Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Release 17.2.1r

Note Use the workflow described in this section only for devices using Cisco IOS XE Catalyst SD-WAN Release 17.2.1r. For later releases, see Cloud OnRamp for SaaS, Cisco IOS XE Release 17.3.1a and Later.

This feature was released as a fully functional beta in Cisco IOS XE Catalyst SD-WAN Release 17.2.1r, with a provisioning workflow subject to change in future releases. This workflow was deprecated in Cisco IOS XE Catalyst SD-WAN Release 17.3.1a and replaced by a unified workflow that addresses Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices.

Table 1: Feature History

Feature Name	Release Information	Description
Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Cloud OnRamp for SaaS is available for Cisco IOS XE Catalyst SD-WAN devices, with a configuration workflow that is entirely different from the workflow that applies to Cisco vEdge devices. This feature is released as a fully functional beta in Cisco IOS XE Catalyst SD-WAN Release 17.2.1r. The provisioning workflow is subject to change in future releases.

Many organizations rely on software-as-a-service (SaaS) applications for business-critical functions. These cloud-based services include Office365, Salesforce, Box, and many others. As cloud-based services, these SaaS applications must communicate with their own remote servers, which are available through internet connections.

At remote sites, SaaS applications may these pose special challenges:

- **Performance**: If remote sites, such as branch offices, route SaaS traffic through a centralized location, such as a data center, performance degrades, with latency that affects the user experience.
- **Inability to optimize routing**: Network administrators may not have any visibility into the performance of these SaaS applications, or any ability to change the routing of the SaaS traffic to more efficient paths.

Cloud OnRamp for SaaS (formerly called CloudExpress service) addresses these challenges. It enables you to select specific SaaS applications and interfaces, and to let SD-WAN determine the best performing path for each SaaS application, using the specified interfaces. For example, you can enable:

- routing through a direct internet access (DIA) connection at a branch site, if available
- routing through a gateway location, such as a regional data center

SD-WAN monitors each available path for each SaaS application continually, so if a problem occurs in one path, it can adjust dynamically and move SaaS traffic to a better path.

For more information, see SD-WAN: Cloud OnRamp for SaaS Deployment Guide.

Overview: How to Configure Cloud OnRamp for SaaS

In contrast to using Cloud OnRamp for SaaS with vEdge devices, configuring the feature for Cisco XE SD-WAN devices includes two steps:

- determining the best paths (configured by feature template)
- using the best paths (configured by policy)

Here is a high level overview of the tasks.

	Task	Component	Summary
1	Determine the best paths for SaaS applications	Feature template	Create a feature template to configure Cloud OnRamp for SaaS to probe paths for specific SaaS application servers, determine the best path for each, and create a table based on these paths. SD-WAN probes periodically and updates the table with the most up-to-date information about the best path. If the topology includes gateway and branch sites, separate feature templates are required for branch sites and gateway sites. See Create a Probes Feature Template. **Note** The probes feature template is not supported for releases later than Cisco IOS XE Catalyst SD-WAN Release 17.2.1r.

	Task	Component	Summary
2	Use the best paths for SaaS applications	Policy	Create a policy to direct specific SaaS applications to use the best paths, as determined by the previous step. **Note** In the policy, specify only SaaS applications that are included in the feature template. If the policy specifies a SaaS application that is not included in the feature template, the traffic for that application uses the default path, as if Cloud OnRamp for SaaS is not enabled. See "Create a Policy for Cloud OnRamp for SaaS".

Common Scenarios for Using Cloud OnRamp for SaaS

For an organization using SD-WAN, a branch site typically routes SaaS application traffic by default over SD-WAN overlay links to a data center. From the data center, the SaaS traffic reaches the SaaS server.

For example, in a large organization with a central data center and branch sites, employees might use Office 365 at a branch site. By default, the Office 365 traffic at a branch site would be routed over SD-WAN overlay links to a centralized data center, and from there to the Office 365 cloud server.

Scenario 1: If the branch site has a direct internet access (DIA) connection, you may choose to improve performance by routing the SaaS traffic through that direct route, bypassing the data center.

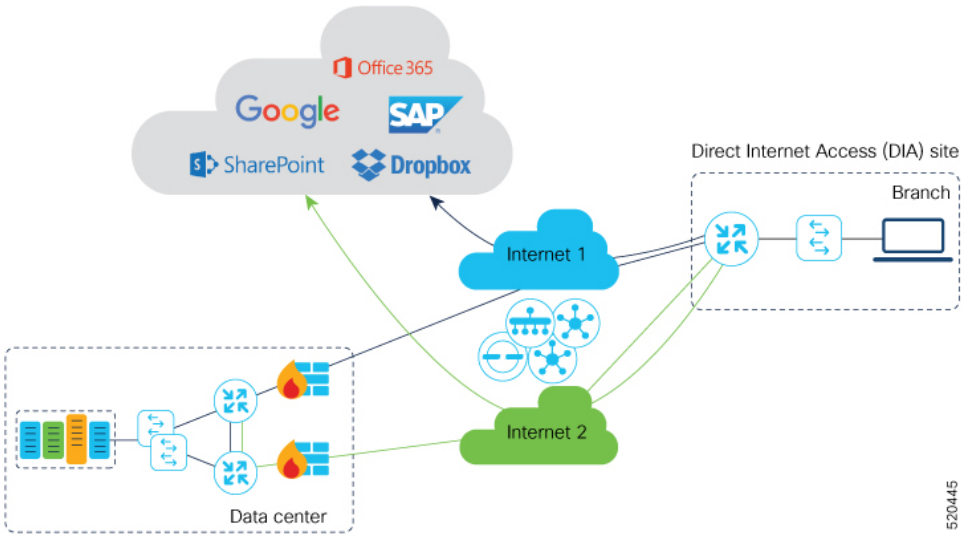
Scenario 2: If the branch site connects to a gateway site that has DIA links, you may choose to enable SaaS traffic to use the DIA of the gateway site.

Scenario 3: Hybrid method.

Scenario 1: Cloud Access through Direct Internet Access Links

In this scenario, a branch site has one or more direct internet access (DIA) links, as shown in the illustration below.

Using Cloud OnRamp for SaaS, SD-WAN can select the best connection for each SaaS application through the DIA links or through the SD-WAN overlay links. Note that the best connection may differ for different SaaS applications. For example, Office365 traffic may be faster through one link, and Dropbox traffic may be faster through a different link.



Configuration Workflow

Create Probes feature template(s) only for branch sites, and configure a policy to use Cloud OnRamp for SaaS.

	Task	Details
Branch sites		

1	Create a Probes feature template for branch sites.	In the Probes feature template, set parameters as follows:
		• **SaaS Mode**: SaaS Branch
		• **TLOCS** : Select either **All DIA TLOC** or **TLOC List** and select the TLOC colors in the drop-down menu.
		  • **All DIA TLOC**: Select this option if DIA is enabled for all TLOCs at a branch.
		  • **TLOC List**: If DIA is enabled only on a subset of TLOCs at a site, you can select this option and then select colors corresponding to the TLOCs that have DIA enabled.
		• **SaaS applications**: Specify applications for Cloud OnRamp for SaaS.
		
		See Create a Probes Feature Template.

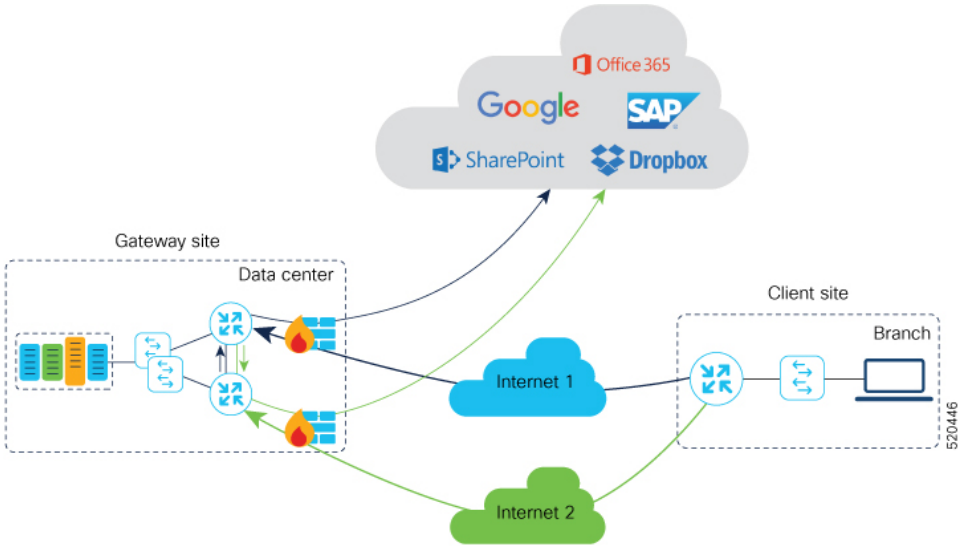
2	Use the feature template in a device template for branch sites.	In the Additional Templates section of the device template, in the Probes field, select the feature template created in the previous step.
3	Apply the device template to branch sites.	

	Task	Details
Policy		
4	Create a policy.	In the App Route Policy, under match conditions, select the Cloud SaaS application, and specify the same applications that you specified while creating the feature template. Select the action to be Cloud SLA. See “Create a Policy for Cloud OnRamp for SaaS”.
5	Activate the policy	Apply the policy to those branch sites to which the feature template created earlier was applied.

Scenario 2: Cloud Access through a Gateway Site

In this scenario, a branch site has one or more direct connections to a gateway site, and the gateway site has links to the internet.

Using Cloud OnRamp for SaaS, SD-WAN can select the best connection for each SaaS application through the gateway site. If the branch site connects to more than one gateway site, SD-WAN ensures that SaaS traffic uses the best path for each SaaS application, even through different gateway sites.



Configuration Workflow

Create Probes feature template(s) for branch sites and for gateway sites, and configure a policy to use Cloud OnRamp for SaaS.

	Task	Details
Branch sites		

	Task	Details
1	Create a Probes feature template for branch sites.	In the Probes feature template, set parameters as follows: • **SaaS Mode**: SaaS Branch • **TLOCS**: All DIA TLOC • **SaaS applications**: Do NOT specify any applications. **Note** Note this difference in this workflow, compared with scenario 1 (Cloud Access through Direct Internet Access Links). In this workflow, specify applications in the gateway site configuration (see below). See Create a Probes Feature Template.
2	Use the feature template in a device template for branch sites.	In the Additional Templates section of the device template, in the Probes field, select the feature template created in the previous step.
3	Apply the device template to branch sites.	
Gateway Sites		
4	Create a Probes feature template(s) for gateway sites.	• Unless the gateway sites use identical routers and interfaces, each gateway site requires a separate feature template. • **SaaS Mode**: SaaS Gateway After selecting **SaaS Gateway**, provide the interface name on which the Probe will be initiated. This interface must be bound to a non-zero VPN. • **SaaS applications**: Specify applications for Cloud OnRamp for SaaS. See Create a Probes Feature Template.
5	Use the feature template created in the previous step in a device template for gateway sites.	In the Additional Templates section of the device template, in the Probes field, select the feature template created in the previous step.
6	Apply the device template to gateway sites.	
Policy		
7	Create a policy.	Specify the same applications as in the feature template in task 4 above. See “Create a Policy for Cloud OnRamp for SaaS”.

	Task	Details
8	Activate the policy.	Apply the policy to those branch and gateway sites to which the feature templates created earlier were applied.

Scenario 3: Hybrid Approach

In this scenario, a branch site has both direct internet access (DIA) links, and links to a gateway site, which also has links to the internet.

Using Cloud OnRamp for SaaS, SD-WAN can select the best connection for each SaaS application, either through DIA links or through the gateway site.

Configuration Workflow

Create Probes feature template(s) for branch sites and for gateway sites, and configure a policy to use Cloud OnRamp for SaaS.

	Task	Details
Branch sites		

1	Create a Probes feature template for branch sites.	In the Probes feature template, set parameters as follows:
		• **SaaS Mode**: SaaS Branch
		• **TLOCS** : Select either **All DIA TLOC** or **TLOC List** and select the TLOC colors in the dropdown menu.
		  • **All DIA TLOC**: You can select this option if DIA is enabled for all TLOCs at a branch.
		  • **TLOC List**: If DIA is enabled only on a subset of TLOCs at a site, you can select this option and then select colors corresponding to the TLOCs that have DIA enabled.
		• **SaaS applications**: Specify applications.
		See Create a Probes Feature Template.

2	Use the feature template in a device template for branch sites.	In the Additional Templates section of the device template, in the Probes field, select the feature template created in the previous step.
3	Apply the device template to branch sites.	
Gateway Sites		

	Task	Details
4	Create a Probes feature template(s) for gateway sites.	• Each gateway site requires a separate feature template unless the gateway sites use identical routers and interfaces. • **SaaS Mode**: SaaS Gateway After selecting **SaaS Gateway**, provide the interface name on which the Probe will be initiated. This interface must be bound to a non-zero VPN. • **SaaS applications**: Specify applications for Cloud OnRamp for SaaS. See Create a Probes Feature Template.
5	Use the feature template created in the previous step in a device template for gateway sites.	In the Additional Templates section of the device template, in the Probes field, select the feature template created in the previous step.
6	Apply the device template to gateway sites.	
Policy		
7	Create a policy.	Specify the same applications as in the feature template in task 4 above. See “Create a Policy for Cloud OnRamp for SaaS”.
8	Activate the policy.	Apply the policy to those branch and gateway sites to which the feature templates created earlier were applied.

Create a Probes Feature Template

Note The probes feature template is not supported for releases later than Cisco IOS XE Catalyst SD-WAN Release 17.2.1r.

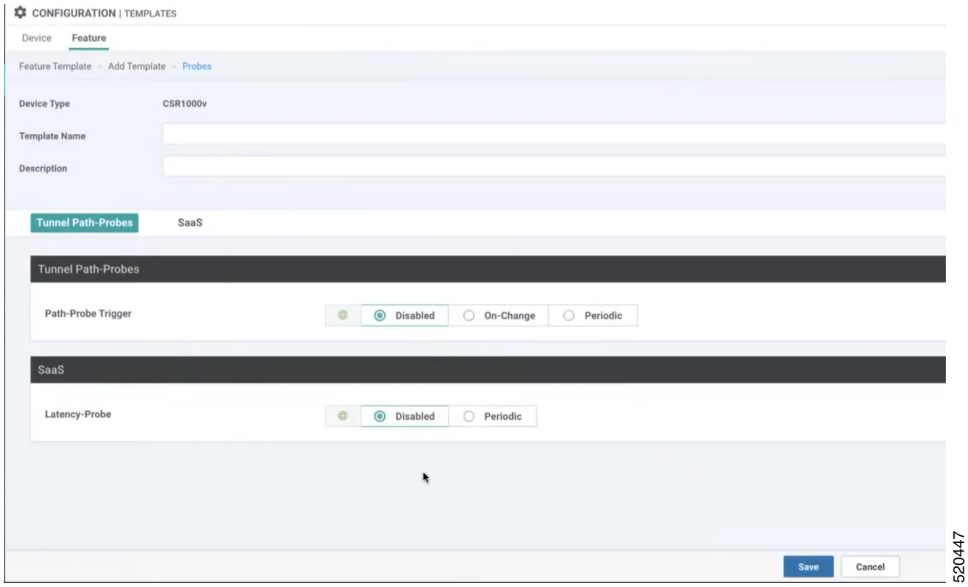
Follow these steps to create a Probes template to use Cloud OnRamp for SaaS on Cisco XE SD-WAN devices.

Create a feature template to apply either to branch site(s) or to gateway site(s). The SaaS Mode option in the template determines whether the template is for use with branch or gateway sites.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Feature Templates**.

Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is titled **Feature**.

3. Click **Add Template**.
4. Choose a device model.
5. In **Other Templates**, click **Probes** to create a probes template for Cloud OnRamp for SaaS.



6. Configure the following fields, as desired. Choosing some of the options changes the options available in other fields.

Field	Description
Tunnel Path-Probes	
Path-Probe Trigger	Must be set to **Disabled**. **Note** Not supported in this release.
Latency-Probe	**Disabled**: Disable Cloud OnRamp for SaaS in this feature template. **Periodic**: Enable Cloud OnRamp for SaaS.
Latency-Probe Frequency	Frequency (seconds) for probing the links between the site(s) and the SaaS application cloud server(s). The probe determines latency on each available path. Range: 0 to 65535 Default: 30 **Note** Recommended: Default value of 30
SaaS Mode	Select the type of site for this feature template. **SaaS Branch**: For a feature template that applies to a branch site. **SaaS Gateway**: For a feature template that applies to a gateway site.

Field	Description
TLOCS	(Available for the SaaS Branch option of SaaS Mode) **All DIA TLOC**: Include all direct internet access (DIA) interfaces at the site that have been assigned a valid color. **TLOC List**: Indicate interfaces to include by specifying one or more colors. These interfaces determine the possible routing paths for the SaaS traffic.
TLOCS List Color	(Available for the TLOC List option of TLOCS) Use the drop-down list to select a color. You can choose multiple colors.
Interface [x]	(Available for the SaaS Gateway option of SaaS Mode) Provide one or more interface names at the gateway site. The feature template applies only to these interfaces. Example: gig2/0
Path-Probe	Must be set to **Disabled**. **Note** Not supported in this release.

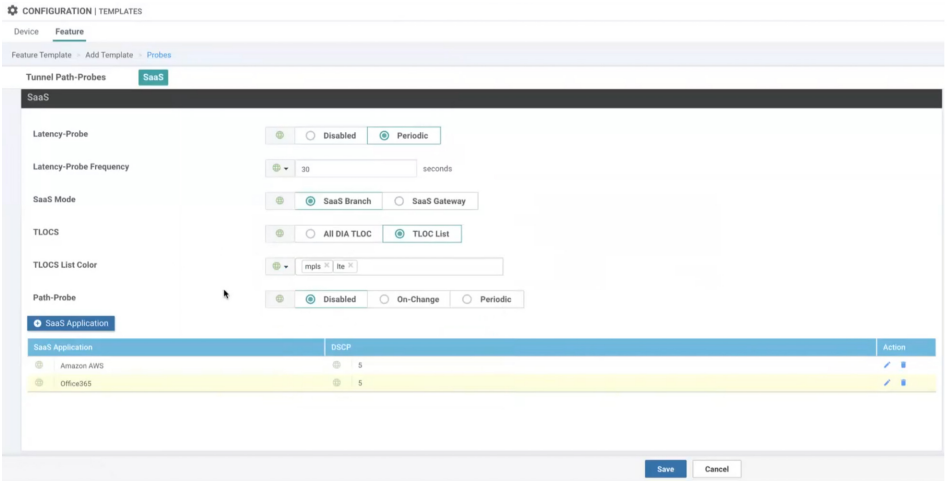
7. Click **SaaS Application** to display the following fields. Use these fields to specify a SaaS application. Repeat the process to add more applications.

   After you specify applications, they appear in a SaaS application table on this window. The table includes an Action column with options to edit or delete applications in the list.

Field	Description
SaaS App	Use the drop-down menu to select an application.
DSCP	**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, Cisco SD-WAN Manager CoR SaaS workflow will NOT push this option. The DSCP value provided is not used even when you enable this configuration option. Enter an integer value for the Differentiated Services Code Point (DSCP). A value must be entered, but it is not used by the system. You can assign the same DSCP value to different applications. Range: 0 to 63

8. Click **Save** to save the template.

   Example: The example below shows a Probes feature template configured for a branch site, including mpls and lte interfaces; it determines the best path for the Amazon AWS and for Office365 SaaS applications.



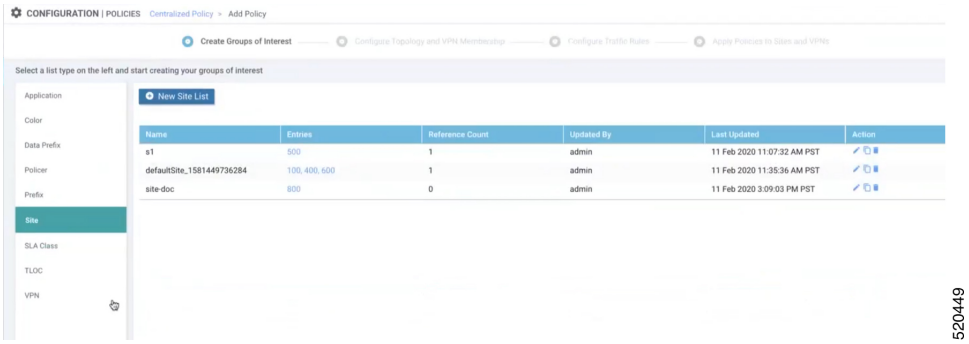
9. To use the feature template in a device template:

   In **Additional Templates** of the device template, in the **Probes** field, choose the feature template created in the mentioned steps.

Create a Policy for Cloud OnRamp for SaaS

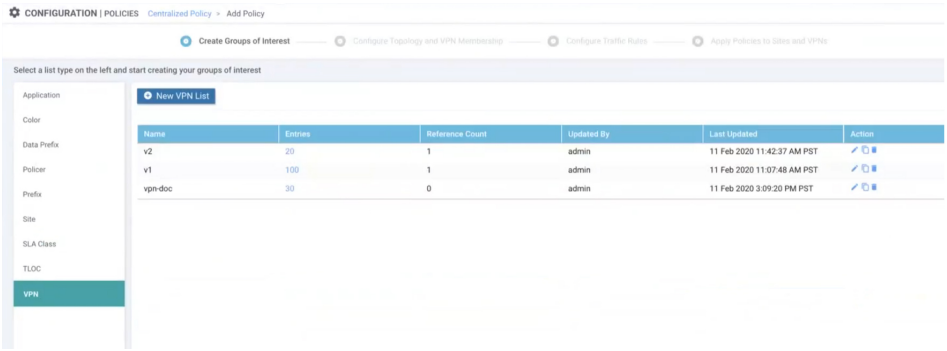
1. Select **Configuration** > **Policy**.
2. Click the **Centralized Policy** tab.
3. Click **Add Policy**.
4. In the left pane, click **Site**.
5. Create a list of sites to which to apply the policy. The list will be used in a later step.
   a. Click **New Site List**.
   b. In the **Site List Name** field, enter a site list name.
   c. In the **Add Site** field, enter one or more site numbers.
   d. Click **Add**.

      The site is added to the table of sites.



6. In the left pane, select **VPN**.
7. Create a list of VPNs to which to apply the policy. The list will be used in a later step.
   a. Click **New VPN List**.
   b. In the **VPN List Name** field, enter a VPN list name.
   c. In the **Add VPN** field, enter one or more numbers.
   d. Click **Add**.

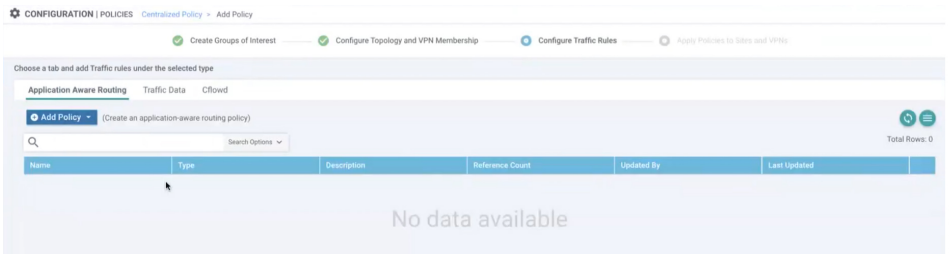
      The VPN is added to the table of VPNs.



520450

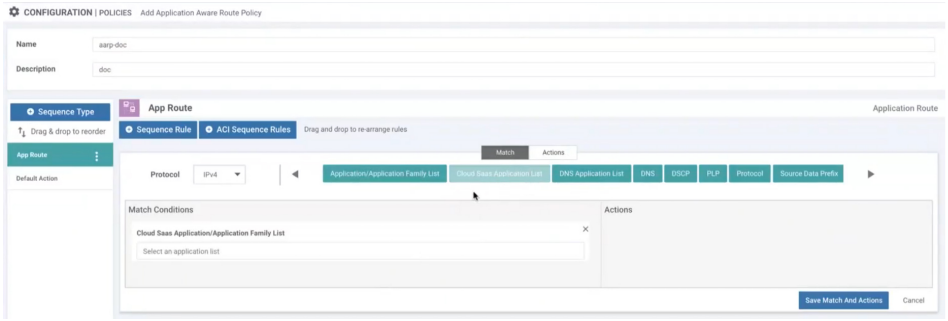
8. Click **Next** twice to display the Configure Traffic Rules step.

   The **Application Aware Routing** tab is selected by default.



520451

9. Click **Add Policy** and select **Create New**.
10. Create a policy.
    a. Enter a name and description for the policy.
    b. Click **Sequence Type**.
    c. Click **Sequence Rule**.
    d. With **Match** selected by default, click **Cloud SaaS Application List**.

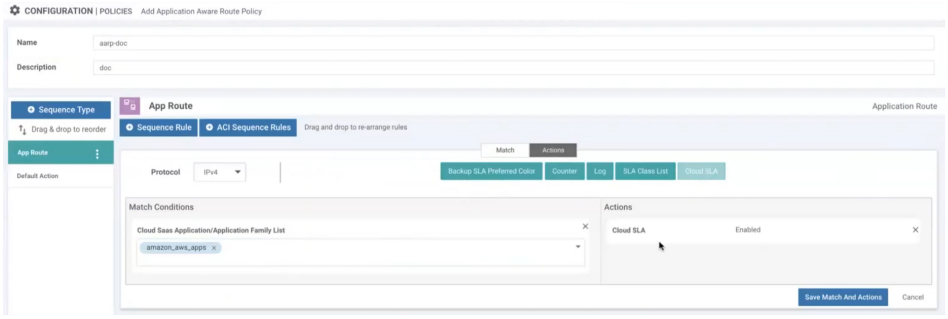


e. In the **Match Conditions** section, specify a SaaS application. Cloud OnRamp for SaaS is enabled for this SaaS application.

f. Click **Actions**.

g. Click **Cloud SLA**.

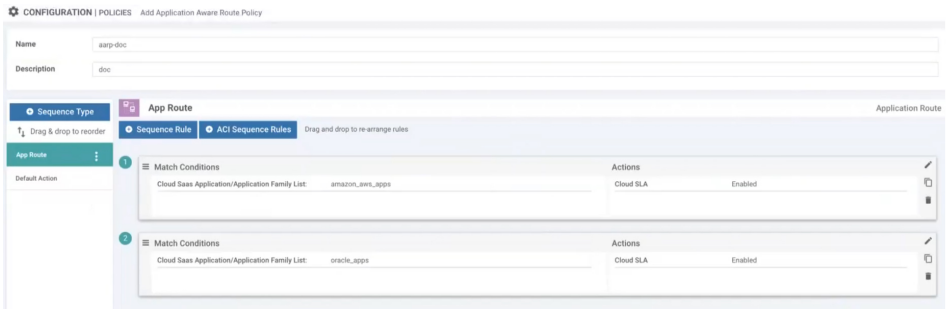
The **Actions** section shows Cloud SLA Enabled.



h. Click **Save Match And Actions**.

i. To add another SaaS application to this policy, click **Sequence Rule** again and follow the steps from 10c.

The following example shows two sequence rules, with Match Condition and Action, each rule specifying a single SaaS application.



j. Click **Save Application Aware Routing Policy**.

k. Click **Next** to display the Apply Policies to Sites and VPNs step.

l. Click the **Application-Aware Routing** tab.

m. Select a policy.

n. Click **New Site List and VPN List**. Select the site list and VPN list created earlier in this procedure.

o. Click **Add**.

p. Click **Save Policy**.

11. Activate the policy.

a. Select **Configuration** > **Policies**.

b. In the list of policies, locate the policy to activate. Click the "more actions" (...) button and select **Activate** to push the policy to the devices specified in the policy by site ID.