Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Releases 20.15.1 and Later

Note For information about template-based configuration of Cloud OnRamp for SaaS in earlier releases, see Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Release 20.3.1 to Cisco Catalyst SD-WAN Release 20.14.x.

Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Releases 20.15.1 and Later

Table 1: Feature History

Feature Name	Release Information	Description
Cloud OnRamp for SaaS Workflow	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Control Components Release 20.15.1	Cisco SD-WAN Manager provides a fully-guided workflow for selecting specific applications to enable Cloud OnRamp for SaaS. Cloud OnRamp for SaaS identifies the best paths for handling traffic for each of these applications.
Cloud OnRamp for SaaS for user-defined SaaS application lists	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	Cisco SD-WAN Manager supports adding, editing, and deleting user-defined probe endpoints for applications listed in the application catalog. Applications with endpoint details are eligible for: • cloud monitoring, and • steering through best path. You can also create an application list with applications having a common probe endpoint and enable Cloud OnRamp for SaaS for that application list.

Information About Cloud OnRamp for SaaS

Cloud OnRamp for SaaS can determine the best network path for each type SaaS application, also called cloud application, traffic. Select specific SaaS applications and Cloud OnRamp for SaaS identifies the best traffic paths for each of the SaaS applications.

Benefits

An organization with multiple branch offices can use Cloud OnRamp for SaaS to ensure that SaaS application traffic at each office uses the most efficient path. Using the most efficient path ensures that the employees at different locations experience consistent and high-quality access to cloud services such as Microsoft Office 365, Salesforce, or Google Workspace.

User-defined probe endpoints for applications

User-defined probe endpoint support is an enhancement that:

- enables adding probe endpoint details directly to applications in the Application Catalog,
- enables any application in the Application Catalog having probe endpoint details to be considered capable of cloud monitoring and/or steering through the best path using Cloud SLA action,
- provides a distinct view of user-defined cloud application lists and all application lists in the guided workflow, and
- simplifies the creation and deployment of application lists with applications having a common user-defined endpoint through a guided workflow.

Cloud OnRamp for SaaS capable applications

An application in Application Catalog that includes endpoint details is capable of supporting:

- Cloud Monitoring: Enabling detailed visibility and monitoring of these applications, and
- Cloud SLA: Ensuring that applications are steered through the best path computed with cloud monitoring.

A Cloud OnRamp for SaaS capable application list includes the following types of application lists:

- Default cloud application lists: 14 predefined application groups with predefined endpoints.
- User-defined cloud application lists: Application lists with applications that have common user-defined endpoints.

To use Cloud OnRamp SaaS capable application lists in policy groups, see the following procedures:

- configure using the workflow: Configure Cloud OnRamp for SaaS Using a Workflow, on page 4
- configure using the procedure: Add SaaS Applications Using Policy Groups, on page 5, and
- deploy using the procedure: Deploy SaaS Applications Using Policy Groups, on page 6.

Prerequisites for Cloud OnRamp for SaaS

- To enable Cloud OnRamp for SaaS for Webex and Microsoft Office 365 applications, ensure that Cisco SD-AVC is enabled (**Administration** > **Cluster Management**).

  Enable Cisco SD-AVC and cloud services.

  For Cisco Catalyst SD-WAN Manager Release 20.16.1 and earlier, enable cloud services in Cisco Catalyst SD-WAN. This also enables the Cisco SD-AVC Cloud Connector. For information on how to enable SD-AVC on SD-WAN Manager, see Enable SD-AVC for Cisco SD-WAN devices.

  Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, Cisco SD-AVC is enabled by default in SD-WAN Manager.

Restrictions for Cloud OnRamp for SaaS, General

Maximum supported applications

A Cloud OnRamp for SaaS capable application list supports maximum eight applications with common endpoint. A device supports maximum of eight user-defined application lists.

Support for SIG tunnels only

If you choose Secure Internet Gateway for Internet Offload Traffic for Cloud OnRamp for SaaS capable applications, it is supported only with the SIG tunnels.

Restrictions for Service VPN Gateway Mode

When you change the VPN settings of the service-VPN DIA interface, and Cloud OnRamp for SaaS is running in service-VPN Gateway mode, Cloud OnRamp for SaaS fails to work with the new service-VPN settings. The system continues to display stale data from the previous service-VPN setting for up to 10 minutes following the change and there is no data for the new service-VPN settings.

(Task)To prevent the issue, perform the following steps:

1. Detach the site from Cloud OnRamp for SaaS sites.
2. Update the VPN settings for the desired DIA interface on the Interface Configuration page.
3. Re-attach the site to Cloud OnRamp for SaaS as a service-VPN Gateway site.

Configure Cloud OnRamp for SaaS Using a Workflow

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library** > **Cloud OnRamp for SaaS**.

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, the application list displays separate lists for default cloud application lists and user-defined cloud application lists. Additionally, there is a tab that displays all available applications.

Step 2 Follow the on-screen instructions to complete the workflow.

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, you have the following options:

- In the **Select application lists** step of the workflow, you can use **+ Add application list** for the following:
  - Create user-defined list with applications having a common probe endpoint. For more information about defining a probe endpoint, see Add a user-defined endpoint to applications, on page 6.
  - Create custom applications with probe endpoints and associate the newly created applications in a new user-defined cloud application list.

To create an inline custom application list with applications having a probe endpoint, follow these steps:

a. Click on the **Applications with probe endpoint** dropdown.

b. Click **+Add Custom Application** and fill the required fields.

   For more information about configuring a custom application with endpoint, see Configure Custom Applications.

- In the **Select Policy** step of the workflow, you can view the devices associated with the policy group and review their update status.

Step 3 When the workflow is complete, you'll be prompted with a success screen to add policies to a policy group or associate devices with the policy groups or deploy the policy groups to the devices.

Add SaaS Applications Using Policy Groups

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Application Priority & SLA**.

2. Create a new **Application Priority & SLA** or edit an existing Application Priority & SLA.

   For more information, see Application Priority & SLA.

Note Use either **Secure Internet Gateway** or **Direct Internet Access** to choose an Cloud OnRamp for SaaS capable appication list.

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, the following scenarios occur depending on whether the application list is Cloud OnRamp for SaaS capable or not Cloud OnRamp for SaaS capable.

- If the application list is Cloud OnRamp for SaaS capable, a cloud SaaS sequence is generated for that application list.
- If the application list is not Cloud OnRamp for SaaS capable, the application list has NAT DIA or SIG configuration.

3. If you are an advanced user, switch to the **Advanced Layout** and configure Cloud OnRamp for SaaS. For more information, see Advanced Layout.

Note

- Choose Cloud OnRamp for SaaS applications from the **Application (Lists)** drop-down list in the **Match** field. For more information on match conditions, see Configure Traffic Rules.
- Choose **Cloud Monitoring** and **Cloud SLA** as **Action** conditions. For more information on action conditions, see Configure Traffic Rules.

Note In the **Advanced Layout**, if you choose an application list that is Cloud OnRamp for SaaS capable and add cloud SaaS actions to the sequence, Cisco SD-WAN Manager generates corresponding App-route policy sequence and Cloud OnRamp for SaaS probe configuration for Cisco IOS XE Catalyst SD-WAN edge device.

If you choose an application list that is not Cloud OnRamp for SaaS capable and add cloud SaaS actions, a warning message appears when you save the configuration. The message informs you that the application list contains applications that are not Cloud OnRamp for SaaS capable. This implies that some applications in the application list have no endpoints or have different endpoints.

The Cloud OnRamp for SaaS probe configuration for this application list is not generated in the Cisco IOS XE Catalyst SD-WAN edge device.

Deploy SaaS Applications Using Policy Groups

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Application Priority & SLA**. The application priority you just created appears here in the list.
2. In the **Policy Group** tab, choose a policy group to deploy. Choose the respective application priority from the drop-down list and click **Deploy**.

   For information about deploying policy groups, see Deploy Policy Groups Workflow.

Note When you've included Cloud OnRamp for SaaS applications in the policy group, the deploy workflow provides options to choose device variables such as **Site Type**, **TLOC**. Cisco SD-WAN Manager populates these fields with default values.

Enable **Secure Internet Gateway (SIG) Interface** if you want to secure your internet gateway.

Select **Enable Load Balancing** to balance the traffic using cloud SaaS probe.

Starting from Cisco Catalyst SD-WAN Manager Release 20.18.1, choose **None** to remove the probe configuration from the applications for a selected site. This option is useful when there are multiple sites associated to a policy group. It allows you to remove the Cloud OnRamp for SaaS capability on specific sites by removing the Cisco SD-WAN Edge probe configuration.

Add a user-defined endpoint to applications

You can add or remove endpoint details for any application in the application catalog using the following procedure.

Before you begin

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1 and Cisco IOS XE Catalyst SD-WAN Release 17.18.1a

- Review the prerequisites and restrictions sections for SaaS application lists.

Procedure

Step 1

If..	Then..
You want to add endpoint details for an existing application, which also includes custom applications.	From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** > **Applications**.
You want to create a custom application with endpoint details.	From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** > **Custom Application**.

Step 2 Follow one of the following procedures to add probe endpoint for an application or multiple applications:

a) To add or edit endpoint details for an existing application, click the ellipsis icon (**...**) next to the application under **Action** and click **Edit**.

Note
If you edit an application list or applications in an application list, you must save the Application Priority and SLA policy again.

b) (Optional) To create a custom application with endpoint details, click **Custom Application**.

To create a custom application with endpoint details, click **Custom Application** and follow the steps mentioned here. After defining the custom application, you can choose to add the endpoint details for it. For more information, see Configure Custom Applications.

Note
For custom applications, to prevent packet loss, do one of the following:

- Add a valid traffic class and business relevance while entering endpoint details on the Application Catalog page. This is the most preferable option.
- Switch to Advanced layout and add data policy sequences.
- Change the policy's default action to "accept."

This action prevents packets from being dropped if you choose the simple layout in Application Policy and SLA with the default action set to "drop".

Alternately, do the following:

a) Choose an application or multiple applications from the application list to add a user-defined endpoint. You can also filter specific applications using the **Search** field.

b) Click **Define Probe Endpoint**.

The applications that you choose are added to the **Selected Application(s)** area, which shows each application.

Step 3 In the **SaaS probe endpoint type** area, choose an endpoint type from the following options:

- **IP Address**: Enter an IP address. Cloud OnRamp for SaaS probes the server using port 80.
- **FQDN**: Enter a fully qualified domain name.
- **URL**: Enter a URL using HTTP or HTTPS. Cloud OnRamp for SaaS probes the server using port 80 or port 443, depending on the URL provided.

Step 4 In **SaaS probe endpoint value** field, enter an endpoint value, based on the endpoint type that you choose.

Example:

192.168.0.1, https://www.example.com, www.google.com

Step 5 Click **Save**.

(Optional) After adding endpoint details, you can also remove them. To remove the endpoint details of an application, click the ellipsis icon (**...**) next to the application under **Action** and click **Edit**. Navigate to the SaaS probe endpoint value area and remove the value field. Ensure you save the changes.

Monitor Cloud OnRamp for SaaS

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

The **Application Snapshots** section displays information such as the number of active sites, and device health.

Step 2 To view the applications that Cloud OnRamp for SaaS is monitoring, click the **Sites** tab.

Table 2: Site Information

Field	Description
Site Name	Site name.
Sites List	Site list that the site is associated with.
Device Name	Device name.
Monitored Applications	Monitored applications.
Site Role	Site role.

The view options include showing only active or inactive sites.

Step 3 To view the details of a site, click site name.

Table 3: Site Details

Field	Description
Application	Application associated with the site.
vQoE Status	vQoE Status. A green circle with a tick indicates that vQoE is good, the status with ! indicates that the vQoE needs some attention, and red X indicates that the vQoE is poor.
vQoE Score	vQoE score. Click the score to view detailed charts about the score.

Field	Description
DIA (Dedicated Internet Access) Status	Interface providing the best path for the cloud application.
Selected Interfaces	List of interfaces associated with the application.
Activated Gateways	For a site that connects to the internet through a gateway site, this indicates the IP address of the gateway site.
Local color	For a site that connects to the internet through a gateway site, this is the local color identifier of the tunnel used to connect to the gateway site.
Remote color	For a site that connects to the internet through a gateway site, this is the remote (gateway site) color identifier of the tunnel used to connect to the gateway site.
Application Usage	You can apply filters to view the specific types of data.

Step 4 To view configuration details, such as the configuration source, policy, number of devices, and so on, click the **Configuration** tab.

Migrate Older Cloud OnRamp for SaaS Path Selection

If you have enabled Cloud OnRamp for SaaS best path selection using the **Application and Policy** page before Cisco Catalyst SD-WAN Manager Release 20.15.1, you must perform the following procedure to configure these applications using the Cloud OnRamp for SaaS workflow:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS** > **Configuration**.
2. The first entry in the configuration tab shows the old app route policies in your Cisco SD-WAN Manager named as **Template Config**.
3. In the **Actions** column, click **...** and choose **Gateways**.
4. Choose the respective Site id and click **Detach Gateways**.
5. Follow the same instructions to detach **Applications and Policy**, **Client Sites**, **DIA Sites**, and **Custom Application Lists**.
6. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
7. On the **Device Templates** page, click **...** adjacent to the device and choose the **Detach Devices** option next to the respective device template to detach the device.
8. Configure the device using Configuration Groups. For more information, see Configuration Groups.
9. Follow the instructions to access the Cloud OnRamp for SaaS workflow and deploy using policy groups. For more information, see Deploy policy group.