
Install on Google Cloud Platform



For supported software information, click [here](#).

This article describes how to install, or instantiate, a Versa branch device on Google Cloud Platform. To perform the installation, you request AMI access to your Google cloud account from Versa Networks. Then, under Private images in Google cloud, you create a cloud management system (CMS) connector on the Versa Director node. The Director node then does the following:

- Orchestrate deployment of the Versa Operating System™ (VOS™) device.
- Apply and instantiate the post-staging configuration to the device to set it to be an SD-WAN gateway. An SD-WAN gateway is the part of an SD-WAN branch that performs routing, firewall, and security functions in an SD-WAN overlay network.
- Instantiate the device to set it to be a virtual customer premises equipment (vCPE) device. A Versa Networks vCPE device is a standalone vCPE device that performs Layer 3 through Layer 7 network functions.

When you request AMI access, ensure that you make the request from the account on which you are provisioning the Versa branch device. Because of Versa Networks security policies, you cannot share the AMI image of one Google cloud account with another account.


Releases 22.1.1 and later support cloud workload protection.

Before You Begin

The CMS connector between the Google cloud virtual machine (VM) and the Director node is associated with an organization. Ensure that you have created the necessary organizations. For more information, see [Configure Basic Features](#).

Add a CMS Connector

1. Log in to the Director node.
2. In Director view, select the Administration tab in the top menu bar.
3. Select Connectors > CMS in the left menu bar. The main pane displays a table of CMS connectors.
4. Select the CMS tab in the horizontal menu bar.

5. Click the  Add icon. In the Add CMS Connector popup window, enter information for the following fields.


Field	Description
CMS Name (Required)	Enter the name of the CMS connector. The name is a text string.
Organization (Required)	Select the organization in which to create the CMS connector.
Cloud Workload Protection	(For Releases 22.1.1 and later.) Click to enable cloud workload protection (CWP) for the CMS connector. Cloud workload protection secures workloads that move across different cloud environments and allows cloud-based applications to work properly without security risks. When you enable cloud workload

Field	Description
	protection, the Director node fetches tags and IP addresses associated with cloud resources. These tags and IP addresses display only when you configure dynamic address groups. For more information, see Configure Address Group Objects .
CMS Flavor	Select GCP as the type of cloud device for the connector. (Other options are AWS, Azure, and Versa.)
Secret Account Key (Required)	Enter the secret key for this connector that was generated by Google Cloud Platform.

6. Click OK.

Verify a CMS Connector

To verify that a CMS connector is working:

1. Log in to Versa Director.
2. In Director view, select the Administration tab in the top menu bar.
3. Select Connectors > CMS in the left menu bar. The main pane displays a table of CMS connectors.
4. Select the CMS tab in the horizontal menu bar.
5. Select the CMS connector you want to verify, and then click  Validate Connector in the horizontal menu bar. This command triggers an API call to the CMS connector to verify its Google Cloud Platform user rights. If the validation is successful, the message "Valid credentials" displays.

Director View | Appliance View | Template View

Monitor | Configuration | Workflows | **Administration** | Analytics

You are currently in Director View

Organizations | Appliances | Connectors

Local | **CMS** | Authentication | Syslog | Kafka | Certificate Authority | AMQP | Analytics Cluster | VMS Connector

Manage CMS Organization

Search [x] [Y] + Add [Delete] [Validate Connector]

	CMS Name	Organization	IP Address	CMS Flavor	Authentication	
					Username	Type
<input type="checkbox"/>	aws	ACME		AWS		
<input type="checkbox"/>	azure	ACME		AZURE		
<input type="checkbox"/>	gcp-sm	Provider-Org		GCP		BASIC_AUTH
<input checked="" type="checkbox"/>	gcp-test	ACME		GCP		BASIC_AUTH
<input type="checkbox"/>	michal-techtalk-cms...	ACME		GCP		BASIC_AUTH
<input type="checkbox"/>	test-aws	Provider-Org		AWS		

Rows per page 25 Showing 1 - 6 of 7

Associate a CMS Connector with an Organization

After you add a CMS connector, you associate it with an organization that is already configured on the Director node. You can do this in one of two ways.

Method 1

1. Log in to Versa Director.
2. In Director view, select the Administration tab in the top menu bar.
3. In the left navigation bar, select Organizations. The main pane displays a table of organizations.

Director View | Appliance View | Template View

Monitor | Configuration | Workflows | **Administration** | Analytics

You are currently in Director View

Organizations | Appliances | Connectors

System | VMS Services | Scheduled Tasks | Notification Configuration | Entitlement Manager | Director User Management | Inventory | SDWAN | Support

Total Organizations: 2

Search [x] [Y] + Add [Delete] [Change Encryption Key] [Reset Encryption Key] [Appliance Proxy]

	Organization Name	Description	Tags	Parent Organization	CMS Connectors	Global Organization	Configured Appliance
<input type="checkbox"/>	ACME	-	-	Provider-Org	gcp-test aws azure michal-techtalk-...	2	View More...
<input type="checkbox"/>	Provider-Org	parent org	-	none	-	1	View More...

Rows per page 25 Showing 1 - 2

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Installation/Insta...

Updated: Wed, 23 Oct 2024 07:18:56 GMT

Copyright © 2024, Versa Networks, Inc.

4. In the main pane, select the name of the organization with which you want to associate the connector. The Edit Organization popup window displays.

Edit Organization

General Authentication **CMS Connectors** CMS Organizations Analytics Cluster Routing Instance Supported User Roles

CMS Connectors Cross Access Roles (AWS)

Available Add All

Search

test-aws >

Selected Remove All

Search

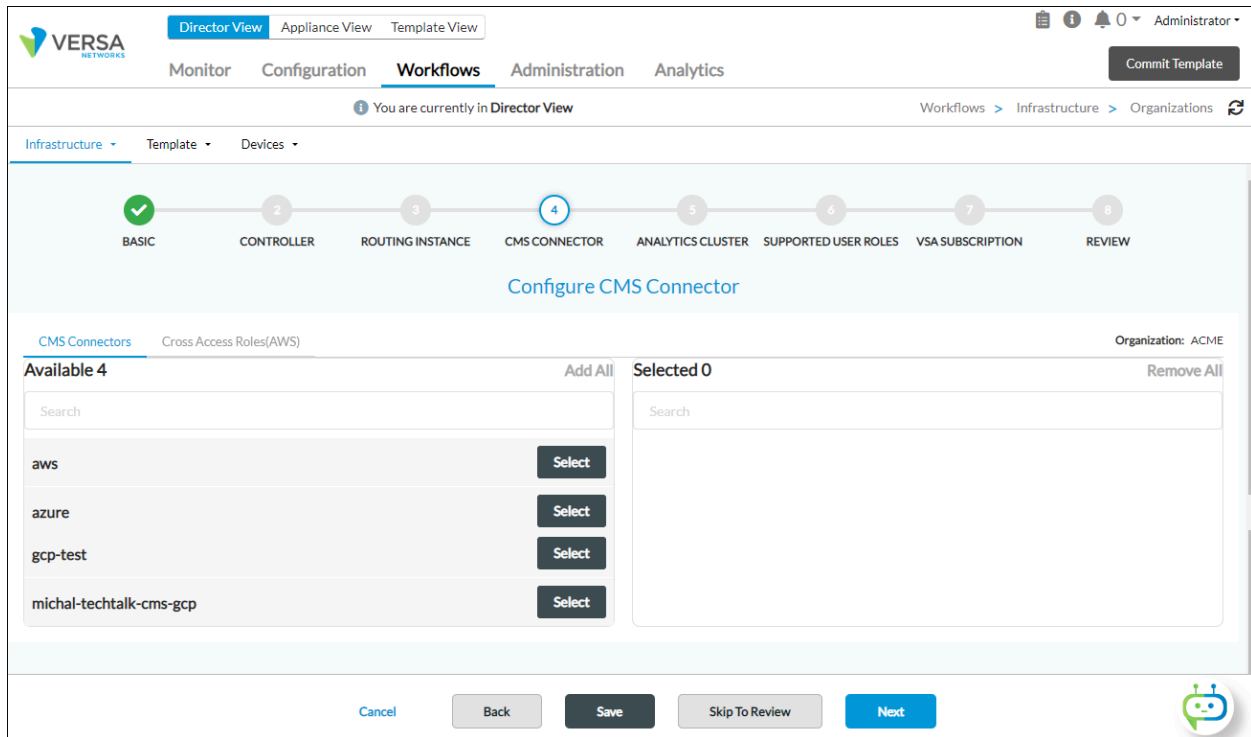
gcp-sm x

OK Cancel

5. Select the CMS Connectors tab.
6. In the Available pane, select the name of the Google Cloud Platform connector.
7. Click the add icon to add the connector to the Selected pane.
8. Click OK.

Method 2

1. Log in to Versa Director.
2. In Director View, select the Workflows tab in the top menu bar.
3. Select Infrastructure > Organizations in the horizontal menu bar. The main pane displays a table of organizations.
4. Select the organization with which you want to associate the connector. The Create Organization popup window displays.
5. Select the CMS Connector tab.
6. In the Available pane, click the Google Cloud Platform connector to add it to the Selected pane.



7. Click Deploy.

After you have created a CMS connector and associated it with an organization, configure the branch device on Google Cloud Platform to be a vCPE or an SD-WAN gateway. For more information, see [Configure a Public Cloud Device To Be a Virtual CPE Router or an SD-WAN Gateway](#).

Configure a Cloud Profile in a Device Workflow

To configure the Google Cloud Platform profile device workflow:

1. Log in to Versa Director.
2. In Director View, select the Workflows tab in the top menu bar.
3. Click the Organization menu icon, select an organization, and then select a device name in the main pane.

	Name	Global Device ID	Status	Last Modified By
<input type="checkbox"/>	Branch-1	101	Deployed	Administrator
<input type="checkbox"/>	gcp-123	104	Deployed	Administrator
<input type="checkbox"/>	michal-techtalk-vos-1	107	Deployed	Administrator
<input type="checkbox"/>	michal-techtalk-vos-a	103	Deployed	Administrator
<input type="checkbox"/>	michal-techtalk-vos-b	105	Deployed	Administrator
<input type="checkbox"/>	test-123	102	Failed	Administrator

- In the device workflow configuration window, select Step 1, Basic, and then enter information for the following fields.

Configure Basic

Device Name: testgcp

Name: testgcp Global Device ID: 111 Organization: ACME

Deployment Type: CPE-Public Cloud Serial Number: 138ac063-e30f-4179-9c2c-9158197493cf Device Group: dg-gcp

Generate Serial Number

Cancel Back Save Next

Field	Description
Name (Required)	Enter a name for the VOS device. The name is a text string.
Global Device ID (Required)	Displays the device ID, which is automatically assigned by the Director node.
Organization (Required)	Select the name of the organization to which the VOS

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Installation/Insta...

Updated: Wed, 23 Oct 2024 07:18:56 GMT

Copyright © 2024, Versa Networks, Inc.

Field	Description
	device belongs.
Deployment Type	Select the deployment type as CPE-Public Cloud, to deploy the device as a gateway to the public cloud.
Serial Number (Required)	Displays the generated serial number. If serial number is not displayed, click Generate Serial Number.
Device Group (Required)	Select the Google Cloud Platform device group to which the VOS device belongs.

5. Click Next.
6. In Step 2, Cloud Profile, enter information for the following fields.

The screenshot displays the Versa Networks Director View interface during the 'Configure Cloud Profile' step of a workflow. The workflow progress bar at the top indicates the current step is 'CLOUD PROFILE' (Step 2), with previous steps 'BASIC' (Step 1) and 'DEVICE SERVICE TEMPLATE' (Step 3) completed, and 'BIND DATA' (Step 4) and 'REVIEW' (Step 5) pending. The 'Configure Cloud Profile' form contains the following fields:

- Connector:** gcp-test
- Region:** asia-east1
- Instance Type:** n1-standard-4
- Image:** versa-flexvnf-577a81b-21-2-2
- Zone:** asia-east1-a

Below these fields is a 'Network/Subnet Mapping' table with the following columns: Interface, Device Network, Subnet, and Public IP required. The table contains one entry:

Interface	Device Network	Subnet	Public IP required
eth-0/0	MGMT	default/default	<input checked="" type="checkbox"/>

At the bottom of the form, there are buttons for 'Cancel', 'Back', 'Save', and 'Next'.

Field	Description
Connector (Required)	Select the connector to use to establish communication between Google Cloud Platform and the Director node. Note that after deploying the cloud VOS branch/hub-controller with the CMS connector, you must remove

Field	Description
	the public IP address of eth0 from the GCP portal. The Director node will manage the VOS branch/hub-controller using the SD-WAN overlay IP address, and will not use the eth0 public IP address. Additionally, you must change the default passwords for all cloud-hosted VOS nodes, for admin and versa accounts.
Region (Required)	Select the geographic region in which to deploy the VOS device.
Instance Type (Required)	Select the Google cloud VM instance type. The VOS software supports standard, high-memory, and high-CPU machine series of N1, N2, and N2D types ranging from 2 through 96 vCPUs.
Image (Required)	Select the VOS image to use to launch the VOS device.
Zone (Required)	Select the Google Cloud Platform availability zone.
Network/Subnet Mapping (Group of Fields)	Configure the subnet mapping for the VOS device.
◦ Subnet	Select the subnetwork that you created for the device.
◦ Public IP Required	Click to provide a public IP address for the network interface.

7. Click Next.

Supported Software Information

Releases 22.1.1 and later support all content described in this article.

Additional Information

[Branch Hardware and Software Requirements](#)

[Branch Overview](#)

[Configure a Public Cloud Device To Be a Virtual CPE Router or an SD-WAN Gateway](#)

[Initial Branch Software Configuration](#)

[Qualified AWS, Azure, and Google Cloud Instances](#)

https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Installation/Insta...

Updated: Wed, 23 Oct 2024 07:18:56 GMT

Copyright © 2024, Versa Networks, Inc.