

---

## Install on AWS

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

This article describes how to install, or instantiate, a Versa branch device on AWS. To perform the installation, you request AMI access to your AWS account from Versa Networks. When you have access to AMI, under Private images in AWS, you create a cloud management system (CMS) connector in the Versa Director node. Then, the Director node 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 used as part of an SD-WAN branch to perform routing, firewall, and security functions as a part of an SD-WAN overlay network.
- Instantiate the device to set it to be a virtual customer premises equipment (CPE) device. A Versa Networks vCPE device is a standalone vCPE device that performs Layer 3 through Layer 7 network functions.

When you make your request for 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 AWS account with another account.

Releases 21.2.1 and later support the AWS Elastic Network Adapter (ENA).

Releases 22.1.1 and later support cloud workload protection.

---

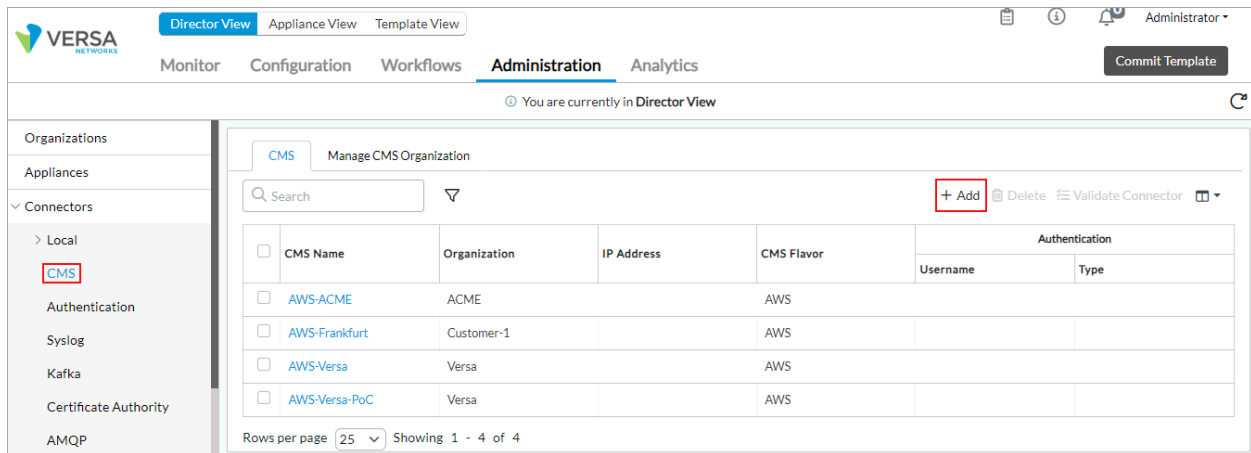
## Before You Begin

The CMS connector between the AWS 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 Versa Director.
2. In Director view, select the Administration tab in the top menu bar.
3. Select Connector > CMS in the left menu bar. The CMS connectors table displays.



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

### Add CMS Connector

CMS Name \*

Organization \*

Organization ▼

☐ Cloud Workload Protection

CMS Flavor

AWS ▼

☐ Use IAM Instance Credentials

Access Key ID \*

Secret Key \*

OK

Cancel

Field	Description
CMS Name (Required)	Enter the name of the CMS connector. The name is a text string.
Organization (Required)	(For Releases 22.1.1 and later.) Select an organization for 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 protection, the Director node fetches tags and IP addresses associated with cloud resources. These

Field	Description
	tags and IP addresses display only when you configure dynamic address groups. For more information, see <a href="#">Configure Address Group Objects</a> .
CMS Flavor	Select AWS for the type of cloud device. (Other options are Azure, Openstack, and VMware vCloud Director.)
Use IAM Instance Credentials	Click to use IAM instance credentials instead of using an access key.
Access Key ID (Required)	Enter the access key for this connector that was generated by AWS.
Secret Key (Required)	Enter the secret key for this connector that was generated by AWS.


- Click OK.

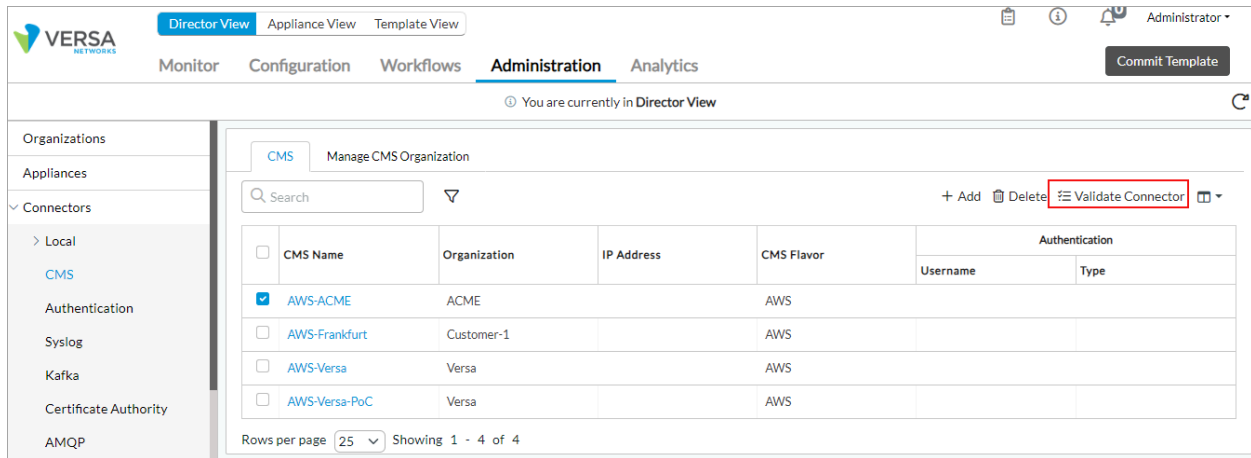
---

## Verify a CMS Connector

*For Releases 21.2.1 and later.*

To verify that a CMS connector is working:

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

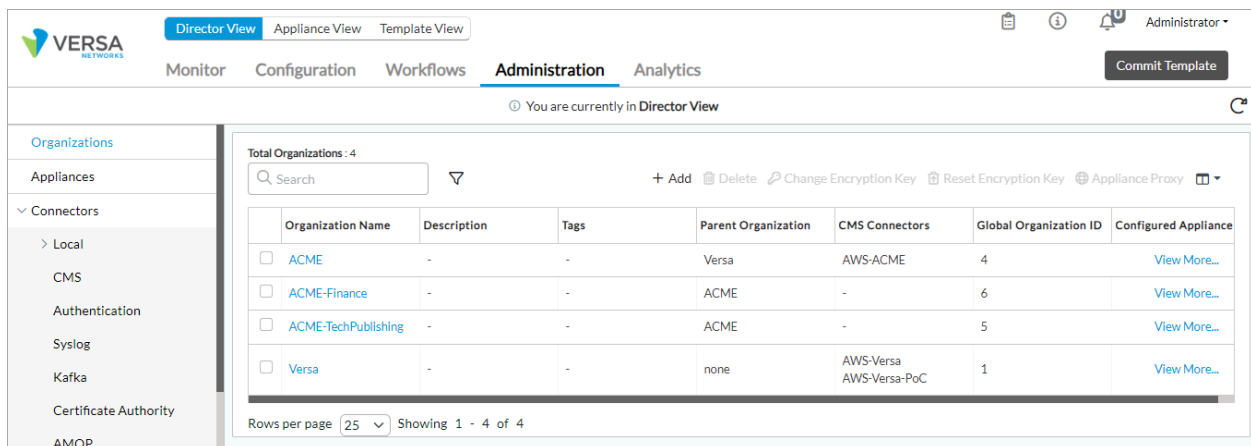


## Associate a CMS Connector with an Organization

After you have added a CMS connector, you associate it with an organization that you have already configured on the Versa Director. 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, click Organizations. The main pane displays a list of organizations.



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.

For Releases 22.1.1 and later:

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

AWS-ACME

Selected

Remove All

Search

OK

Cancel

For Releases 21.2 and earlier:

**Edit Organization**

Name\*  
NOV

Description

Tags

Global Organization ID\* 4    Organization Label This may be used for organization mapping    ☐ Shared Control Plane

Parent Organization Coke    Authentication Connector --Select--    Subscription Profile\* Default-All-Services-Plan

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

Available

Add All

Search

Versa-Azure-DEV

Selected

Search

Versa-AWS-Dev

aws-versa-ponnaiyan

OK   Cancel

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

## Method 2

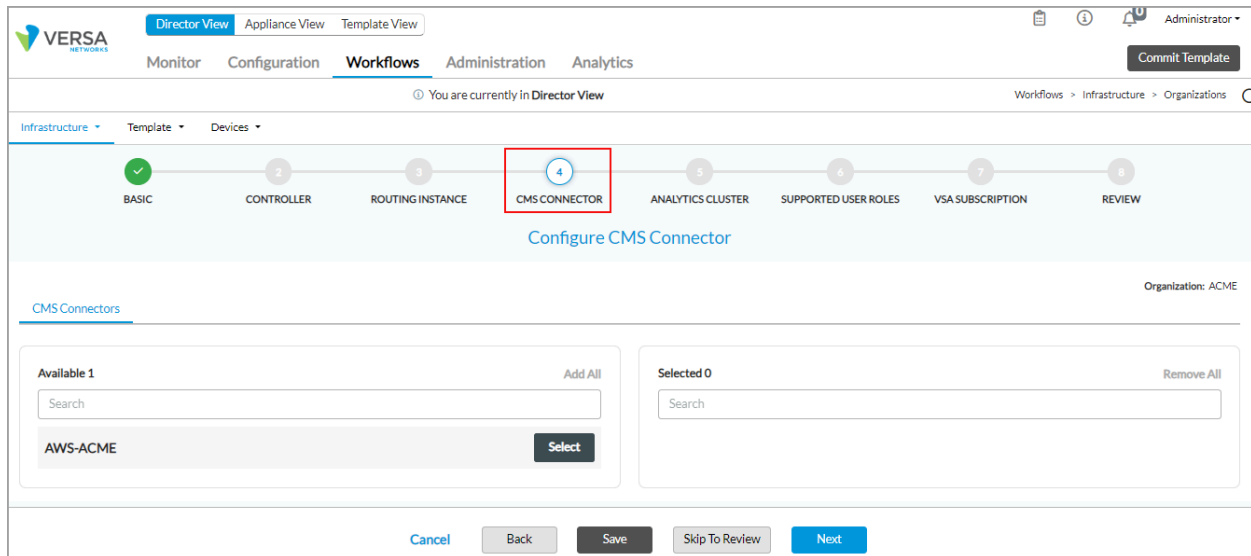
1. Log in to Versa Director.
2. Select the Workflows tab in the top menu bar.
3. Select Infrastructure > Organizations in the left menu bar. The main pane displays a list of organizations.
4. Select the name of the organization you want with which you want to associate the connector. The Create Organization popup window displays.
5. Select Step 4, CMS Connector. For Releases 21.2 and earlier, select the CMS Connectors tab.
6. In the Available pane, click the AWS connector to add it to the Selected pane.

For Releases 22.1.1 and later:

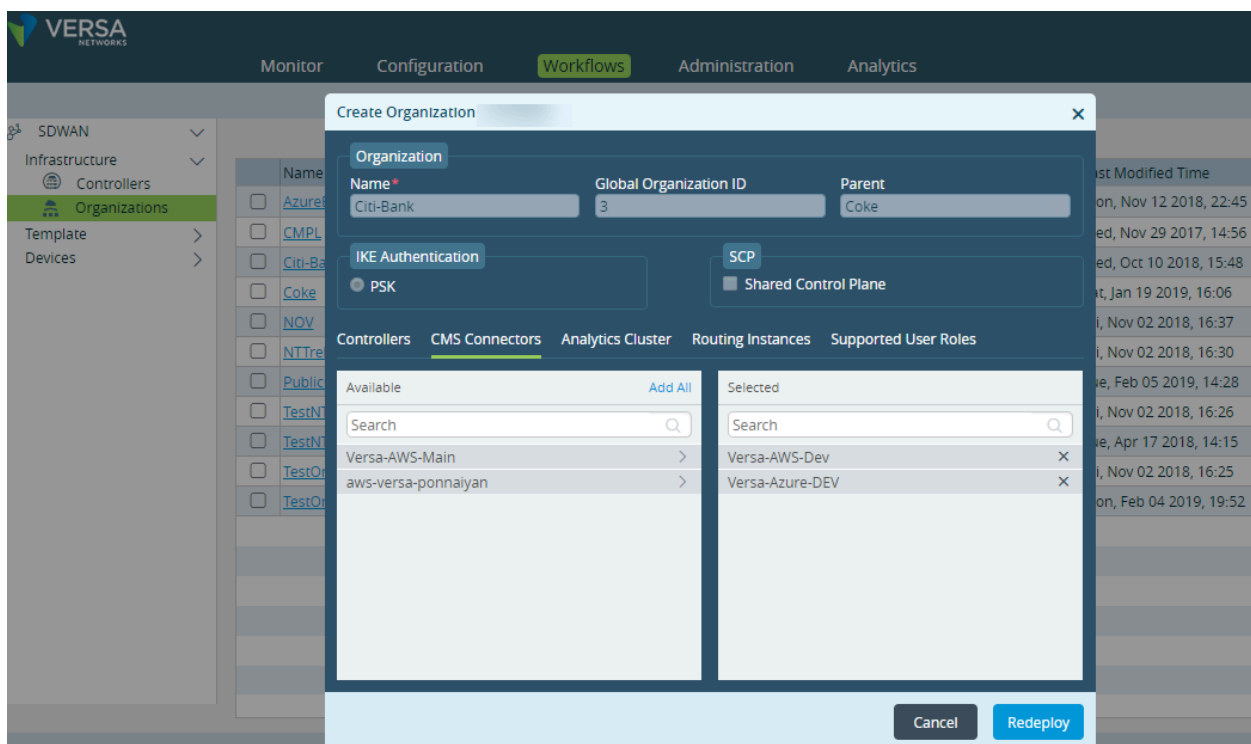
[https://docs.versa-networks.com/Getting\\_Started/Deployment\\_and\\_Initial\\_Configuration/Branch\\_Deployment/Installation/Insta...](https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Installation/Insta...)

Updated: Wed, 23 Oct 2024 07:16:47 GMT

Copyright © 2024, Versa Networks, Inc.



For Releases 21.2 and earlier:



7. Click Skip To Review, and then click Redeploy. For Releases 21.2 and earlier, click Redeploy.

After you have created a CMS connector and associated it with an organization, configure the branch device on AWS 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](#).

---

## IAM Policy for a CMS Connector

When you perform authentication using a CMS connector, use the following IAM policy so that the CMS connector functions on AWS:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAddresses",
        "ec2:DescribeInstances",
        "ec2:MonitorInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeAccountAttributes",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeSubnets",
        "ec2:AllocateAddress",
        "ec2:ReleaseAddress",
        "ec2:DescribeKeyPairs"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:TerminateInstances",
        "ec2:CreateTags",
        "ec2:RunInstances",
        "ec2>DeleteNetworkInterface",
        "iam:ListInstanceProfiles",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:StopInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:ReplacelamInstanceProfileAssociation",
        "ec2:CreateVolume",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteVolume",
        "iam:PassRole",
        "ec2:StartInstances",
        "ec2:DisassociatelamInstanceProfile",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteSecurityGroup",
```



```

        "ec2:AssociateIamInstanceProfile"
    ],
    "Resource": [
        "arn:aws:iam::*:instance-profile/*",
        "arn:aws:iam::*:role/*",
        "arn:aws:ec2::*:subnet/*",
        "arn:aws:ec2::*:instance/*",
        "arn:aws:ec2::*:volume/*",
        "arn:aws:ec2::*:security-group/*",
        "arn:aws:ec2::*:network-interface/*",
        "arn:aws:ec2::*:key-pair/*",
        "arn:aws:ec2::*:image/*"
    ]
}
]
}

```

## IAM Policy for VRRP-Based Failover

When you use VRRP failover, assign an IAM role to the Versa VOS EC2 instance with the following IAM policy.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeInstanceAttribute",
        "ec2:UnassignPrivateAddresses",
        "ec2:AssignPrivateAddresses",
        "ec2:*Subnets",
        "ec2:*VpcEndpoint",
        "ec2:ReplaceRoute",
        "ec2:DescribeRouteTables"
      ],
      "Resource": "*"
    }
  ]
}

```

## Set Up a Branch Without Using a CMS Connector

To install a Versa branch device on AWS without using a CMS connector:

1. Edit the `/etc/ssh/ssh_config` and add the following lines at the end of the file, just after the `ClientAliveInterval` line. If the branch device is reachable from the Director node using a public IP address, specify this public IP address in the line below.

[https://docs.versa-networks.com/Getting\\_Started/Deployment\\_and\\_Initial\\_Configuration/Branch\\_Deployment/Installation/Insta...](https://docs.versa-networks.com/Getting_Started/Deployment_and_Initial_Configuration/Branch_Deployment/Installation/Insta...)

Updated: Wed, 23 Oct 2024 07:16:47 GMT

Copyright © 2024, Versa Networks, Inc.

```
Match Address Director-northbound-IP-address/32
PasswordAuthentication yes
Match Address Director-southbound-IP-address/32
PasswordAuthentication yes
Match all
```

2. Restart the SSH service:

```
sudo service ssh restart
```

3. If you created the VM using an AWS marketplace AMI image, issue the **sudo passwd admin** command to change the default password of the admin account to "versa123".

You can now run the staging.py script to start the ZTP process.

---

## Software Release Information

Releases 20.2 and later support all content described in this article, except:

- Release 21.2.1 adds support for the AWS Elastic Network Adapter (ENA).
- Releases 22.1.1 adds support for cloud workload protection field.

---

## Additional Information

[Branch Hardware and Software Requirements](#)

[Branch Overview](#)

[Configure Address Objects](#)

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

[Initial Branch Software Configuration](#)

[Qualified AWS and Azure Instances](#)