Revised: June 2, 2025

Configure Site-Cloud Support for AWS Using Branch Connect Solution, Release 17.15.x

What's new and changed

This table lists the features available with the current release.

Cisco IOS XE release	Feature name	Description	Supported platforms
Cisco IOS XE 17.15.1a	Configure Site-Cloud Support to AWS Using Configuration Groups	You can now configure site to cloud connectivity from an SD-Routing branch to Amazon Web Services using Configuration Groups.	• Cisco Catalyst 8000V Edge software

Site to Cloud support for AWS using Branch Connect solution

With growing business needs there is an increased demand to extend the infrastructure without increasing costs. Cisco Catalyst SD-WAN's Cloud OnRamp solution offers the facility to connect an SD-Routing branch to an Amazon Web Services (AWS) cloud and thereby provide access to applications hosted on public clouds. The SD-Routing branch can be a data centre, branch site or campus network. This multicloud solution helps to integrate public cloud infrastructure into enterprise WAN.

This release introduces support to configure site to cloud connectivity from an SD-Routing branch to AWS using the Feature Profiles available as part of Configuration Groups. The Branch Connect solution available as part of Cloud onRamp Multicloud offering uses the Global VRF and Ethernet Interface created using Feature Profiles to establish a connection with the Transit Gateway and then automates the creation of Transit Gateway, deployment of the transit VPC (Virtual Private Cloud), and interconnection between the site and cloud.

Workflow to configure Site to Cloud Support for AWS

This figure shows the high-level workflow of the process to configure a site to cloud connectivity for AWS.

To know more about each step in the workflow, refer the following table.

Steps to Configure Site to Cloud Connectivity	To Know More
Prerequisites	Prerequisites to Configure Site to Cloud support
Onboard an SD-Routing Device	Onboard an SD-Routing device, on page 3to Cisco SD-WAN Manager.
Generate Bootstrap Configuration	Generate Bootstrap configuration , on page 5 to deploy an SD-Routing device in AWS using an AWS AMI image.
Deploy C8000v in AWS using AMI	Deploy C8000v Software as an AMI in AWS Console, on page 5 to make C8000v instance acessible across the internet.
Set Up Cloud Account	Set Up Cloud Account, on page 6to establish a connection between Catalyst SD-WAN Manager and Amazon Web Services (AWS). Cloud Global Settings, on page 7 to specify the solution you want to deploy on your Transit Gateway.
Discover VPC	Discover Host Private Network and use Tags to mark the VPC.
Manage	Manage Cloud Gateways , on page 9 to configure a Cloud Gateway. Gateway Management, on page 9 to attach onboarded SD-Routing device to the Transit Gateway.
Intent Management	Intent Management - Cloud Connectivity, on page 10to establish connectivity between VPCs Audit, on page 10to check if there are errors.
Verify	Verify configuration using Configuration Groups, on page 10 Verifying Configuration Using Commands
Monitor	Monitor MultiCloud using Catalyst SD-WAN Manager, on page 11

Configure Site to Cloud Support for AWS using Branch Connect solution

This section describes the various steps involved in configuring site to cloud support for AWS using a Branch Connect solution.

AWS Requirements

Set up an AWS cloud account and subscribe to AWS Marketplace using Cisco Catalyst 8000V for SD-WAN & Routing instance as an Amazon Machine Image (AMI).

For details see, Overview of Cisco Catalyst 8000v Edge Software on Amazon Web Services.

IOS XE Software Requirements

The functionality to use a Feature Profile to configure a Global VRF and Ethernet Interface is available from Cisco IOS XE 17.15.1a only. If you are on a release earlier than IOS XE 17.15.1a, you can configure VRF and Ethernet Interface using CLI Configuration Group or CLI Add-on Profile. For details, see Cloud Infrastructure on SD-Routing Devices.

Onboard an SD-Routing device

The first step to deploying the multicloud solution is to onboard the SD-Routing device into the Cisco SD-WAN Manager. After ensuring that the prerequisites are met, onboard an existing virtual or new virtual SD-Routing device into the Cisco SD-WAN Manager.

Onboard an existing virtual device

After ensuring that the prerequisites are met, onboard an existing virtual SD-Routing device into the Cisco SD-WAN Manager.

Step 1 Onboard the existing virtual device using the information in Onboard an Existing Software(Virtual) Routing Device Manually

Step 2 On the Cisco Catalyst SD-WAN Manager, select **Configuration > Configuration Groups**. Select the solution type as **SD Routing**.

Step 3 Select **Create Configuration Group**. Specify a name and description and select the **CLI Configuration Group** checkbox.

Step 4 Select the device that you onboarded in Step 1 from **Load Running config from reachable device**. Make any configuration changes as required. Any commands displayed in the **Classic CLI** pane are commands that do not have supported YANG models and therefore should be deleted. Click **Save** and **Done**.

Step 5 Select the CLI configuration group you created, click **+ Add**. Select the chassis ID of the device onboarded in Step 1. Click **Save**. This associates the CLI configuration group to the onboarded device. Select **Deploy**.

What's next

This completes the process of onboarding. After this, proceed with setting up a cloud account to configure site to cloud connectivity from an SD-Routing branch to AWS.

Onboard a new virtual device using CLI Configuration Group

Onboarding a new virtual device into Cisco SD-WAN Manager using a CLI Configuration Group

Step 1 On the Cisco Catalyst SD-WAN Manager, select **Configuration > Configuration Groups**. Select the solution type as **SD Routing**.

Step 2 Select **Create Configuration Group**. Specify a name and description and select the **CLI Configuration Group** checkbox.

Step 3 In the **Config Preview** pane, paste the following configuration and specify the details specific to your deployment such as system IP, site ID, org name and so on.

```
sd-routing
system-ip <system ip>
site-id <site id>
organization-name <org name>
sp-organization-name <SP-org name>
vbond port 12346 vbond ip <vbond ip>

wan-interface GigabitEthernet1
 !
hostname <hostname>
license boot level network-advantage addon dna-advantage
username admin privilege 15 secret 0 <password>
```

```
!

interface GigabitEthernet1
no shutdown negotiation auto
ip address dhcp
ipv6 enable
ipv6 address dhcp
ipv6 nd autoconfig default-route
exit
!
```

Step 4 Associate and deploy the Configuration Group to an SD-Routing device, on page 5.

Step 5 Generate Bootstrap configuration , on page 5.

Step 6 Deploy C8000v Software as an AMI in AWS Console, on page 5.

What's next

This completes the process of onboarding. After this, proceed with Setting up a cloud account to configure site to cloud connectivity from an SD-Routing branch to AWS.

Onboard a new virtual device using Feature Parcels

Onboard a new virtual device into Cisco SD-WAN Manager using a Feature Parcels.

Step 1 On the Cisco Catalyst SD-WAN Manager, select **Workflows > Workflow Library**. Select **Create SD-Routing Config** to automatically create a new configuration group with basic settings.

Step 2 Specify Name and Description. Click **Create SD-Routing Config**. After the System Profile, Service Profile, and Transport and Management Profile are automatically created, skip adding devices to the Configuration Group. Go back to Configuration Groups listing page and select the configuration group you created.

Step 3 Use down arrow to expand the configuration group and select **Transport and Management Profile**, click **Edit**. A global VRF is automatically created.

Step 4 Click **+** and select **Ethernet Interface**. Select **+ Add New** to add an ethernet interface to the global VRF. See Add Ethernet Interface for details. Click **Save**.

Tip If you prefer to configure the global VRF and ethernet interface using commands, see Create a CLI based Configuration Group.

The SD-Routing branch can have multiple custom VRFs but currently only the global VRF is supported to connect to the Transit Gateway. Any custom VRF's created are identified as SD-Routing VRF's during onboarding and are available in Cisco SD-WAN Manager under **Administration > VPN Groups** and in **Device > Interface.** But these VRF's are not displayed or available for Intent Management - Cloud Connectivity, on page 10 and therefore cannot be used for any purpose

Step 5 Configure Boot Level License

a) On the Cisco Catalyst SD-WAN Manager, select **Configuration > Configuration Groups**. Select the solution type as **SD Routing**

b) select the Configuration group you created for onboarding the device. Click **+ Add Profile**. Select **CLI Add-On Profile** and select **Create New** to create a new CLI Add-On Profile. Specify name and description of the profile.

c) In the Config Preview pane, enter command:`licenseboot level network-advantage addon dna-advantage`

d) Click **Save** and **Done**.

Step 6 Associate and deploy the Configuration Group to an SD-Routing device, on page 5.

Step 7 Generate Bootstrap configuration , on page 5.

Step 8 Deploy C8000v Software as an AMI in AWS Console, on page 5.

What's next

This completes the process of onboarding. After this, proceed with setting up a cloud account to configure site to cloud connectivity from an SD-Routing branch to AWS.

Associate and deploy the Configuration Group to an SD-Routing device

This task involves associating the Configuration Group to one or more devices and provisioning the configuration changes.

Ensure that the configuration group you select is created for SD-Routing devices.

Step 1 On Cisco SD-WAN Manager, select the **Configuration Group** created earlier.

Step 2 Click **+ Add** and select the devices from the list. Click **Save** to attach the configuration group to the selected devices.

Step 3 To provision the configuration changes, click **Deploy**.

a) Select the device on which you want to provision the configuration changes. Click **Next**.

b) For each device, review or update the IP address, hostname. Specify the password to access these devices. Click **Next**.

c) If you want to review the configuration changes, click **Preview CLI**. Select the device to view the configuration changes either inline or side by side. The configurations that are removed are highlighted in red and the new configuration is highlighted in green. To remove or add any device from the list of selected devices, **click Edit Device List**.

d) Click **Deploy** to provision the configuration changes on the devices.

Generate Bootstrap configuration

The bootstrap configuration you generate includes details such as UUID (Universally Unique Device Identifier) of the SD-Routing device, the global VRF, ethernet interface and the boot level license as well. This bootstrap configuration is used to deploy an SD-Routing device in AWS using an AWS AMI image.

Step 1 On Cisco SD-WAN Manager, select **Configuration** > **WAN Edges**.

Step 2 Select a device, click … and select **Edit**. Select **Bootstrap Configuration**.

Step 3 Select **Cloud-Init**. Click **Ok**.

Step 4 In the MIME file pop-up window, click **Download**.

The system downloads the file to your local system and saves it in your directory for downloads. The file name is *chassis***.cfg**, where chassis is the device chassis ID that you uploaded in Step 1 of this task.

Deploy C8000v Software as an AMI in AWS Console

An Amazon Machine Image (AMI) is an image that provides the software that is required to set up and boot an Amazon Elastic Compute Cloud (Amazon EC2) instance. This image creates a virtual machine within EC2.

When you set up an AMI in AWS the bootstrap configuration file and public IP address are used to deploy a Cisco C8000v instance and make it accessible across the internet. For more information, see Reference for Amazon EC2 instance configuration parameters.

Verify control connection of SD-Routing device

Control connections are secure tunnels that run between a WAN edge router and an SD-WAN controller. Use this task to verify that control connections are formed after the virtual device is onboarded.

Ensure that you have onboarded the existing virtual device or virtual device into the Cisco SD-WAN Manager.

	Command or Action	Purpose
Step 1	On Cisco SD-WAN Manager, go to **Tools** > **SSH Terminal**	Execute these commands to check the status of control connections: • show sd-routing control local-properties summary • show sd-routing control local-properties wan ipv4 • show sd-routing control connections summary • show sd-routing control connections history
Step 2	Verify the output of the commands to see interface and port details.	

Set Up Cloud Account

Setting up a cloud account involves setting up a connection between Catalyst SD-WAN Manager and Amazon Web Services (AWS). To form the association, the API details and Secret Key configured while setting up the Amazon Web Services account is required. Also determine if this cloud account should function as a Transit Gateway. A Transit Gateway is a software component that acts as a bridge between the branch and the AWS cloud.

Step 1 Go to Cisco Catalyst SD-WAN Manager. Select **Configuration** > **Cloud OnRamp for Multicloud**. Go to **Workflows**. Select **Associate Cloud Account**.

Step 2 Specify these details to perform the association between Catalyst SD-WAN Manager and AWS:

Table 1: Associate Cloud Account

Cloud Provider	Select the cloud provider you want to integrate with SD-WAN Manager. For deploying a multicloud solu **select Amazon Web Services**.
Cloud Account	Specify a name to identify the cloud account you ar
Description	(Optional) Specify a description for the cloud accou
Use for Cloud Gateway	Select **Yes** to create a Transit Gateway that connects to AWS.

Log in to AWS with	Specify how you want to log in to your AWS clo If you choose **Key**, specify the following details • **API Key** • **Secret Key** **Note :** The API Key and Secret key are generate AWS account. If you choose the **IAM Role**, specify the followi • **Role ARN** • **External ID** For details on how to configure an IAM Role, see Role.

Step 3 Click **Save**.

Cloud Global Settings

After establishing a connection between Catalyst SD-WAN Manager and AWS, specify the solution you want to deploy on your Transit Gateway. The current support is only for **Transit Gateway - Branch Connect**. In this solution each SD-Routing device establishes two IPSec tunnels to the Transit Gateway and runs one BGP session per IPSec tunnel. In a Branch Connect solution no C8000v instances are deployed inside the Transit Gateway.

Step 1 Go to Cisco Catalyst SD-WAN Manager. Select **Configuration** > **Cloud OnRamp for Multicloud**. Go to **Workflows**. Select **Cloud Global Settings**.

Step 2 Select the cloud provider for which you want to configure details. Click **Edit.** Specify details to configure the cloud setup.

Enable Configuration Group	This toggle setting is only applicable if you are deplo Cloud Gateway. The scope of IOS XE 17.15.1a release is limited to a solution. A Branch Connect solution uses the Configu through the Workflow Library.
Cloud Provider	Select **Amazon Web Services**. The current support i Web Services.
Cloud Gateway Solution	This option determines the kind of solution or peerin **Transit Gateway – Branch-connect**. This indicates up a connection between the Transit Gateway and the
Cloud Gateway BGP ASN Offset	Specify a number that is a multiple of 10 and follows 6[4-5][0-9][0-7]0. For example : 64520. The valid ra 65500.
Intra Tag Communication	Intra tag communication means if VPCs are set up, and have the same tag, communication can be establishe setting tags to VPCs, see *Host Private Networks.*

Program Default Route in VPCs towards TGW	The communication between the VPC and the Transit G through IPsec tunnels. This option is enabled by default IPsec tunnels for the Transit Gateway to communicate w
Enable Periodic Audit	This option is enabled by default for Catalyst SD-WAN periodic checks on the connections to AWS. These chec every 2 hours. The status of these checks is visible in the Catalyst SD-WAN Manager. Click **Completed** to view st
Enable autocorrect	This option is disabled by default. If enabled the Catalyst S identifies any errors with the multicloud solution.

Step 3 Click **Update** to save changes. The Transit Gateway set up is complete.

Discover

After the Transit Gateway set up is complete, a virtual network is allocated to your AWS account based on the region in which you have created the Transit Gateway. This network is termed as a VPC (Virtual Private Cloud). The integration of AWS with Catalyst SD-WAN Manager makes the process of discovering all host VPCs automatic.

Host Private Network

You can select one or more regions and use Tags to mark the VPC. Tags are metadata that you can assign to resources to easily organize, search, identify resources, and control access to resources. This is useful when you have many resources of the same type—you can quickly identify a specific resource based on the tags that you've assigned to it.

By using Tags you indicate that the VPC's with the same tags can communicate with each other therefore establishing peering.

You can tag and untag these VPCs and use it for future connectivity. The same tag can be used to map VPCs (that is, establish connectivity between VPCs) if the *Intra-Tag communication* in Global settings is enabled.

Step 1 Go to Cisco Catalyst SD-WAN Manager. Select **Configuration** > **Cloud OnRamp for Multicloud**. Go to **Workflows**. Select **Host Private Networks**.

Step 2 Select one or more regions from the list. Click **Tag Actions** > **Add Tag**.

Step 3 Specify a tag name. These tag names are saved in the cloud account with a prefix of *CiscoSdwanV2*.

Step 4 Verify the list of regions for which tagging has to be done. Also verify the list of VPCs corresponding to each of the regions.

Step 5 Click **Add** and **Save**.

Manage

After setting up the cloud account and configuring the global settings, you can create or manage a Transit Gateway by adding or removing SD-Routing branches. Additionally, you can also set up the number of tunnels for the Transit Gateway and also determine if each of these tunnels require acceleration through the AWS Global Accelerator.

Manage Cloud Gateways

A Cloud Gateway provides a path for network traffic to travel between a Virtual Private Cloud (VPC) and the public internet. It plays a crucial role by facilitating communication and data transfer between disparate networks, making it possible for different systems to work together seamlessly.

After setting up the cloud account and associating tags for the regions, configure a Cloud Gateway. Only one Cloud Gateway can be created per region.

Step 1 Go to Cisco Catalyst SD-WAN Manager. Select **Configuration** > **> Cloud OnRamp for Multicloud**. Go to **Workflows**. Select **Create Cloud Gateway** .

Step 2 Specify details to configure the cloud gateway.

Cloud provider	As the initial configuration involved selecting the clo configuring the cloud account, AWS is already selec Provider.
Cloud Gateway Name	Specify a name for the Cloud Gateway.
Description	(Optional) Specify a description for the Cloud Gatev
Account Name	Select an account name from the list. This is the clou specified during configuration of the cloud account.
Region	Specify the region in which the Cloud Gateway shou

Step 3 Click **Add** to start the process of creation of a Cloud Gateway. If creation of the Cloud Gateway is successful, the status is shown as **Success**.

Gateway Management

After the Transit Gateway is created, attach the onboarded SD-Routing device to the Transit Gateway.

Step 1 Go to Cisco Catalyst SD-WAN Manager. Select **Configuration** > **Cloud OnRamp for Multicloud**. Go to **Workflows** > . Select **Gateway Management**.

Step 2 Select the Transit Gateway you created and click …, select **Attach SD-Routing**. As part of **Cloud Global Settings**, if you have chosen to configure this solution using Configuration Groups, the VRF and Ethernet details created are already attached to the Transit Gateway.

Step 3 Click **Attach Sites**. From the list of branches in **Available Sites**, select a branch you want to attach to the Transit Gateway. Click **>** to move the selected branch to the **Selected Sites** pane. Click **<** to remove a site from the Selected Sites pane.

Step 4 Click **Next**. Select the interface that you configured as part of the Onboarding task. This is the WAN interface associated with the Global VRF.

Step 5 The **Public IP** of the SD-Routing branch is automatically populated if the SD-Routing branch is not configured behind a NAT Gateway. In case the SD-Routing branch is set up behind a NAT Gateway, replace the local IP address with the NAT Gateway IP address. Click **Next**.

Step 6 Specify the number of tunnels you want to create for the Transit Gateway. The range is from 1 – 8 and each tunnel gives a bandwidth of 2.5 Gbps. Each tunnel automatically creates two IPSec tunnels from the SD-Routing branch to the Transit Gateway.

Step 7 Enable **Accelerated VPN** if you want the AWS Global Accelerator to optimize the performance of your applications for local and global users. Click **Next**.

Step 8 Click **Next.** Verify the configuration. Click **Save and Exit.**

Intent Management

Ensure that you have enabled *Intra Tag Communication* in Global settingsbefore you start configuring intent for the VPCs .

The Intent Management workflow in Catalyst SD-WAN Manager enables connectivity between VPCs using tags created as part of *Discover Host Private Network* option. If two VPCs have the same tags, they can communicate with each other.

Intent is realized only if the region has a Transit Gateway connected to a branch. You can configure intent mapping without a Transit Gateway being present in different regions. The mapping intent is preserved and realized when a new Transit Gateway or mapping change is discovered.

When you deploy **Transit Gateway – Branch Connect** solution, only Global-VRF is supported to establish a communication channel between the Transit Gateway and branch . Any other VRFs configured for SD-Routing devices are not displayed for Intent Mapping. To establish communication between the SD-Routing branch and VPC hosts, intent mapping is required for the Global VRF. Intent Mapping can also be configured between the Global VRF and SD-WAN VPN.

Intent Management - Cloud Connectivity

Step 1 Go to Cisco Catalyst SD-WAN Manager. Select **Configuration** > **Cloud OnRamp for Multicloud** . Go to **Workflows**. Select **Cloud Connectivity.**

Step 2 Click **Edit**. All the tags associated with a specific branch are displayed. Each cell in the table corresponds to a region in the AWS cloud. If the region you select has a Cloud Gateway deployed, intent is realized and communication can flow between these VPCs.

Step 3 Click **Save**.

Audit

After all the configuration is done and the Transit Gateway is connected to the branch, run a check to see if the deployment is functioning without errors.

Step 1 Go to Cisco Catalyst SD-WAN Manager. Select **Configuration** > **> Cloud OnRamp for Multicloud**. Go to **Workflows**. Select **Audit**.

Step 2 Select **AWS** as the Provider. The status of the deployment is displayed. If any errors are detected in the connection between the Transit Gateway and branch the status is displayed as **Out of Sync**. In such cases, click **Fix Sync Issues** to automatically resolve any connection errors.

Verify configuration using Configuration Groups

After the site-cloud connectivity is established between the SD-Routing branch and AWS, verify that the configuration is accurate and there are no errors.

Step 1 On the Cisco Catalyst SD-WAN Manager, select **Configuration > Configuration Groups**. Select the solution type as **SD-Routing**.

Step 2 Select the configuration group created for the Global VRF and Ethernet Interface. Click down arrow to expand the Configuration Group, select the **Transport and Management Profile**. Click **Edit** to view the contents of this profile. The profile contains these auto-generated details for each SD-Routing device:

- Two auto-generated IPsec interfaces

- BGP Routing configuration
- Multicloud connection configuration
- Route policy for the Transit Gateway.

Verify configuration using commands

After the Transit Gateway is configured and communication is established between the site and AWS, verify the connection using show commands.

<table>
<tr><th></th><th>Command or Action</th><th>Purpose</th></tr>
<tr><td>Step 1</td><td>On Cisco SD-WAN Manager, go to Tools > SSH Terminal</td><td>Execute these commands to check the status of the connection:
<table>
<tr><th>Use command</th><th>To</th></tr>
<tr><td>show ip interface brief</td><td>display all tunnels and interfaces on the device, including the status.</td></tr>
<tr><td>show ip route</td><td>display all propogated routes. Propagated routes, in the context of Amazon Virtual Private Cloud (Amazon VPC), are routes that a virtual private gateway (VPG) automatically adds to route tables.</td></tr>
<tr><td>show ip bgp all</td><td>display routes hosted under all subnets.</td></tr>
</table></td></tr>
<tr><td>Step 2</td><td>Verify the output of the commands to see route, tunnel and interface details.</td><td></td></tr>
</table>

Monitor MultiCloud using Catalyst SD-WAN Manager

The Multicloud dashboard helps you monitor the Transit Gateway, connected VPCs and tunnels.

On the Cisco Catalyst SD-WAN Manager, choose **Monitor > Multicloud**. The status of the connection between Amazon Web Service and SD-Routing branch is displayed based on these parameters:

- Cloud Gateways
- Tunnels
- Connected Host VPCs