00 4 E 0,75 8 E 0,00	interactive jitterjins; [] [2] [2] [2] [2] [2] [2] [2] [2]	3232 E 324 E 326 E 200 E 200 E 200 E

You can view the following metrics:

- **Application**: The application or application object name.
- Site: The name of the site.
- Virtual Service: The virtual path service used.
- Real-time QoE: The QoE score for real-time traffic.
- Interactive QoE: The QoE score for interactive traffic.
- Real-time Latency: The latency in milliseconds for real time traffic.
- Real-time Loss: The loss percentage for real-time traffic.
- Real-time Jitter: The jitter observed in milliseconds for real time traffic.
- Interactive Latency: The latency in milliseconds for interactive traffic.
- Interactive Loss: The loss percentage for interactive traffic.
- Interactive Jitter: The jitter observed in milliseconds for interactive traffic.

Тір

For every value, you can hover the mouse cursor over the graph icon to view a mini-graph, or click to open graph view in another window.

For more information, see Statistics.

Bandwidth report

March 12, 2021

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

In the Citrix SD-WAN configuration, traffic flowing through the virtual paths is classified as belonging to realtime, interactive, or bulk class types. The classes are predefined, but you can customize these classes and apply rules to them. For more information, see Customizing Classe and Rules by IP Addess and Port Number.

Using Citrix SD-WAN Center, you can view, along with the basic bandwidth statistics, the bandwidth consumed by applications belonging to these class types at each site, path or WAN link level.

To view bandwidth statistics:

In Citrix SD-WAN Center, navigate to **Reporting** > **Sites**, and in the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.

					Re	eporting										
Doportin	-															
Reportin	g															
Region: Default_R	egion 🗸 🖓															
New View Open.	Save Save	e As														0
Time:	September 25,	2018 2:11pm	📰 Last:	Hour / Day / Week	/ Month								Mode: Re	lative (1 week ago - 12 sec	onds ago) 🗸 🕑	
<	28. Aug	30. Aug	1. Sep	3. Sep	5. Sep	7. Sep	9. Sep	11. Sep		13. Sep	15. Se	p 17. Sep	19. Sep	21. Sep 23.	Sep 25. Sep	
															. I.	
	19. Sep	12:00pm	20. S	p 12:00pm	21	. Sep 12:0	00pm 2	22. Sep	12:00p	m	23. Sep	12:00pm	24. Sep		Sep 12:00pm	
														i ≪ ► ≫ ≫i Inter	val: 1 minute 🗸	
Routing Domain:	Any	~														
Applications	HDX MOS	Services	Classes Si	es Virtual Paths	Paths	WAN Links M	PLS Queues	Ethernet	GRE	IPsec	Events					
Show Bandwidth/	Data in Kbps/k	æ v Filte	ers: +												Br	i 📥 🚯
10 🗸 / page		ving 1 - 4 of 4						Search								
10 V page	51104	virig 1 - 4 01 4						Search								
						LAN to WAN								WAN to LAN		•
Name 🔨	Bandwidth 🛃	Available Ba	andwidth 🛃	Permitted Bandwidt	n 🛃 🛛 Cor	ntrol Bandwidth 🛃	Realtime Ba	andwidth 🛃	Interac	ctive Bar	idwidth 🛃 🛛	Bulk Bandwidth 🛃	Bandwidth 🛃	Available Bandwidth 🛃	Permitted Bandwidt	
+ Def-Site1-SC	18.10 🖃	1	20,000.00 🛃	16,333	88 🖂	18.10	Ø	0.00	3		0.00 🛃	0.00 🖬	15.05 🛃	19,600.00 🖻	15,762	25 🖬
+ MCN-NY	49.54 🛃	1	50,000.00 🛃	49,988	95 🛃	49.54		0.00 🖻	3		0.00 🛃	0.00 🛃	55.70 🛃	49,000.00	48,990	.45 🛃
+ R1-RCN-MUM	35.81 🖃	1	250,000.00 🛃	27,230	67 🛃	35.68	8	0.00	3		0.14 🖃	0.00 🖂	38.87 🛃	245,000.00 🖃	60,023	.67 🖂
R2-RCN-SA	20.14 🛃	1	100,000.00 🖬	17,737	22 🛃	20.14	Ø	0.00 🖻	3		0.00 🛃	0.00 🖬	16.12 🛃	98,000.00 🖻	50,072	.00 🖂
Data from 09/18/18	2:11pm to 09/25	5/18 2:11pm (A	Asia/Kolkata Tir	ne)												

You can view the following metrics:

- **Bandwidth**: Total bandwidth consumed by all packet types. Bandwidth = Control Bandwidth + Realtime Bandwidth + Interactive Bandwidth + Bulk Bandwidth. For example, in the above screen shot, at SITE2, Bandwidth = 1120.99+166.61+117.21+810.78+26.40
- Available Bandwidth: Total bandwidth allocated to all the WAN links of a site.
- **Control Bandwidth**: Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.
- **Permitted Bandwidth**: Bandwidth available for transmitting information.
- **Realtime Bandwidth**: Bandwidth consumed by applications that belong to the realtime class type in the Citrix SD-WAN configuration. The performance of such applications depends to a great extent upon network latency. A delayed packet is worse than a lost packet (for example, VoIP, Skype for Business).
- **Interactive Bandwidth**: Bandwidth consumed by applications that belong to the interactive class type in the Citrix SD-WAN configuration. The performance of such applications depends to a great extent upon network latency, and packet loss (for example, XenDesktop, XenApp).
- **Bulk Bandwidth**: Bandwidth consumed by applications that belong to the bulk class type in the Citrix SD-WAN configuration. These applications involve very little human intervention and are mostly handled by the systems themselves (for example, FTP, backup operations).

Class report

March 12, 2021

The virtual services can be assigned to particular QoS classes, and different bandwidth restraints can be applied to different classes. A class can be one of three basic types:

- **Real-time classes**: Serve traffic flows that demand prompt service up to a certain bandwidth limit. Low latency is preferred over aggregate throughput.
- **Interactive classes**: Serve traffic flows that are sensitive to loss and latency. Interactive classes have lower priority than real-time but have absolute priority over bulk traffic.
- **Bulk classes**: Serve traffic flows that require high bandwidth and are sensitive to loss. Bulk classes have the lowest priority.

Specifying different bandwidth requirements for different classes enables the virtual path scheduler to arbitrate competing bandwidth requests from multiple classes of the same type. The scheduler uses the Hierarchical Fair Service Curve (HFSC) algorithm to achieve fairness among the classes.

For more information about customizing classes, see Customizing Classes.

To view class statistics:

In Citrix SD-WAN Center, navigate to **Reports** > **Classes**, and in the timeline control select a time period.

You can select and view reports of a particular period by using the timeline controls. For more information, see, Timeline controls.

Note

You can view the Class data of last 30 days. Any data beyond this period is automatically removed from the SD-WAN Center collector and the respective regional collectors.

You can also create, save and open report views. For more information, see, Manage views.

				Reporting	Administ									
Reportin														
Region: Default_Re		e As												0
Time:	October 3, 2018	3:10pm	Last: Hour / Day / Week /	Month						Mode: Re	lative (1 second ago)	~	C	
< 4. Sep	6. Sep	8. Sep	10. Sep 12. Sep	14. Sep	16. Sep	18. Sep	20. Sep	22. Sep	24. Sep 26. Sep	28. S	ер 30. Sep	2. Oct		
4. Sep	6. Sep	8. Sep	10. Sep 12. Sep	14. Sep	16. Sep	18. Sep	20. Sep	22. Sep	24. Sep 26. Sep	28. S	ep 30. Sep K K >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	2. Oct Interval: 1 minut	• 🗸	
Show Bandwidth/	HDX MOS Data in Kbps/Ki		Sites Virtual Paths P.	aths WAN Links	MPLS Queues	Ethernet GRE		Events					80	± @
10 V / page	Shov	ving 1 - 10 of 162 Virtual Service		Name			Search	ait Time (ms)	Sent Bandwidth	-	Data Pending 🛃	Dra	p (%) 🛃	¢
Def-Site1-SC	Def-Site1-	SC-MCN-NY	control_class	vame	control_c	Type	**	aic rime (ms) 0.		17.13	Data Pending 🗠	0.00	0.0	
Def-Site1-SC		SC-MCN-NY	_ bulk_unused_class		bulk_clas			0.		0.00 🖬		0.00 🖬		_
Def-Site1-SC	Def-Site1-	SC-MCN-NY	bulk_background_cla	55	bulk_clas	5		0.	00	0.00 🖬		0.00 🖬		
Def-Site1-SC	Def-Site1-	SC-MCN-NY	interactive_very_low_	class	interactiv	e_class		0.	00	0.00 🖬		0.00 🖬		
Def-Site1-SC	Def-Site1-	SC-MCN-NY	interactive_low_class		interactiv	e_class		0.	00	0.00 🖬		0.00 🛃		
Def-Site1-SC	Def-Site1-	SC-MCN-NY	interactive_medium_	class	interactiv	e_class		0.	00	0.00 🖬		0.00 🖬		
Def-Site1-SC	Def-Site1-	SC-MCN-NY	interactive_high_class	5	interactiv	e_class		0.	00	0.00 🖬		0.00 🖬		
Def-Site1-SC	Def-Site1-	SC-MCN-NY	realtime_class		realtime_	class		0.	00	0.00 🛃		0.00 🛃		
Def-Site1-SC	Def-Site1-	SC-MCN-NY	class_9		bulk_clas	5		0.	00	0.00 🛃		0.00 🛃		
Def-Site1-SC	Def-Site1-	SC-MCN-NY	class_8		bulk_clas	5		0.	00	0.00 🖬		0.00 🖬		
Data from 10/03/18	3:01pm to 10/03	/18 3:11pm										1 2 3 4	5 17	> »I

You can view the following metrics:

- Name: Class name
- **Type**: Class Type. Releatime, interactive, or bulk.
- Wait Time: The time interval between transmitting packets in milliseconds.
- Sent Bandwidth: Transmitted bandwidth
- Data Sent: Data sent, in Kbps.
- Packets Sent: Number of packets sent.
- Data Pending: Data to be sent, in Kbps.
- Packets Pending: Number of packets to be sent.
- **Drop**: Percentage of data dropped.
- Data Dropped: Data dropped, in Kbps.

- **Packets Dropped**: Number of packets dropped, because of network congestion.
- Data Coverage: Percentage of the selected period for which data is available.

Note

Click the settings icon to select the metrics that you want to view.

Ethernet interface report

March 12, 2021

Citrix SD-WAN Center provides a central view of all the Ethernet interfaces on the different Citrix SD-WAN appliances on your SD-WAN network. This helps you during troubleshooting to quickly see whether any of the ports are down. You can also view the transmitted and received bandwidth, or packet details at each port. You can also view the number of errors that occurred on these interfaces during a certain time period.

The Ethernet interfaces are configured on each Citrix SD-WAN appliance during setting up the SD-WAN network.

For information about configuring interface groups for MCN sites, see Configure MCN.

For information about configuring interface groups for branch sites, see Configure Branch Node.

To view Ethernet interface statistics:

In Citrix SD-WAN Center, navigate to **Reports** > **Ethernet**, and in the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.

				Reporting	Adminis						
Reportin	ig										
egion: Default_R	Region 🗸 🕐										
New View Open	n Save Sa	ve As									<u>(</u>
Time:	September 25	5, 2018 3:11pm 🛗 Li	ast: Hour / Day / Week	/ Month				Mod	e: Relative (1 week ago - 1	14 seconds ago) 🗸 😅	
<											1
	28. Aug	30. Aug 1. Sep	3. Sep	5. Sep 7. Sep	9. Sep	11. Sep 13. S	p 15. Sep	17. Sep 19.	Sep 21. Sep	23. Sep 25. Sep	
	19. Sep	12:00pm 20	. Sep 12:00pm	21. Sep	12:00pm	22. Sep 12:00pm	23. Sep	12:00pm 24. Sep	12,00	25. Sep 12:00pm	
	19. Sep	12:00pm 20	. Sep 12:00pm	21. Sep	12:00pm	22. Sep 12:00pm	23. Sep	12:00pm 24. Sep		25. Sep 12:00pm Interval: 1 minute v	
								A1		Thinks 1	
Routing Domain:	Αον	~									
meaning boundary.		*									
	7419	*									
	HDX MOS	Services Classes	Sites Virtual Paths	Paths WAN Links	MPLS Queues	Ethernet GRE IPse	Events				
Applications	HDX MOS	Services Classes	Sites Virtual Paths	Paths WAN Links	MPLS Queues	Ethernet GRE IPse	Events				
	HDX MOS	Services Classes	Sites Virtual Paths	Paths WAN Links	MPLS Queues	Ethernet GRE IPse	Events			C	ri ÷ ®
Applications	HDX MOS	Services Classes	Sites Virtual Paths	Paths WAN Links	MPLS Queues	Ethernet GRE IPse	Events			e 1	ri ∸ ®
Applications Show Bandwidth/ 10 v / page	HDX MOS	Services Classes		Paths WAN Links Worst State	MPLS Queues		Events	RX Band	width 🛃	Errors Z	
Applications Show Bandwidth/ 10 v / page	HDX MOS V/Data in Kbps. ge Sho	Services Classes KB V Filters: + owing 1 - 8 of 8			MPLS Queues	Search	21.49 🗹		width 🔁 18.71 [Errors 🖃	r ± €
Applications Show Bandwidth/ 10 v / page	HDX MOS V/Data in Kbps. ge Sho	Services Classes KB V Filters: + owing 1 - 8 of 8	пе	Worst State	MPLS Queues	Search				Errors 🗗	4
Applications Show Bandwidthv 10 v / page bef-Site1-SC bef-Site1-SC	HDX MOS V/Data in Kbps. ge Sho	Services Classes KB V Filters: + owing 1 - 8 of 8	ne 2	Worst State UP	MPLS Queues	Search	21.49		18.71	Errors 2	0 2
Applications Show Bandwidth/ 10 v / page ef-Site1-SC ef-Site1-SC ICN-NY	HDX MOS V/Data in Kbps. ge Sho	KB V Filters: +	ne 2	Worst State UP UP	MPLS Queues	Search	21.49 🖻 0.00 🖻	I	18.71	Errors 2	0 🖂
Applications Show Bandwidth/ 10 v / page	HDX MOS V/Data in Kbps. ge Sho	Services Classes KB S Filters: + owing 1 - 8 of 8 Nat 1/2	ne 2	Worst State UP UP UP	MPLS Queues	Search	21.49 ਦ 0.00 ਦ 58.33 ਦ		18.71 (0.00 (68.45 (Errors 2 2 2 2	0 2 0 2 0 2
Applications Show Bandwidth/ 10 v / page Per-Site1-SC Per-Site1-SC KCN-NY KCN-NY	HDX MOS V/Data in Kbps. ge Sho	Services Classes KB S Filters: + owing 1 - 8 of 8 Nat 1/2	ne 2 2 1	Worst State UP UP UP UP	MPLS Queues	Search	21.49 ਵ 0.00 ਵ 58.33 ਵ 0.13 ਵ		18.71 0.00 68.45 0.00	Errors 2 2 2 2 2 2 2 2 2 2 2 2 2	
Applications Show Bandwidth/ 10 v / page ef-Site1-SC tef-Site1-SC tcN-NY tcN-NY 1-RCN-MUM	HDX MOS V/Data in Kbps. ge Sho	Services Classes KB S Filters: + owing 1 - 8 of 8 Nat 1/2	ne 2 2 1	Worst State UP UP UP UP UP	MPLS Queues	Search	21.49 = 0.00 = 58.33 = 0.13 = 42.21 =		18.71 0.00 0 68.45 0 0.00 0 45.26 0	Errors 2	
Applications Show Bandwidthy 10 v / page ef-Site1-SC ef-Site1-SC ICN-NY ICN-NY I-RCN-MUM 1-RCN-MUM	HDX MOS V/Data in Kbps. ge Sho	Services Classes KB S Filters: + owing 1 - 8 of 8 Nat 1/2	ne 2 2 1 2 2 1	Worst State UP UP UP UP UP	MPLS Queues	Search	21.49 2 0.00 2 58.33 2 0.13 2 42.21 2 0.00 2		18.71 (0.00 (68.45 (0.00 (45.26 (0.13 (Errors 2	

You can view the following metrics:

- Name: Name of the Ethernet interface.
- Worst State: Worst state observed during the selected time period.
- **TX Bandwidth**: Bandwidth transmitted.
- **RX Bandwidth**: Bandwidth received.
- **TX Packets**: Number of packets transmitted.
- **RX Packets**: Number of packets received.
- Errors: Number of errors observed during the selected time period.
- Data Coverage: Percentage of the selected time period for which data is available.

Note

Click the settings icon to select the metrics that you want to view.

Event report

March 12, 2021

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

For more information about events, see Events.

To view event statistics:

In Citrix SD-WAN Center, navigate to **Reports** > **Events**, and in the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.

Dashboard	Fault	Monit	oring	Configuration	R	Reporting	Administ	ration M	litro API					
Reportin	n													
gion: Default_R	-													
sion. Delaul														
ew View Open	Save Sa	ve As												
Time:	September 25	i, 2018 3:15pm	🗄 Last:	Hour / Day / Wee	k / Mont	h						Node: Relative (1 month	ago - 3 seconds ago) 🗸	C
<	28. Aug	30. Aug	1. Sep	3. Sep	5. Sep	the last month 7. Sep	9. Sep	11. Sep	13. Sep	15. Sep	17. Sep	19. Sep 21. Sep	23. Sep 25. Se	ep
	0	0	1											
	28. Aug	30. Aug	1. Sep	3. Sep	5. Sep	7. Sep	9. Sep	11. Sep	13. Sep	15. Sep	17. Sep	19. Sep 21. Sep	23. Sep 25. Se	ep
												▲ 100 CC ► >>	Interval: 1 minute	~
outing Domain:	Any	~												
Applications	HDX MOS	Services	Classes Si	ites Virtual Paths	Paths	WAN Links	MPLS Queues	Ethernet GR	IPsec E	vents				
how Bandwidth	/Data in Kbps	KB 🗸 Filt	ers: +											9 ci ż 6
10 ~ / page	e Sho	owing 1 - 4 of 4						Search						
Site 🖌		Debug Ev	ents	Info Events	N	otice Events	Warn	Ing Events	Error Eve	nts	Alert Events	Critical Events	Emergency Event	ts ·
Def-Site1-SC			0	0		7	9 🖬	15 [3	1 🖬	6 💽	3	0	0 💿
MCN-NY			0	3	Ð	22	4 🖬	77 [3	11 🖬	25	1	0 🗊	0
			0	0		149	1 🖬	350 [3	0	26 🖪		74 🖬	0 -
R1-RCN-MUM						7	9 🖬	14 🖸	7	2 🖬	9 🖬	7	0	0
R1-RCN-MUM			0	0		,	× 🖬		-	- 0	- 6			< 1 >>>

You can view the following metrics:

- **Info Events**: Number of information events that occurred during the selected time period. These are low-level events.
- **Notice Events**: Number of notice events that occurred during the selected time period. These are events that the administrator should know about.
- **Warning Events**: Number of warning events that occurred during the selected time period. These are events that require action in the near future.
- **Error Events**: Number of error events that occurred during the selected time period. These are events that indicate some type of error.
- Alert Events: Number of alert events that occurred during the selected time period. These are events that might require action.
- **Critical Events**: Number of critical events that occurred during the selected time period. These are events that indicate an imminent crisis.
- **Emergency Events**: Number of emergency events that occurred during the selected time period. These are events that indicate an immediate crisis (for example, power supply failure, fan

failure, hard disk threshold exceeded, service disabled).

• **Debug Events**: Number of debugging events that occurred during the selected time period. Debug events are generated when Test Email or Test Syslog options are used on the Citrix SD-WAN appliances.

Note

Click the settings icon to select the metrics that you want to view.

The following table lists a few examples of the state changes of objects for which events are reported.

Event	Object Type	Previous State	Current State
NOTICE	LAN to WAN path	BAD	GOOD
		GOOD	BAD
	WAN to LAN path	BAD	GOOD
		GOOD	BAD
	Dynamic virtual path	BAD	GOOD
		GOOD	BAD
WARNING	Virtual path	GOOD	BAD
	WAN link congestion	UNCONGESTED	CONGESTED
		CONGESTED	UNCONGESTED
	Usage congestion	UNCONGESTED	CONGESTED
		CONGESTED	UNCONGESTED
	LAN to WAN path	GOOD	DEAD
		BAD	DEAD
	WAN to LAN path	GOOD	DEAD
		BAD	DEAD
ALERT	Virtual path	BAD	DEAD
		DEAD	BAD
ERROR	WAN-link	GOOD	DEAD
	Ethernet	GOOD	UNDEFINED
		UNDEFINED	DEAD
INFO	Proxy-arp	UNDEFINED	ACTIVE
		UNDEFINED	STANDBY

You can configure Citrix SD-WAN Center to send external event notifications for different event types as email, SNMP traps or syslog messages. For more information, see Event notifications.

GRE tunnel report

March 12, 2021

You can use a tunneling mechanism to transport packets of one protocol within another protocol. The protocol that carries the other protocol is called the transport protocol, and the carried protocol is called the passenger protocol. Generic Routing Encapsulation (GRE) is a tunneling mechanism that uses IP as the transport protocol and can carry many different passenger protocols.

The tunnel source address and destination address are used to identify the two endpoints of the virtual point-to-point links in the tunnel.

For more information about configuring GRE tunnels on Citrix SD-WAN appliances, see GRE Tunnel.

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

To view GRE tunnel statistics:

In Citrix SD-WAN Center, navigating to **Reporting** > **GRE**, and in the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.

ashboard	Fault	Monitoring	Configuration	Reporting	Administration	Nitro API								
eportir	ng													
in: Default_R	Region 🔻 🕐													
w View Oper	n., Save Sav	e As												
Time:	October 4, 2018	3 1:49pm	Last: Hour / Day / Wee	k / Month							Mode:	Relative (23 seconds from now)	• ©	
<	6. Sep	8. Sep	10. Sep	12. Sep	14. Sep 16. Se	p 18. Sep	20. Sep	22. Sep	24. Sep	26. Sep 28. Se	p 30	. Sep 2. Oct	4. Oct	
	6. Sep	8. Sep	10. Sep	12. Sep	14. Sep 16. Se	p 18. Sep	20. Sep	22. Sep	24. Sep	26. Sep 28. Se		Sep 2. Oct	4. Oct	
												KK KK 🕨 🔅 🔅	1 minute V	
uting Domain:	Any	•												
pplications	HDX MOS	Senices Classes	Sites Virtual Paths	Paths WAN Links	MPLS Queues Etherne	t GRE IPsec Events								
now Bandwidth	h/Data in Kbps/K	B 🔻 Filters: +											. Č	i - 6
10 🔻 / pag	ge Sho	ving 1 - 1 of 1				Search								
Site 🔺		Name		Worst State	MTU	TX Bandwidth 🛃		RX Bandwidth 🛃		Packets Dropped 🖻		Packets Fragment	ted 🖻	
N_VPX	Appllar	nce-Tunnel-1		DOWN	1476		0.04 🛃		0.00 🖻		0 🖻			0 🖻
a from 10/04/1	18 1:45pm to 10/0-	4/18 1:49pm (Asla/Calcu	itta Time)											

You can view the following metrics:

- Worst State: Worst state observed during the selected time period.
- **MTU**: Maximum transmission unit the size of the largest IP datagram that can be transferred through a specific link.

- **TX Bandwidth**: Bandwidth transmitted.
- **RX Bandwidth**: Bandwidth received.
- **TX Packets**: Number of packets transmitted.
- **RX Packets**: Number of packets received.
- Packets Dropped: Number of packets dropped, because of network congestion.
- **Packets Fragmented**: Number of packets fragmented. Packets are fragmented to create smaller packets that can pass through a link with an MTU that is smaller than the original datagram. The fragments are reassembled by the receiving host.
- Data Coverage: Percentage of the selected time period for which data is available.

Note

Click the settings icon to select the metrics that you want to view.

HDX report

March 12, 2021

Select one of the following report types from the drop-down list:

- HDX Site Stats
- HDX Summary (applicable for both HDX information channel available and unavailable sessions)
- HDX User Sessions (applicable for only HDX information channel available sessions only)
- HDX Apps (applicable for only HDX information channel available sessions only)

HDX site statistics

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

Summary view

The Summary view shows the following data for a site:

- **QoE Index** The Quality of Experience (QoE) is a numeric value between 0–100. The higher the value the better the user experience.
- **Users** The number of active users on the site.
- **TCP Flows** The number of active HDX sessions on the site that use the TCP protocol.
- **UDP Flows** The number of active HDX sessions on the site that use UDP protocols.

• **Sessions** – The total number of active HDX sessions on the site that includes both Small-Scale Integration (SSI) and Medium-Scale Integration (MSI) sessions.

Detail view

You can click an individual site to view details about all the variables affecting QoE. Each pair of row shows the QoE factors for data calculated at local and remote sides for a given virtual path.

Latency, jitter, and packet drop variables affecting QoE are the effective numbers that the Citrix SD-WAN appliance is measuring. For example, there might be larger percent of packet drop in the network, since Citrix SD-WAN corrects the packet drops through its own protocol, the effective packet loss seen by the application would be much lesser, hence improves the QoE for HDX applications.

Similarly, latency improvement through packet duplication also improves the QoE for HDX applications. In other words, Citrix SD-WAN improves the QoE for HDX traffic by improving the factors affecting the QoE. For more information see, HDX QoE.

To view HDX Reports:

In the Citrix SD-WAN Center, navigate to **Reporting** > **HDX**, and in the timeline control select a period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save, and open report views. For more information, see, Manage views.

ashboard	J	Fault	M	Ionito	ring	Confi	guratio	п кер	orting	Adn	ninistration	Nitro	D APT							
porting																				
ion: Defa	ult_Region	• 7																		
ew View	Open	Save	Save As																	
1	Time: Ma	ıy 15, 2019	11:59pm		📋 Las	t: Hour /	Day / W	Veek / Month							Mode:	Relative (1 v	veek ago - 1 v	veek ago)	: ©	
<	26.	Apr	28. Apr	3	30. Apr	2. May	4.1	May 6. Ma	iy -	8. May	10. May	12. May	14. May	16. Ma	y 1	8. May	20. May	22. May	24. May	
,	15. May	2:00an	1	4:00	am	6:00am		8:00am	10:00am	12	:00pm	2:00pm	4:00pm	1	6:00pm		:00pm	10:00pm		
outing Dor	main: An	у		¢													▶ >> >>i	, and rear	1 minute 🗘	
Application	ns HD	App (QOE N	IOS	Services	Classes	Sites	Virtual Paths	Paths	WAN Links	MPLS Queu	es Etherne	t GRE	IPsec	Events					
port Type	e : HDX Sit	e Stats	•																	
		in Kbps		Filters	: +															1 - 0
10 \$/p	page	Sh	owing 1 -	1 of 1							Search									
Si	ite			Qo	E Index 🗸			Users			TCP Flows			UD	P Flows			Sess	ons	
									1				D				4			1

HDX summary

Select the **HDX Summary** report and the site from the drop-down list. The HDX summary report displays each user's report that has logged in during the selected time period.

Applications	HDX App QoE	MOS	Services	Classes	Sites	Virtual Paths	Paths	WAN Links	MPLS Queues	Ethernet	GRE	IPsec	Events					
Report Type H			lect Site : DC														Hů	±®
10 ¢ / page	Showing	1 - 3 of 3	3					Se	arch									
User	Client IP		SSI sest	ions		MSI sessions		Bytes F	rom Client 🗸		Bytes I	From Serv	rer		HDX Channel A	Availability		\$
	192.168.1.60				0		2		148,81	5.00			623,237.0	0 No				
and a day	192.168.1.66				4		4		54,54	3.00			290,657.0	0 Yes				
ravindra																		
ravindra	192.168.1.60				2		0		2,00	5.00			7,449.0	0 Yes				

In the HDX summary report, you can view the following parameters:

- **User**: Name of the user.
- Client IP: Client IP address.
- **SSI sessions**: Number of active Single Stream ICA (SSI) sessions.
- MSI sessions: Number of active Multi Stream ICA (MSI) sessions.
- Bytes from Client: Size in bytes from client.
- Bytes from Server: Size in bytes from server.
- **HDX Channel Availability**: Provides the HDX information channel availability status as **Yes/No**. If the channel is not available, then the user name shows as a hyphen (-).

HDX user sessions

In the HDX user sessions report, you can see every sessions detail used by each user. Select the site, user, and SSI or MSI from the drop-down list. By default, the **Select User** and **Select SSI/MSI** fields shows **ALL**.

Applications HDX App QoE	MOS Service	es Classes	Sites	Virtual Paths	Paths	WAN Links MPLS	Queues Eth	ernet GRE	IPsec	Eve	ents			
Report Type HDX User Sessions	Select Site :	DC	•	Select Use	d all	•	elect SSI/MSI : A	ม	÷					
Show Bandwidth/Data in Kbps/KB \$	Filters: +												≝₫≛	•
10 ¢ / page Showing 1	- 10 of 10					Se	arch							
Session Key	Client IP	Server IP	Session Type	ssi / Msi	Server Name	Server Version	ICA RTT (ms)	WAN Latency (ms) /	\CR	Bytes From Client 🗸	Bytes From Server	Connection State	Packe
61C2934DC106462CB387A787E6E7D850	192.168.1.66	192.168.2.7	APP	MSI	VDA4	7.18.0.16	32		12	0	19,159.00	173,440.00	0	
46B5B8A583AC42BB8F3864C7FFACA990	192.168.1.66	192.168.2.7	DESKTOP	MSI	VDA4	7.18.0.16	28		12	0	11,704.00	17,853.00	0	
741F64DD06ED4EC696D4A0CE4282C975	192.168.1.66	192.168.2.7	APP	SSI	VDA4	7.18.0.16	44		12	0	9,521.00	38,233.00	0	
46B5B8A583AC42BB8F3864C7FFACA990	192.168.1.66	192.168.2.7	DESKTOP	SSI	VDA4	7.18.0.16	96		12	0	8,585.00	17,508.00	0	
45245CB68D5441A4ADDECF055D6BFD97	192.168.1.66	192.168.2.6	APP	MSI	VDA3	7.18.0.16	NA		11	0	1,792.00	13,067.00	0	
90BCDF10354146D9A23E298453997F58	192.168.1.66	192.168.2.6	APP	SSI	VDA3	7.18.0.16	NA		12	0	1,740.00	19,030.00	0	
46B5B8A583AC42BB8F3864C7FFACA990	192.168.1.60	192.168.2.7	DESKTOP	SSI	VDA4	7.18.0.16	36		12	0	1,460.00	4,162.00	0	
1ED256B0619843CDB1E187E1271FC21C	192.168.1.66	192.168.2.6	DESKTOP	MSI	VDA3	7.18.0.16	31		11	0	1,311.00	7,597.00	0	
1ED256B0619843CDB1E187E1271FC21C	192.168.1.66	192.168.2.6	DESKTOP	SSI	VDA3	7.18.0.16	27		12	0	736.00	3,929.00	0	
1ED256B0619843CDB1E187E1271FC21C	192.168.1.60	192.168.2.6	DESKTOP	SSI	VDA3	7.18.0.16	21		12	0	546.00	3,287.00	0	
Data from 05/15/19 12:00am to 05/16/19 1	2:00am (Asia/C	alcutta Time)											$1 \rightarrow$	

You can use the **Search** or **Filter:+** options to find out the required session information as per your requirement.

- Session Key: The session key represents the unique identity for an ICA session.
- Client IP: Client IP address for each session.
- Server IP: Server IP address for each session.
- Session Type: Type of the sessions (Desktop, App).
- **SSI/MSI**: Shows whether it is an SSI or MSI session.
- Server Name: Shows the name of the server.
- Server Version: Shows the version of the server.
- **ICA RTT (ms)**: Shows the ICA Round Trip Time (RTT) in milliseconds. This is an end-to-end round trip time between the client and the server.
- **WAN Latency**: Latency over the WAN, that is between the two SD-WANs over the virtual path. This latency doesn't include client-side or server-side network latency.
- ACR: Shows the auto client reconnect counts.
- Bytes from Client: Size in bytes from client.
- Bytes from Server: Size in bytes from server.
- Connection State: Hover the mouse to see the connection state.
 - For MSI, there are four connections. These connections are L4 level (TCP/UDP state).
 - For SSI, there is only one connection.



- Packet from Client: Number of packets from client.
- Packet from Server: Number of packets from server.

HDX apps

You can see all the application used by a specific user or by all users. Select the **Site** and the **User** to view the applications details.

Applications HDX	App QoE MOS Services Classe	s Sites Virtual F	Paths Paths	WAN Links	MPLS Queues	Ethernet	GRE	IPsec	Events					
Report Type : HDX Apps Show Bandwidth/Data in	Select Site : DC Kbps/KB Filters: +	✓ Selet	t User: All		·							P	1 ch 📥	•
10 \$ / page	Showing 1 - 10 of 28				Search									
Application Name	Session Key		SSI / MSI	Applica	tion Launch Time	~	Appli	cation Te	rmination '	lime	A	pplication Duration (mir	1)	¢
Task Manager	3D2883E8A3FA4F3E93E783A4AD51676	E	MSI	2019-05-16 1	8:14:36	20	019-05-16	18:28:42					14.10	
fask Manager	0B4CF553E68B43959AB3C9D71742100	A	MSI	2019-05-16 0	8:40:20	A	ctive						15570.25	
Calculator	0E3ED486534A44B58C98FFA507A9429	:	MSI	2019-05-16 0	8:17:16	20	019-05-16	08:30:52					13.60	
ask Manager	4841A0F5453246DD956D48BF473CCB	:4	MSI	2019-05-16 0	8:09:58	20	019-05-16	08:14:58					5.00	
Calculator	C1148C7D68F2439F83E8D5F3F0855EE	3	MSI	2019-05-16 0	6:16:48	20	019-05-16	06:26:26					9.63	
ask Manager	7F643C228C184BC9BF3D5C89B9D61A	7	MSI	2019-05-16 0	4:41:01	20	019-05-16	05:01:07					20.10	
Paint	90BCDF10354146D9A23E298453997F5	В	SSI	2019-05-15 1	5:53:06	20	019-05-15	15:56:52					3.77	
Administrative Tool	741F64DD06ED4EC696D4A0CE4282C9	5	SSI	2019-05-15 1	5:52:55	20	019-05-15	15:52:56					0.02	
ask Manager	741F64DD06ED4EC696D4A0CE4282C9	75	SSI	2019-05-15 1	5:52:39	20	019-05-15	15:56:36					3.95	
Paint	45245CB68D5441A4ADDECF055D6BFD	97	MSI	2019-05-15 1	5:40:35	20	019-05-15	15:43:41					3.10	
Data from 04/27/19 9:40am	n to 05/27/19 9:40am (Asia/Calcutta Time)											< 1 2 3	> >	ж

- Application Name: Provides the name of the HDX application.
- Session Key: Provides the unique session key which is used for that particular application.
- SSI/MSI: Shows whether it is an SSI or MSI session.
- Application Launch Time: Provides the application launch time with date.
- **Application Termination Time**: Provides the application termination time with date. If an application is active, it shows active instead of the termination time.
- Application Duration (min): Provides the application time duration in minutes.

Note

- If there is any unintended error such as, if the HDX session information is unavailable on the appliance, then the HDX user-based reports are not shown even if the **HDX User Reporting** is enabled. Some of the fields such as user name, server name, server version, ICA RTT in the reports might be shown as **NA**.
- Application termination time in HDX Apps report is shown only if SD-WAN receives Application Termination Time from Xen Application/Xen Desktop Server. Otherwise, some of the applications are reported to be active even if closed.

IPsec tunnel report

March 12, 2021

IP Security (IPsec) protocols provide security services such as encrypting sensitive data, authentication, protection against replay, and data confidentiality for IP packets. Encapsulating Security Payload (ESP), and Authentication Header (AH) are the two IPsec security protocols used to provide these security services. In IPsec tunnel mode, the entire original IP packet is protected by IPsec. The original IP packet is wrapped and encrypted, and a new IP header is added before transmitting the packet through the VPN tunnel.

For more information about configuring IPsec tunnels on Citrix SD-WAN appliances, see IPsec Tunnel Termination.

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

To view IPsec tunnel statistics:

In Citrix SD-WAN Center, navigate to **Reporting** > **IPsec Tunnels**, and in the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save, and open report views. For more information, see, Manage views.

ashboard	Fault	Monitorin	g Config	uration	eporting	Administr	ation 1	Nitro API						
eportin	n													
tion: Default_Re	-													
jon: Detaut, He	igion : (f)													
ew View Oper	Save	Save As												
Time:	September 12	2, 2018 3:44pm	Last Hour / I	Day / Week / Morr	h				Mode:	Relative (1 mor	th ago - 2 second	s ago) d	C	
<	16. Aug	18. Aug	20. Aug 22.	Aug 24. Aug	26. Aug	28. Aug	30. Aug 1	Sep 3	I. Sep 5. Sep	7.Sep	9.54p	11. Sep		
					.									
14. Auj	; 16. Aug	18. Aug	20. Aug 22.	Aug 24. Aug	26. Aug	28. Aug	30. Aug 1	.Sep 3	1. Sep 5. Sep	7. Sep	9.5ep	11. Sep	_	
									A	100 400	30 304 linter	val: 1 minute	•	
louting Domain:	Any	0												
Applications	HDX MOS	Services Clas	ses Sites Vir	tual Paths Paths	WAN Links	MPLS Queues	Ethernet GR	E IPsec	Events					
how Bandwidth/	Data in Kops	NB 1 Fiters: +											108	8
10 \$ / page	9	owing 1 - 1 of 1				Search								
Name /		Char.	P /			IPsec Tunnel V	Kinese France 73	MTU	TX Bandwidth P		indwidth 🗐	Data Dropp		
w_intranet_Servi		Site R1-CB1000 In	Service Type tranet	Intranet Service	Type		e E	MIU		0 2	0.00 🖂		0.00 E	4
									-					× .

You can view the following metrics:

- Name: Application name.
- Site: Name of the site.
- Service Type: Type of the service.
- **Intranet Service Type**: Type of intranet service associated with the IPsec tunnel. The following are the type of intranet services:
 - Default
 - Microsoft Azure Virtual WAN

- Zscaler
- Citrix SaaS Gateway
- **IPsec Worst State**: Worst state observed during the selected time period.
- **MTU**: Maximum transmission unit—size of the largest IP datagram that can be transferred through a specific link.
- **TX Bandwidth**: Bandwidth transmitted.
- **RX Bandwidth**: Bandwidth received.
- **TX Packets**: Number of packets transmitted.
- **RX Packets**: Number of packets received.
- Data Dropped: Data dropped, in Kbps.
- Packets Dropped: Number of packets dropped.

Note

Click the settings icon to select the metrics that you want to view.

Link performance report

March 12, 2021

Citrix SD-WAN Center can show performance statistics at the site, service, virtual path, or WAN-link level.

Consider a network in which organization ABC has four branch offices. Brownouts have been reported at SITE3. That is, the employees are sometimes unable to view the intranet pages. You suspect that it's because of the performance of the underlying links.

You can get a high-level view of the link statistics by hovering your mouse cursor over the path between a site and the data center on the Network Map on the Dashboard.

Network Map								
Configuration: Istest-m	cn 🗸							
Routing Domain: Any	v							
• डायट	SITE3-SHIE4						Site Filter	•
SITE2 Master-S SITE2-SITE7 S	Master-WL-2->SITE3-WL-2	4 PM to 11/	eState Reaso SILENCE	0.00	D	ter Loss		
Mast	ei SITE3-WL-2->Master-WL-2 Master-WL-1 >SITE3-WL-1 SITE3-WL-1 >Master-WL-1	BAD BAD	SILENCE LOSS LOSS	0.00 15.91 12.78	0 11 11	8 10.1% 6 9.8%		
SITE7								

The above screen shot shows that there are two WAN links (WL-1 and WL-2) between SITE 3 and the Master Controller Node (MCN), and displays statistics for the most recent 10 minutes.

The virtual paths Master-WL2->SITE3-WL2 and SITE3-WL2 ->Master-WL2 are not functioning, and alternative paths Master-WL1->SITE3-WL1 and SITE3-WL1 ->Master-WL1 are in poor condition, losing a significant percentage of the transmitted data. That is the probable cause of the brown-out issue at SITE3.

Alternatively, you can view the link statistics by navigating to **Reporting** >**Paths**.

In the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.

Dashbo	ard	Fault		Monitorin	g Con	figuration	Reporting	Administration	Nitro API							
Repo	orti	ng														
		Region 🗸 🤇)													
New View	Ope	en Save	Save As	5												
	Time	e: October 4,	2018 10	:01am	Last: Hour	/ Day / Week / I	Month						Mode: Relative (1 seco	ond ago)	~ C	
	<	6. Sep		8. Sep	10. Sep	12. Sep	14. Sep	16. Sep 18. Sep	20. Sep	22. Sep	24. Sep	26. Sep	28. Sep 30. Sep	9 2. Oct	4. Oct	
		6. Sep		8. Sep	10. Sep	12. Sep	14. Sep	16. Sep 18. Sep	20. Sep	22. Sep	24. Sep	26. Sep	28. Sep 30. Sep	9 2. Oct	4. Oct	
													▲ w w >	>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	minute 🗸	
Routing	Domair	n: Any		~												
Applica	ations	HDX M	DS S	ervices Clas	sses Sites	Virtual Paths Pa	aths WAN Links	MPLS Queues Ethern	et GRE IPsec	Events						
		h/Data in Kt		_	+										묘법	÷ ®
10	✔ / pag	ze	Showing	g 1 - 9 of 9					arch							
Name 🔨	Site	From WAN Link	Site	To WAN Link	Worst State 🖂	Bandwidth 🖂 Co	ntrol Bandwidth 🖂	LAN to WAN	nteractive Bandwidth	며 Bulk Bandwidth	Congestion I	에 Worst State F	Bandwidth 🖂 BOWT	WAN to LAN	ms) Loss (%)	000 FR
Def- Site1-	Def- Site1-	Def-Site1- SC-WL-1		MCN-NY- WL-1	600D 🖂	17.80 🖬	17.80 🛃		0.00	1		GDOD 🛃	13.41 🖬	2 🖂		0 🖻
MCN- NY-WL-	MCN- NY	MCN-NY- WL-1	Def- Site1- SC	Def-Site1- SC-WL-1	GOOD 🛃	13.18 🖻	13.18 🖬	0.00 🖬	0.00	0.00	NO 🖬	G00D 🛃	17.60 🖃	2 🖻	2. 0.0	0 🖂
MCN- NY-WL- 1->R1- RCN- MUM- WL-1	MCN- NY	MCN-NY- WL-1	R1- RCN- MUM	R1-RCN- MUM-WL-1	GOOD 🛃	13.58 🖬	13.58 🖬	0.00 🖬	0.00	☑ 0.00	NO 🛃	GOOD 🛃	18.79 🖬	2 🖬	2 0.0	₀ ₪
MCN-	MCN- NY	MCN-NY- WL-1	R2- RCN- SA	R2-RCN-SA- WL-1	GOOD 🛃	13.50 🛃	13.50 🖬	0.00 🖻	0.00	☑ 0.00	NO 🖻	GOOD 🛃	18.73 🖬	2 🖬	2 0.0	0 🖻
R1-RCN- MUM- WL- 1->MCN- NY-WL-1	R1- RCN- MUM	R1-RCN- MUM-WL-1	MCN- NY	MCN-NY- WL-1	GOOD 🛃	18.89 🖬	18.89 🖬	0.00 🖬	0.00	0.00	NO 🖬	GOOD 🛃	13.75 🖃	2 🖬	2 0.0	0 🖬
R1-RCN- MUM- WL- 1->R1- Site1- BLR- WL-1	R1- RCN- MUM	R1-RCN- MUM-WL-1	R1- Site1- BLR	R1-Site1- BLR-WL-1	GOOD 🛃	13.49 🖬	13.49 🛃	0.00 🖬	0.00	■ 0.00	NO 🛃	GOOD 🛃	22.59 🖬	2 🖾	2 0.0	0 🗹
R1-RCN- MUM- WL- 1->R1- Site3- Del- WL-1	R1- RCN- MUM	R1-RCN- MUM-WL-1	R1- Site3- Del	R1-Site3-Del- WL-1	DEAD 📑	1.15 🖻	1.15 🖻	0.00	0.00	■ 0.00	UNKNOWN	DEAD 📑	0.00 🖂	0 🖂		
	R2- RCN- SA	R2·RCN·SA· WL·1	MCN- NY	MCN-NY- WL-1	GOOD 🖂	18.56 🖬	18.56 🖬	0.00 🖬	0.00	0.00	NO 🖬	good 🛃	13.36 🖬	2 🖬	2 0.0	0 🗹
R2-RCN- SA-WL- 1->R2- Site1-JB- WL-1	R2- RCN- SA	R2·RCN·SA· WL·1	R2- Site1- JB	R2-Site1-JB- WL-1	DEAD 📑	1.15 🖬	1.15 🖬	0.00 🖬	0.00	0.00		DEAD 📑	0.00 🖬	0 🖂		

You can view the following metrics:

- Name: The path name.
- From (Site and WAN Link): The source site and WAN link.
- To (Site and WAN Link): The destination site and WAN link.
- LAN to WAN
 - Work State:
 - **Bandwidth**: Total bandwidth consumed by all packet types. Bandwidth= Control Bandwidth + Real-time Bandwidth + Interactive Bandwidth + Bulk Bandwidth.
 - **Control Bandwidth**: Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.

- Real-time Bandwidth: Bandwidth consumed by applications that belong to the real-time class type in the SD-WAN configuration. The performance of such applications depends on a great extent upon network latency. A delayed packet is worse than a lost packet (for example, VoIP, Skype for Business).
- Interactive Bandwidth: Bandwidth consumed by applications that belong to the interactive class type in the SD-WAN configuration. The performance of such applications depends on a great extent upon network latency, and packet loss (for example, XenDesktop, XenApp).
- Bulk Bandwidth: Bandwidth consumed by applications that belong to the bulk class type in the SD-WAN configuration. These applications involve very little human intervention and are mostly handled by the systems themselves (for example, FTP, backup operations).
- **Congestion**: Congestion due to increased traffic or unexpected delay in packet flow in the WAN.
- WAN to LAN:
 - Worst State: The worst WAN to LAN state observed during the time period.
 - Bandwidth:
 - **BOWT Latency(ms)**: Best one-way time (BOWT) taken for a packet to move from one point to another, in milliseconds.
 - Jitter (ms): Variation in the delay of received packets, in milliseconds.
 - Loss (%): Percentage of packets lost.
 - **OOO (%)**: Percentage of packets that are not in the right order or out of order (OOO).
 - **Congestion**: Congestion due to increased traffic or unexpected delay in packet flow in the WAN.

Click on **Settings** icon and select the parameters that you wants to view on reports.

MOS for applications

March 12, 2021

The mean opinion score (MOS) provides a numerical measure of the quality of the experience that an application delivers to end users. It is primarily used for VoIP applications. In Citrix SD-WAN, MOS is also used to assess the quality of non-VoIP applications by judging the traffic as if it were a VoIP call.

Citrix SD-WAN Center calculates and displays MOS for the traffic that passes through the virtual path. Enable the **Estimate MOS** option for each application on every Citrix SD-WAN appliance to display the MOS scores of these applications in Citrix SD-WAN Center.

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

Note

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

To view MOS for applications:

In Citrix SD-WAN Center, navigating to **Reporting** > **Applications**, and in the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.

nortin	0																	
eportin	ig																	
in: Default_Re	egion 🔻 🖓																	
v View Open.		C																
v View Open.	Save	Save As																
Time:	October 3, 2	018 3:38pm	🛗 La	st: Hour ,	/ Day / Week	A Month							Mode:	Relative (2 m	inutes from now)	٣	C	
4 . Sep	6. S	ep 8.	Sep	10. Sep	12. Sep	14.	Sep 16.	Sep 18	3. Sep	20. Sep	22. Sep	24. Sep	26. Sep	28. Sep	30. Sep	2. Oct		
				10.0	12. Sep	14.1	Sep 16. !	Son 19	8. Sep	20. Sep	22. Sep	24. Sep	26. Sep	28. Sep	30. Sep	2. Oct		
4. Sep	6. S	ep 8.	Sep	10. Sep	12. Sep		p	Seb 10	s. sep	Lo. Jep	aa. sep		Lo. Jup	au. sep	So. Sep	2.00		
			Sep	10. Sep	12. sep			Jep 10	s. sep	20. Jep	ALL JUP		A			val: 1 minute	¥	
uting Domain:		•			12. sep Virtual Paths			IPLS Queues	Ethernet		Psec Events						•	
uting Domain:	Any HDX MO	s Services	Classes															
uting Domain:	Any HDX MO	s Services															•	÷
uting Domain:	Any HDX MO Data in Kbp	s Services	Classes						Ethernet									÷.
uting Domain:	Any HDX MO: Data in Kbp	s Services	Classes Iters: + 2					IPLS Queues	Ethernet	GRE I				ж «		val: 1 minute		÷ 4
uting Domain: upplications ow Bandwidth/I 10 V page	Any HDX MO: Data in Kbp	s Services	Classes Iters: + 2 Virtua	Sites			WAN Links M	IPLS Queues	Ethernet	GRE I	Psec Events			ж «	>> >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	val: 1 minute		÷ 6

You can view the following metrics:

- Name: Name of the application.
- Average Virtual WAN MOS: Average quality score calculated over the selected time period.
- Lowest Virtual WAN MOS: Lowest quality score calculated within the selected time period.

The scores are graded as follows:

- 5 Users are very satisfied.
- 4 Users are satisfied.
- 3 Users are dissatisfied.
- 2 Users are very dissatisfied.
- 1 –Not recommended.

MPLS queues report

March 12, 2021

MPLS Queues provide service queues controlled by standard Differentiated Services Code Point (DSCP) tags. The tags control the quality of service between two sites on the Virtual WAN.

MPLS Queues allow MPLS providers to identify traffic on the basis of DSCP markings, so that class of service can be applied by the provider.

For more information about configuring private MPLS WAN links on Citrix SD-WAN appliances, see MPLS Queues.

To view MPLS queue statistics:

In Citrix SD-WAN Center, navigate to **Reports** > **MPLS Queues**, and in the timeline control select a time period.

You can select and view reports of a particular time frame by using the timeline controls. For more information, see, Timeline controls.

You can also create, save and open report views. For more information, see, Manage views.

						on Rep	orting	Admini												
Repoi	rting																			
Region: Def	fault_Regio	n v 🖓																		
New View	Open	Save	ave As																	0
	Time: 0	ctober 3, 20)18 3:41pm	📰 La	ast: Hour /	Day / Week	/ Month								Mode:	Relative (2 minutes from now)	٣	C	
<	4. Sep	6. Se	ip l	8. Sep	10. Sep	12. Sep	14.	Sep	16. Sep	18. Sep	20. Sep		22. Sep	24. Sep	26. Sep	28. Sep	30. Sep	2. Oct		
	4. Sep	6. Se	0	8. Sep	10. Sep	12. Sep	14	. Sep	16. Sep	18. Sep	20. Sep	1	22. Sep	24. Sep	26. Sep	28. Sep	30. Sep	2. Oct		
															A			1 minute	٣	
Routing Do	omain: A	ny	•																	
				_																
Applicatio	ons HD	X MOS	Services	Classes	Sites \	/irtual Paths	Paths	WAN Links	MPLS Queues	Ethernet	GRE	IPsec	Events							
Show Band	dwidth/Dat	a in Kbp	s/KB ¥	Filters: +															80	÷ ®
10 🔻	/ page	St	nowing 1 - 8 c	if 8					Se	arch										
				_						LAN	to WAN									
Site 🔺	MPLS WA	N Link	Name		Control E	Bandwidth 🛃	Realtime E	Bandwidth 🛃	Interactive Ban	dwidth 🛃 Bu	ılk Bandv	idth 🖂	Mismatch	ed Bandwidth 🛃	Available Bandwi	ith 🖂 Per	mitted Bandwidth 🖂 I	Bandwidth [BOW	T Latency (i
ANZ_RCN	ANZ_RCM	N-WL-2	ANZ_RCN- queue2	40.26		40.26 🛃		0.00 🛃	I	0.00 🖬		0.00 🖬		0.00 🖂	198,00	0.00 🛃	198,000.00 🖂	53.88		
ANZ RCN	ANZ_RCM		ANZ_RCN- queue1	20.06	2	18.91 🖬		0.00 🖂	I	1.15 🖂		0.00 🖂		0.00 🖬	2,670,00	0.00 🛃	2,670,000.00 🖂	14.79	H	

You can view the following metrics:

- MPLS WAN Link: Name of the MPLS WAN link that the MPLS queue is a member of.
- Name: The DSCP tag name.
- **Bandwidth**: Total bandwidth consumed by all packet types. Bandwidth = Control Bandwidth + Realtime Bandwidth + Interactive Bandwidth + Bulk Bandwidth.

- **Control Bandwidth**: Bandwidth used to transfer control packets that contain routing, scheduling, and link statistics information.
- **Realtime Bandwidth**: Bandwidth consumed by applications that belong to the realtime class type in the Citrix SD-WAN configuration. The performance of such applications depends to a great extent upon network latency. A delayed packet is worse than a lost packet (for example-VoIP, Skype for Business).
- **Interactive Bandwidth**: Bandwidth consumed by applications that belong to the interactive class type in the Citrix SD-WAN configuration. The performance of such applications depends to a great extent upon network latency, and packet loss (for example, XenDesktop, XenApp).
- **Bulk Bandwidth**: Bandwidth consumed by applications that belong to the bulk class type in the Citrix SD-WAN configuration. These applications involve very little human intervention and are mostly handled by the systems themselves (for example, FTP, backup operations).
- **Mismatched Bandwidth**: Frames that do not match the defined DSCP tags are mapped to a default queue designated for mismatched bandwidth.
- Available Bandwidth: The sum of bandwidth allocated to all the WAN links of a site.
- **Permitted Bandwidth**: Bandwidth available for transmitting information.
- **BOWT Latency**: Best one-way time taken for a packet to move from one point to another, in milliseconds.
- Jitter: Variation in the delay of received packets, in milliseconds.
- Packets Lost: Number of packets lost.
- Loss: Percentage of packets lost.
- **OOO**: Percentage of packets that are not in the right order.
- Congestion: Congestion due to increased traffic or unexpected delay in packet flow in the WAN.

Note

Click the settings icon to select the metrics that you want to view.

Administration

March 12, 2021

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

Configure date and time

HTTPS certificates

Import MCN configuration

Manage database

Mangae views Software upgrade Timeline controls User accounts

Configure date and time

March 12, 2021

You can change the date and time of the Citrix SD-WAN Center management system either manually or by using an NTP server. If you select the **Use NTP server** option, then you cannot manually enter a current date and time.

To manually set the date and time:

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

Dashboard	Fault	Monitoring Co	onfiguration	Reporting	Administration		
User/Authentication	Settings	Administration /	Global Settings	/ TimeZone			
Global Settings		Management In	iterface	HTTPS Certificate	TimeZone	Software Upgrade	
Database Maintenan Storage Maintenance		Date and Time Time Zone: UTC Date: 09/13/2016	Time: 123 PM	Use NTP server			٢
		Apply					

- 3. In the **Time Zone** field, select a **city** in your current time zone. Alternatively, enter the current date and time for your time zone.
- 4. Click Apply.

You can synchronize the Citrix SD-WAN Center clock with an external NTP server.

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

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

3. Select Use NTP Server.

This disables the Date and Time fields, and displays the NTP Servers table.

Dashboard Fault	Monitoring Configuration	on Reporting	Administration			
User/Authentication Settings	Administration / Global Sett	ings / TimeZone				
Global Settings	Management Interface	HTTPS Certificate	TimeZone	Software Upgrade		
Database Maintenance Storage Maintenance	Date and Time Time Zone: Lybljana Date: 199/12/2016 3:28 P	-		NTP Servers + Address	VerifyDelete	0
	Apply					

- 4. To add a new NTP server, click the + icon next to NTP Server.
- 5. In the Address field, enter the IP Address for the NTP Server.

You can specify up to three NTP servers, but you must specify at least one. These act as backup NTP servers, if one server is down the Citrix SD-WAN Center automatically synchronizes with the other NTP server.

If you specify a domain name for an NTP server, you must also configure a DNS server unless you have already done so. To remove a server entry from the table, click the **Delete** icon in the Delete column of the entry.

- 6. Click **Verify** to verify that the server is reachable, before applying your settings.
- 7. Click Apply.

HTTPS certificates

March 12, 2021

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

View installed HTTPS certificate details

CitrixTo evaluate the current certificate, you can display the certificate details.

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

- 1. In the Citrix SD-WAN Center web interface, click the **Administration** tab.
- 2. Click Global Settings and then click HTTPS Certificate.

The HTTPS certificate details appear in the **Installed HTTPS Certificate** section.

		Monitoring Conf		porting	Administration		
User/Authentication	n Settings	Administration / G	obal Settings / HTTPS C	ertificate			
Global Settings		Management Inter	face HTTPS C	Certificate	TimeZone	Software Upgrade	
Database Maintena	nce						
Storage Maintenano	:e	Installed HTTPS Cer issued to: Country: State/Province: Locality: Organizational Unit Common Name: Email:	US California San Jose Citrix Systems, Inc.	Issuer: Country: State/Provinc Locality: Organization Organization Common Nat Email:	San Jose Citrix Systems, al Unit: Engineering		٢
		Certificate Details: Certificate Fingerpr Start Date: End Date: Serial Number:	Int: 55:58:28:D9:FC:9A:A2 Aug 23 06:39:53 2010 Aug 23 06:39:53 2010 EC60282F6C3E593A	5 GMT	9:70:96:A0:77:43:47:F5		

Upload and install an HTTPS certificate

Installing an HTTPS Certificate puts Citrix SD-WAN Center into Maintenance Mode until the operation is complete. When the operation is complete, the web server is restarted, invalidating all connected sessions. If the connection to the server is lost when the web server is restarted, the maintenance mode screen automatically reloads the previous page and displays a security notice from the browser. If the screen does not reload, click **Continue** to reload the previous page.

To upload and install the HTTPS certificate:

- 1. In the Citrix SD-WAN Center web interface, click the **Administration** tab.
- 2. Click Global Settings and then click HTTPS Certificates.
- 3. In the **HTTPS Certificate upload and Install** section, in the **HTTPS certificate file** field, click **Browse** and select a HTTPS certificate.
- 4. For the field HTTPS private key file, click Browse and select an HTTPS private key file.
- 5. Click Upload and Install.

HTTPS Certificate upload and Install	0
Uploading and installing the certificate and private key that are used to secure the Management HTTPS connection to this SD-WAN Center will cause the HTTP server to resta Invalidating all connected sessions.	rt,
HTTPS certificate file: Browse File Type:.crt	
HTTPS private key file: Browse File Type: .key Upload and Install. Clear	

Regenerate the HTTPS certificate

You can regenerate a self-signed certificate that secures the Management HTTPS connection to Citrix SD-WAN Center. Regenerating the HTTPS Certificate puts Citrix SD-WAN Center into Maintenance Mode until the operation is complete. When the operation is complete, the web server is restarted, invalidating all connected sessions.

If the connection to the server is lost when the web server is restarted, the maintenance mode screen automatically reloads the previous page and displays a security notice from the browser. If the screen does not appear, click **Continue** to reload the previous page.

To regenerate the HTTPS certificate:

- 1. In the Citrix SD-WAN Center web interface, click the **Administration** tab.
- 2. Click Global Settings and then click HTTPS Certificates.
- 3. In the Regenerate HTTPS Certificate section, click Regenerate HTTPS Certificate.

Regenerate HTTPS Certificate	0
Regenerating the Management HTTPS Certificate will Invalidate all connected sessions.	
Regenerate HTTPS Certificate	

The Regenerate HTTPS Certificate message appears. Click **Regenerate**.



Import MCN configuration

March 12, 2021

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

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

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

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

Import Virtual WAN Configuration		(?) ×
From Network: Active MCN	or]	From File: Browse
Valid Extension: cfg/zip Import to: New Package		etwork Maps from: Package
		Import Cancel

- 3. In the **From Network** field select one of the following options:
 - Active MCN: Connect to the active MCN and download the current Configuration.
 - **Other**: Connect to an IP address of a different MCN and download the current Configuration. You may have to install the security Certificate from this Citrix SD-WAN Center in the MCN before you can Import the Configuration.

For more information, see, Install the Citrix SD-WAN Center Certificate.

- 4. Alternatively, in the **From File** section, click **Browse** and select a Configuration to be uploaded from your computer.
- 5. In the **Import** to field select **Current Package** to import the contents of the selected file into the current open package.
- 6. In the Use Network Maps from, field select one of the following options.
 - Current Package: Retain the currently saved set of network maps after the import.
 - **New Package**: Use the network maps from the imported package and discard the current set of maps.
 - Both Packages: Use the imported maps in addition to the currently saved maps.
- 7. Click Import. The configuration is imported.

scale_256Branch_1DC_aes128_cb5100_2048Pathsospf_routefilters New Open Save Save As Import Export	Q All 🔻 Global Actions 🔻	i 0
Global O	Network Map +	
 DC5k BR257 BR258 BR259 BR260 BR261 BR262 BR263 BR264 BR265 BR267 BR266 BR267 BR268 BR271 <l< td=""><td>● 取 本 This Network Map is currently empty. To populate it. drag individual Sites from the tree on the left. You may also set a background on this map by clicking Configure (</td><td></td></l<>	● 取 本 This Network Map is currently empty. To populate it. drag individual Sites from the tree on the left. You may also set a background on this map by clicking Configure (

8. In the **Network Map** section. Click the settings icon and select **Auto populate** to automatically add and arrange each site in the configuration to the map.

Network Map +	
Network Map	0
	Branch-EE-Branch Branch & Branch MCN_DC-BranckBranch1-Branch3 MCN_DC-Branch3Branch3

Manage database

March 12, 2021

You can monitor and manage the database to ensure that there is enough available disk space to store the polling data from all the discovered appliances on the network.

Viewing database statistics

The **Statistics** table displays the available database statistics, and includes input fields for specifying the database disk usage thresholds for notifications and polling.

To view database statistics:

- 1. In the Citrix SD-WAN Center Web UI click the Administration tab.
- 2. Click **Database Maintenance**. Under **Statistics** section the following information is displayed.
 - **Record Time:** Displays the date and timestamp for the oldest and most recent records in the database. This column contains the following information:
 - **Start:** Displays the date and timestamp of the oldest record in the database.
 - End: Displays the date and timestamp of the most recent record in the database.
 - Active Storage Size (MB): Displays the current active storage's disk space.
 - **Database Size (MB)**: Displays the current database size and use information. This column contains the following information:
 - Total (MB): Displays the total size in MB of the database.
 - Usage (%): Displays the percentage of database disk usage in current active storage' s disk space.

Statistics						0
Record Time			Databa	se Size	Threshold	ds (96)
Start	End	Active Storage Size (MB)	Total (MB)	Usage (%)	Notification	Stop Polling
2016-09-06 08:59	2016-09-19 18:49	7416	893	12	45% ~	50% ~
Apply						

To set the notification and polling threshold:

1. In the **Notification** field, enter the percentage of the database size or active storage size to use as a threshold for generating a database usage notification. An email notification will be sent when database use exceeds this threshold.

- In the Stop Polling field, enter the database disk usage threshold (percentage) at which to stop statistics polling. Select a value from 10% to 50% from the drop-down menu. The default is 50%.
- 3. Click Apply.

Configuring auto cleanup

To keep database disk usage under control, you can specify thresholds that, when exceeded, trigger the removal of older records from the database.

To enable database cleanup and configure the thresholds:

- 1. In the Citrix SD-WAN Center Web UI click the **Administration** tab.
- 2. Click Database Maintenance.
- 3. Under **Auto Cleanup** section, select the **Remove oldest records by day when**... check box to enable database cleanup.

Auto Cleanup	0
Based on current usage, SD-WAN Center will reach the storage threshold in 212 days.	
 Remove oldest records by day when database usage exceeds 50% • of active storage size OR • database has more than 1 Month • of data 	
Apply	

When enabled, the database is automatically checked at 2:00 AM every day. The check initiates a database cleanup if the specified thresholds are met or exceeded. By default, this is not enabled.

Earlier, the default setting for SD-WAN Center database auto clean-up was as following:

- Remove oldest records by day when:
 - ...database usage exceeds 50% of active storage size
 - Operator must be select as AND
 - ...database has more than 6 months of data

With 11.1.1 release and above, the default setting for SD-WAN Center database auto clean-up has now changed to following:

- Remove oldest records by day when:
 - ...database usage exceeds 50% of active storage size

- Operator must be select as OR
- ...database has more than 1 month of data

Note

The change in settings will have no impact for the already provisioned SD-WAN Center systems which are upgraded to 11.1.1 release. It is only applicable to freshly provisioned 11.1.1 release or above SD-WAN Center systems.

- 4. Select ... database usage exceeds (%) of active storage size and then select a percentage from the drop-down menu to specify the threshold for a database cleanup. The options are from 10% to 50% in increments of 5%.
- 5. Select **AND** or **OR**, an operator from the drop-down menu between the "...database usage exceeds..."and "...database has more than..."thresholds to specify an operator how to apply for this rule. The default is **OR** since 11.1.1 release.
- 6. Select ...database has more than [# months] months of data and then select the number of months from the drop-down menu to specify the time span threshold for a database cleanup for which to keep data in the database. The options are from **1 month** to **12 months** in increments of one month.
- 7. Click Apply.

Configuring manual cleanup

You can manually remove statistics and events records from the database, based on specified criteria.

To perform a manual database cleanup:

- 1. In the Citrix SD-WAN Center web interface click the **Administration** tab.
- 2. Click Database Maintenance.
- 3. Under **Manual Cleanup section** select a filter from the **Remove Records** drop-down menu. The filter options are:
 - **older than:** Remove records collected before a specified date. When you select this filter, a date field and calendar selection button appear. Click the calendar button to select a date. All records older than the specified date will be removed.

Manual Cleanup	0
Remove records older than 🗸 09/07/2018	
Remove	

• **for Site:** Remove records collected before a specified date. When you select this filter, a date field and calendar selection button appear. Click the calendar button to select a date. All records older than the specified date will be removed.

Manual Cleanup		0
Remove records for Site 🗸	SITE5 SITE2 SITE3	
Remove		

4. Click Remove.

Manage views

March 12, 2021

The Fault, Reporting, Network Map and Statistics page allows you to create, display, modify and delete the respective views.

Note

The screenshots used in the procedure may vary from the actual user interface depending on the type of the view.

To create a new view:

- 1. Click **New View**, this creates a new, unnamed view and resets the time specification to the current time.
- 2. Create and apply filters or make the necessary changes.
- 3. Click Save As.
- 4. In the **Save View** dialog box enter a name for your view.
- 5. Click Save.

Save Report View	×
Name:	
View1	
	Save Cancel

To open and modify an existing view:

- 1. Click Open.
- 2. In the **Open View** dialog box, select a report view from the drop-down list.
- 3. Click **Open**. The event view opens.
- 4. Make the necessary modification as required.
- 5. Click Save.

Open Report View	×
Select a Report View View1	
	Open Cancel

To delete a view, open the view and click the delete icon.

Software upgrade

March 12, 2021

You can use the Software Upgrade option to upgrade your Citrix SD-WAN Center software to the latest version. The software upgrade process places Citrix SD-WAN Center into maintenance mode. If a database migration is required, this process can take several hours. During this time, no statistics data will be collected from the Virtual WAN, and all Citrix SD-WAN Center functionality will be unavailable.

Important

Running the upgrade during maintenance hours is recommended.

Note

Download the appropriate Citrix SD-WAN Center software package to your local computer. You can download this package from **Downloads** page.

To upload and install a new version of the Citrix SD-WAN Center software

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

User/Authentication Settings	Administration / Global Settings / Software Upgrade	
Global Settings	Management Interface HTTPS Certificate TimeZone Software Upgrade	
Database Maintenance Storage Maintenance	SD-WAN Center Software Update	Ø
and age that the arts	Current Version: R9_1_0_81_537013 built on 08/23/16	
	Browse_ Upload Clear	
	VWC55LCert1.gz	
	Instal 🗘	

- 3. Click **Browse** to open a file browser, and select the software package you want to upload.
- 4. Click **Upload** to upload the selected software package to the current Citrix SD-WAN Center virtual machine.
- 5. After the upload completes, click **Install**.
- 6. When prompted to confirm, click **Install**.
- 7. In the dialog box that appears, select the **I accept the End User License Agreement** checkbox, and then click **Install**.

Timeline controls

March 12, 2021

The Timeline at the top of the Fault, Reporting, Network Map and Statistics page provides controls for restricting the time frame of the current View. You can view a time frame of up to 30 days of data from the current database.

Note

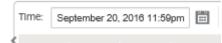
Based on selected time period, you can view the historic data irrespective of the current Citrix SD-WAN network configuration.

Time

You can use the following elements for specifying a time frame for the current View:

- **Time** Enter a date and time in the **Time** field to narrow the graph results to a specific date and time. The format can be any of the following:
 - Month Day, Year Hour: Minutes [am / pm] For example: September 7, 2015 2:00pm.

- *MM/DD/YYYY HH:MM* [am / pm] For example: 09/07/2015 8:36am.
- M/D/YY H:MM [am / pm] For example: 9/7/15 10:14pm
- **Calendar** (Calendar icon) Click the calendar icon to the right of the Time field and select a date to restrict the view results to that date.



• **Time line** - Click and drag to another point on a timeline to select a time frame of at least 30 minutes.



• Last: Hour / Day / Week / Month - Click an option (Hour, Day, Week, or Month) to restrict the view results to that time frame.

Last: Hour / Day / Week / Month

Mode

The Timeline mode determines how the timeline interprets time frame selections, and how automatic updates are reflected in the current view and on the Dashboard. There are two mode options, **Relative** (*selected time frame*) and **Absolute** (*selected time frame*), where selected time frame is the time frame specified in the **Time** field.

To change the Timeline mode, select either **Relative** or **Absolute** from the **Mode** drop-down menu at the top far right corner of the Timeline.

Relative Mode

If you select **Relative** mode, the Timeline treats the time frame specified for **Time** as a time relative to now. If you save the view and open it later, the information represented in the view will be relative to the time that the view was opened. If you have enabled automatic updates and a statistics update is detected, the view is updated relative to the latest time recorded in the database.

The currently specified time frame is shown in parenthesis as part of the **Relative** menu option. For example, if you selected **Last: Day** as the time frame, the **Relative** option displays as Relative (1 day ago - 1 minute from now).

Absolute Mode

If you select **Absolute** mode, the Timeline treats the time frame specified for **Time**: as absolute (static) points in time. The view will always represent the selected time, even if you save the view and open it at a later time, or if you enable automatic updates. The currently specified time frame is shown in parenthesis as part of the **Absolute** menu option, using the following format:

Absolute (*start_date start_time-end_date end_time*)

For example, if you selected **Last: Day** as the time frame, and the current date and time are 9/7 4:43 PM, the **Absolute** option displays as **Absolute (9/6 4:43 PM - 9/7 4:43 PM)**.

User accounts

March 12, 2021

You can view a list of all local and remote user accounts that have logged into Citrix SD-WAN Center virtual machine at least once. Remote user accounts are authenticated through RADIUS or TACACS+ authentication servers. You can also add a new local user account to Citrix SD-WAN Center.

Note

If a user-account is available on a remote authentication server but is never used to log on to Citrix SD-WAN Center, it is not displayed in the **Users** list.

To view user accounts in the SD-WAN Center web interface, navigate to **Administration > User/Au-thentication Settings**.

A list of user accounts appears in the **Users** section.

Dashboard Fault	March	a de a	Confloren	ntion Depend	la a	inistration	at law	o API				
Dashboard Fault	Monit	oring	Configura	ation Report	ang Adm	Inistration	NIT	O API				
		Administrati	on / User/Aut	thentication Settings								
User/Authentication Settings												
Global Settings	L L	Jsers +									0	
Database Maintenance	Se	arch										
Storage Maintenance	Na	me 🖍 Typ	e Level	Created	Modified	Last Lo	gin	Last Active	Two-factor Enabled	Write Access to Firewall	Manage	
Diagnostics	ad	min Local	User Admin	2019-04-11 08:29:47	2019-04-11 08:29:4	7 2019-05-13	09:03:13	2019-05-13 09:03:29	No	Yes	\$	
	roc	ot Local	User Guest	2019-04-11 08:30:13	2019-04-11 08:30:1	3 Never		No Session	No	Yes	\$	
	P	Primary Authentication										
	RADIUS Authentication					⑦ TACACS+ Authentication					0	
			ADIUS Authenti		Ŭ			Enable TACACS+ Authentication				
					Appl	Verify				Apply	erify	
	s	Secondary A	uthenticatio	n								
		RADIUS A	uthenticatior	ı		0	TACA	ACS+ Authentication			0	
		🗌 Enable S	econdary RADII	US Authentication			🗆 En	nable Secondary TACACS+	Authentication			

The following information is displayed:

- Name: The user name.
- **Type**: The type of user account, it can be one of the following:
 - Local: User accounts created and managed locally using the SD-WAN Center interface.
 - RADIUS: Remote user accounts authenticated by the RADIUS server.
 - **TACACS+**: Remote user accounts authenticated by the TACACS+ server.
- Level: The following are three levels of account privilege:
 - Admin: Admin account has administrative privileges. It has read-write access to all the sections.
 - Guest: Guest account is a read-only account with access to Dashboard, Reporting, and Monitoring page.
 - Security Admin: A Security Administrator has the read-write access only for the Firewall and security related settings in Config Editor, while having read-only access to the remaining sections.

Add Local User		×
User Name:		
User1		
Guest		
🗸 Admin		÷
Security Admin		P
Password:		
•••••		
Confirm Password:		
•••••		
	Add	Cancel

NOTE

- * Only the administrator and security administrator can change or modify the security feature configuration.
- * Security administrator can enable or disable the write access to the firewall for all user accounts except the super administrator.

Administration / User/Authentication Settings

Users +											0
Search											
Name 🔨	Туре	Level	Created	Modified	La	st Login	Last Active	Two-factor Enabled	Write	Access to Firewall	Manage
dmin	Local User	Admin	2019-04-05 07:00:08	2019-04-05 07:00:08	2019-0)5-07 05:33:50	2019-05-07 05:37:21	No	Yes		¢
uest	Local User	Guest	2019-04-23 08:42:11	2019-04-23 08:42:11	2019-0)4-23 08:42:24	2019-04-23 08:44:59	No	Yes	Set Password	
reetham	Local User	Security Admin	2019-05-07 05:34:10	2019-05-07 05:34:10	2019-0	5-07 05:34:54	2019-05-07 05:37:45	No	Yes	Disable Write Acces	s to Firew
ot	Local User	Guest	2019-04-11 06:47:54	2019-04-11 06:47:54	Never		No Session	No	Yes	Reset	
Primary	Authentic	ation									
RADIU	JS Authent	ication			0	TACACS+	Authentication				0
🗆 Ena	ble RADIUS A	luthentication				Enable T	ACACS+ Authentication				
				Apply Verify						Apply Ve	

A notification bar appears to all the users after the security administrator changes the firewall write permission for any specific user. This notification is shown per user and hence each logged in user must acknowledge the warning for it to removed.

Users +										0
Search										
Name 🔨	Туре	Level	Created	Modified	Las	it Login	Last Active	Two-factor Enabled	Write Access to Firewall	Manage
	Local User	Guest	2019-05-09 07:50:14	Never	Never		No Session	No	Yes	¢
admin	Local User	Admin	2019-04-05 07:00:08	2019-05-07 05:38:49	2019-0	5-14 05:52:31	2019-05-14 05:52:54	No	No	¢
guest	Local User	Guest	2019-04-23 08:42:11	2019-05-14 05:53:08	2019-0	4-23 08:42:24	2019-04-23 08:44:59	No	No	¢
preetham	Local User	Security Admin	2019-05-14 05:50:41	2019-05-14 05:50:41	2019-0	5-14 05:52:51	2019-05-14 05:53:10	No	Yes	¢
root	Local User	Guest	2019-04-11 06:47:54	2019-04-11 06:47:54	Never		No Session	No	Yes	¢

• Network Admin: A Network Administrator has read-write permissions to all the sections and can fully provision a branch except for the firewall and security related settings in the Configuration Editor.

Add Local User	×
User Name:	
Guest	
Admin	
Security Admin	
 Network Admin 	÷
Password:	*
Confirm Password:	
	*
	Add Cancel

The hosted firewall node is not available for the network administrator. In this case, the network administrator must import a new configuration. Both network and security related settings are maintained by the super administrator (Admin).

The network administrator and security administrator can make changes to the configuration and also deploy it on the network.

NOTE

The network administrator and security administrator cannot add or delete user accounts. They can only edit their own account passwords.

- **Created**: For local user accounts, the date the user account was created. For a remote user account, the date of the first login session.
- **Modified**: For local user accounts, the date the password was last changed. For remote users, the date of the first login session.

- Last Login: The date the user last successfully logged in. A tooltip displays the IP Address of the device used to log in.
- Last Active: The date the last request was made to the server. A tooltip displays the IP Address of the device used to log in.
- Manage: Click the gear icon to view a menu containing the following options:
 - **Set Password**: Change Password for the local user account. The current root password is required to change the root password. You cannot change passwords of remote user accounts.
 - **Reset**: Remove the workspaces and preferences for this user account.
 - **Delete**: Delete the local user account, workspaces, and preferences from SD-WAN Center. You cannot delete remote and admin accounts.
 - **Two-factor Enabled:** Enable two-factor authentication for the local and remote user account. For more information, see two-factor authentication.
- Write Access to Firewall: Shows the Write Access to Firewall is enabled or disabled.

To add a new local user account to the Citrix SD-WAN Center:

Note

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

1. Click the add icon + next to **Users**. **The Add Local User** dialog box appears.

Add Local User	×
User Name:	
JohnDoe	
Level:	
Guest	•
Password:	
•••••	
Confirm Password:	
Enable Two-factor	
	Add Cancel

- 2. Enter values for the following parameters:
 - User Name: The user name for the local user account.
 - Level: The account privilege. A guest user account is a read-only account limited to viewing dashboard, reports, and statistics. The guest user account does not have the privilege to edit and export the network configuration package to the MCN.
 - **Password**: The password for the user account.
 - **Confirm Password**: Reenter the password for confirmation.
- 3. Select **Enable Two-factor** to enable two-factor authentication for the local user account.

Note

The **Enable Two-factor** option appears only when the secondary authentication server is configured.

Configure a secondary authentication server, either RADIUS, or TACAS+ authentication. Ensure that the user account is configured on the secondary authentication server. For more information, see Secondary authentication.

4. Click **Add**. The new user account is created and the account information is added to the **Users** table.

Note

Citrix SD-WAN Center can have up to 600 local users.

Diagnostics

March 12, 2021

Citrix SD-WAN Center Diagnostics utilities provide Ping, Traceroute, and Packet Capture feature to test and investigate connectivity issues on Citrix SD-WAN Center appliance. The diagnostic options in the **Citrix SD-WAN Center dashboard control data** collection.

To use the Diagnostics tool, navigate to **Administration > Diagnostics**.

Citrix SD	-WAN (Center				R10_2_0_94_727224 ~	admin 🔻
					Administration		
C User/Authentication	Settings	Administrat	ion / Diagnostics / Pin	g			
Global Settings		Ping	Traceroute	Packet Capture			
Database Maintenan	ce						
Storage Maintenance	e	Ping IP Address:	Ping Count:	Packet Size:			
Diagnostics		8.8.8.8	5		Stop Ping 🔞		

Ping

You can ping any management IP address in the SD-WAN Center network using the **Ping** option.

Administration / Diagnostics / Ping

IP Address: Ping Count: Packet Size: 8.8.8.8 5 50 Ping PING 8.8.8.8 (8.8.8.8) 50(78) bytes from 8.8.8.8: icmp_req=1 t1=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=2 t1=116 time=30.7 58 bytes from 8.8.8.8: icmp_req=3 t1=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=4 t1=116 time=30.7 58 bytes from 8.8.8.8: icmp_req=4 t1=116 time=30.6 ms 58 bytes from 8.8.8.8: icmp_req=4 t1=116 time=30.6 ms 8.8.8 timesion 8.8.8 timesion bytes from 8.4.8.9 timesion bytes from 8.4.8.9 timesion bytes from 8.4.8.9 t1 t1 t1 <t< th=""><th>88.8.8 5 50 Ping Stop Ping 3 PING 8.8.8.8 (8.8.8.9) 50(78) bytes of data. 58 bytes from 8.8.8.9: icmp_req=1 ttl=116 time=30.7 ms 58 bytes from 8.8.8.9: icmp_req=2 ttl=116 time=30.7 ms 58 bytes from 8.8.8.9: icmp_req=3 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=4 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=4 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=4 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=5 ttl=116 time=30.6 ms</th><th>Ping</th><th>Traceroute</th><th>Packet Capture</th><th></th><th></th><th></th></t<>	88.8.8 5 50 Ping Stop Ping 3 PING 8.8.8.8 (8.8.8.9) 50(78) bytes of data. 58 bytes from 8.8.8.9: icmp_req=1 ttl=116 time=30.7 ms 58 bytes from 8.8.8.9: icmp_req=2 ttl=116 time=30.7 ms 58 bytes from 8.8.8.9: icmp_req=3 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=4 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=4 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=4 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=5 ttl=116 time=30.6 ms	Ping	Traceroute	Packet Capture			
<pre>58 bytes from 8.8.8.8: icmp_req=1 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=2 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=4 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=4 ttl=116 time=30.6 ms 8.8.8.8 ping statistics 5 packets transmitted, 5 received, 0% packet loss, time 4006ms</pre>	<pre>58 bytes from 8.8.8.8: icmp_req=1 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=2 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=4 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=4 ttl=116 time=30.6 ms 8.8.8.8 ping statistics 5 packets transmitted, 5 received, 0% packet loss, time 4006ms</pre>	IP Address:			ing 🕐		
58 bytes from 8.8.8.8: icmp_req=3 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=4 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=5 ttl=116 time=30.6 ms 8.8.8.8 ping statistics 5 packets transmitted, 5 received, 0% packet loss, time 4006ms	58 bytes from 8.8.8.8: icmp_req=3 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=4 ttl=116 time=30.7 ms 58 bytes from 8.8.8.8: icmp_req=5 ttl=116 time=30.6 ms 8.8.8 ping statistics 5 packets transmitted, 5 received, 0% packet loss, time 4006ms	58 bytes	from 8.8.8.8: icmp_	req=1 ttl=116 time=30.7 m			
5 packets transmitted, 5 received, 0% packet loss, time 4006ms	5 packets transmitted, 5 received, 0% packet loss, time 4006ms	58 bytes 58 bytes	from 8.8.8.8: icmp_ from 8.8.8.8: icmp_	req=3 ttl=116 time=30.7 m req=4 ttl=116 time=30.7 m	s 5		
		5 packets	transmitted, 5 rec	eived, 0% packet loss, ti	me 4006ms		

Provide a valid IP address along with the number of ping counts (amount of times to send the ping request) and packet size (number of data bytes). Click **Stop Ping** to stop an ongoing ping search.

Traceroute

Use the **Traceroute** option to ensure that the IP addresses are reachable. You can traceroute any management IP address in the network by displaying the route and measuring transit delays of packets.

Administration	/ Diagnostics / Tra	ceroute			
Ping	Traceroute	Packet Capture			
Trace Route					
8.8.8.8	Trace Route	⑦ to this IP address			
1 10.102	.78.1 (10.102.78.1)	.8), 30 hops max, 60 by) 0.591 ms 0.791 ms 0.425 ms 0.501 ms 0.	1.019 ms		
4 * * * 5 * * * 6 * * * 7 * * * 8 * 9 * * *					
10 * * * 11 * * * 12 * * * 13 * * 14 * * *					

Enter a valid management IP address to trace route. Click **Trace Route**.

NOTE:

The traceroute result display maximum 30 hops.

Packet capture

Use the **Packet Capture** option to intercept the data packet that is traversing over the selected active interface present in the selected site.

Dashboard	Fault	Monitoring	Configur	ration	Reporting	Administration	Nitr	ro API				
		Administra	ation / Diagno:	stics / Packe	t Capture							
er/Authenticatio	n Settings											
obal Settings		Ping	Tracero	ute	Packet Capture							
tabase Maintena	nce											
rage Maintenan	ce	Packet	Capture									
		Region:		Site: MCN-VPX1	Interface							
gnostics		Default_	Region 🚽	MCN-VPX1	* XMGI	X1 X2						
		Duration	seconds): Max	# of packets t	o view: Capture I	Filter (Optional):						
		5	¢ 10	\$ 000		(Capture)				
			Interface	Protocol	Time		Length	Source	Destination	Src Port	Dst Port	Src MAC
		1		UDP	APR 29, 2019 (06:06:20.188884243 UTC	66	15.1.1.16	15.1.2.15	4980	4980	56:44:91
		2		UDP	APR 29, 2019 (06:06:20.190739451 UTC	66	15.1.2.15	15.1.1.16	4980	4980	FE:43:35
		3		UDP		06:06:20.239489501 UTC		15.1.1.16	15.1.2.15	4980	4980	56:44:91
		4		UDP	APR 29, 2019 (06:06:20.239497013 UTC	98	15.1.1.16	15.1.2.15	4980	4980	56:44:91
		5		UDP		06:06:20.239950766 UTC	98	15.1.2.15	15.1.1.16	4980	4980	FE:43:35
		6		ARP		06:06:20.270641940 UTC		172.200.1.10	172.200.1.1			FFIFFIFI
		7		UDP		06:06:20.286831175 UTC	66	15.1.2.15	15.1.1.16	4980	4980	FE:43:35
		8		UDP		06:06:20.289765349 UTC		15.1.1.16	15.1.2.15	4980	4980	56:44:91
		9		UDP		06:06:20.303668776 UTC		15.1.2.15	15.1.1.16	4980	4980	FE:43:35
		10		UDP		06:06:20.303676930 UTC	210	15.1.2.15	15.1.1.16	4980	4980	FE:43:3
		11		UDP		06:06:20.339579458 UTC	66	15.1.1.16	15.1.2.15	4980	4980	56:44:91
		12		UDP		06:06:20.339841014 UTC	210	15.1.1.16	15.1.2.15	4980	4980	56144191
		13	2	UDP		06:06:20.339845379 UTC 06:06:20.339848016 UTC	210 98	15.1.1.16 15.1.1.16	15.1.2.15 15.1.2.15	4980 4980	4980 4980	56:44:91
		14	2	UDP		06:06:20.340309229 UTC	98 98	15.1.2.15	15.1.1.16	4980	4980	FE:43:3
		16	MGT	ARP		06:06:20.421190610 UTC	42	10.105.173.216	10.105.173.216	4300	4300	FF:FF:FI
		10	MGT	ARP		06:06:20.421390308 UTC	42	10.105.173.216	10.105.173.216			FF:FF:FF
		18	MGT	ARP		06:06:20.421674549 UTC		10.105.173.216	10.105.173.216			FFIFFIFI
		19	MGT	ARP		6:06:20.490994358 UTC		10.105.173.201	10.105.173.129			
		20		UDP		06:06:20.387732865 UTC	66	15.1.2.15	15.1.1.16	4980	4980	FE:43:35
		21		UDP		06:06:20.390732429 UTC	66	15.1.1.16	15.1.2.15	4980	4980	56:44:91
		22		ARP	APR 29, 2019 (6:06:20.422031221 UTC		172.200.1.10	172.200.1.10			FF:FF:FI
		23		ARP	APR 29, 2019	6:06:20.422038355 UTC	42	172.200.1.10	172.200.1.10			FF:FF:FI
		24		ARP	APR 29, 2019	06:06:20.422042418 UTC	42	172.200.1.10	172.200.1.10			FF:FF:FF
		25		UDP	APR 29, 2019	06:06:20.438409499 UTC	66	15.1.2.15	15.1.1.16	4980	4980	FE:43:35
		26		UDP	APR 29, 2019	06:06:20.440153570 UTC	98	15.1.1.16	15.1.2.15	4980	4980	56:44:91
		27		UDP	APR 29, 2019	06:06:20.440515730 UTC	98	15.1.2.15	15.1.1.16	4980	4980	FE:43:35
		28		UDP		06:06:20.489045489 UTC	66	15.1.2.15	15.1.1.16	4980	4980	FE:43:35
		29		UDP	APR 29, 2019 (06:06:20.490358173 UTC	66	15.1.1.16	15.1.2.15	4980	4980	56:44:91

Provide the following inputs for packet capture operation:

- **Region** Select a region that is managed by the SD-WAN Center from the drop-down list.
- Site Available sites in the selected region. Select a site from the drop-down list.
- **Interface** Active interfaces are available for packet capture in the selected site. Select an interface or add interfaces from the drop-down list. At least select one interface to trigger a packet capture.

NOTE:

The ability to run packet capture across all the interfaces at once helps to speed up the troubleshooting task.

- **Duration(seconds)** Duration (in seconds) for how long the data have to be captured.
- Max # of packets to view Maximum limit of packets to view in the packet capture result.
- **Capture Filter (Optional)** The optional **Capture Filter** field accepts a filter string that is used to determine which packets are captured. Packets are compared to the filter string and if the

comparison result is true, then the packet is captured. If the filter is empty, then all packets are captured. For more information, see Capture Filters.

Following are some examples of this capture filter:

- Ether proto\ARP Captures only ARP packets
- Ether proto\IP Captures only IPv4 packets
- VLAN 100 Captures only packets with a VLAN of 100\
- **Host 10.40.10.20** Captures only IPv4 packets to or from the host with the address 10.40.10.20
- Net 10.40.10.0 Mask 255.255.255.0 Captures only IPv4 packets in the 10.40.10.0/24 subnet
- IP proto \ TCP Captures only IPv4/TCP packets
- Port 80 Captures only IP packets to or from port 80
- **Port range 20–30** Captures only IP packets to or from ports 20 through 30
- Host 10.40.10.20 and Port 80 and TCP Captures only IP packets to or from TCP port 80 on the host 10.40.10.20

Note:

The maximum capture file size limit is up to 575 MB. Once the packet capture file reaches this size, packet capturing is stopped.

Click **Capture** to view the packet capture result.

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.