



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, on page 1](#)
- [Information About Cloud OnRamp for SaaS, on page 2](#)
- [Prerequisites for Cloud OnRamp for SaaS, on page 2](#)
- [Configure Cloud OnRamp for SaaS Using a Workflow, on page 2](#)
- [Add SaaS Applications Using Policy Groups, on page 2](#)
- [Deploy SaaS Applications Using Policy Groups, on page 3](#)
- [Monitor Cloud OnRamp for SaaS, on page 3](#)
- [Migrate Older Cloud OnRamp for SaaS Path Selection, on page 5](#)

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. |

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.

Prerequisites for Cloud OnRamp for SaaS

- Cisco SD-AVC

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

- Cisco SD-AVC Cloud Connector

To enable telemetry for Webex and Microsoft Office 365 applications, ensure that Cisco SD-AVC Cloud Connector is enabled (**Administration** > **Settings**).

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

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](#).

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.

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. |
| 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](#).

