Cloud onRamp for SaaS, Cisco SD-WAN Release 20.3.1 and Later

Table 1: Feature History

Feature Name	Release Information	Description
View Details of Microsoft Telemetry and View Application Server Information for Office 365 Traffic	Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	This feature adds better visibility into how Cloud onRamp for SaaS determines the best path for Microsoft Office 365 traffic, if you have opted to use Microsoft telemetry. One enhancement is a chart that shows how Microsoft rates the connection quality of different interfaces, specifically for different types (called service areas) of Office 365 traffic. This is helpful for troubleshooting Office 365 performance issues. Another addition is the **SD-AVC Cloud Connector** page, which shows a list of Microsoft URL and IP endpoints and categories that Cisco SD-WAN receives from Microsoft Cloud.

Many organizations rely on software-as-a-service (SaaS) applications for business-critical functions. These cloud-based services include Amazon AWS, Box, Dropbox, Google Apps, Office 365, 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 pose these 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 Cisco 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

Ensuring the best path for cloud traffic is critical. 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.

Information About 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.

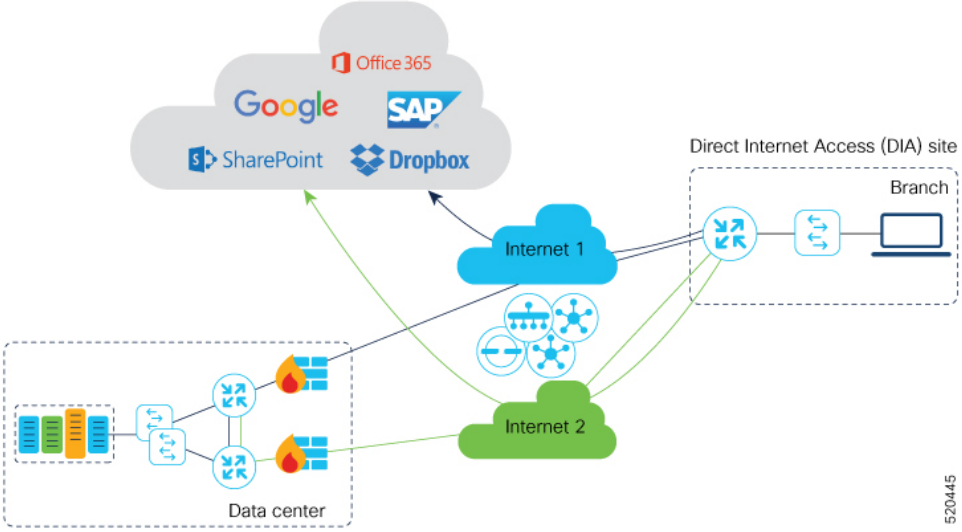
Scenario 2: If the branch site connects to a gateway site that has DIA links, you may choose to enable SaaS traffic to use the DIA of the gateway site.

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.

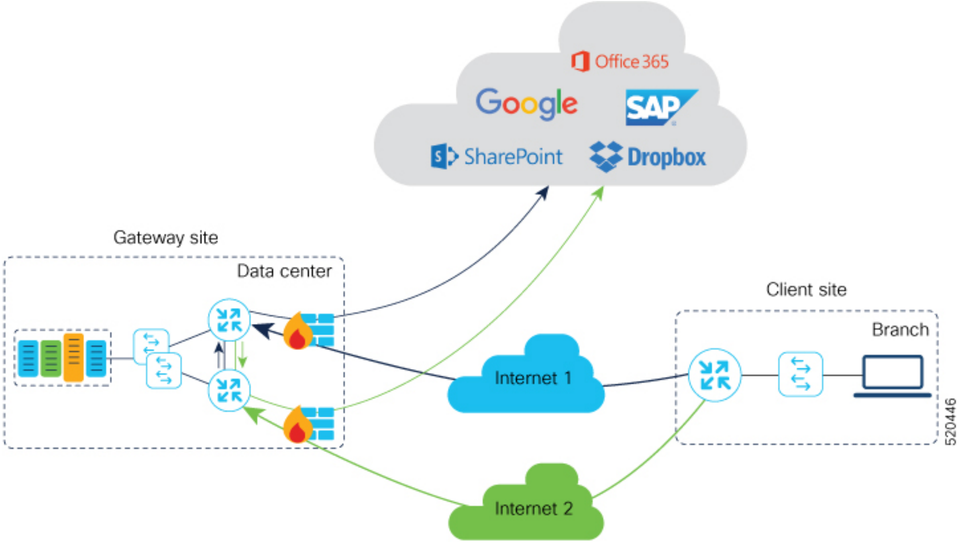
Using Cloud onRamp for SaaS, SD-WAN can select the best connection for each SaaS application through the DIA links or through the SD-WAN overlay links. Note that the best connection may differ for different SaaS applications. For example, Office365 traffic may be faster through one link, and Dropbox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



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.



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.

Best Path Determination

Cloud onRamp for SaaS selects the best path for each application using an algorithm that takes input from the following sources.

	Input	All Cloud Application Traffic	Office 365 Traffic
1	Cloud onRamp for SaaS metrics based on path probing	Yes	Yes
2	Application response time (ART) metrics	No	Yes (if enabled)
3	Microsoft telemetry metrics	No	Yes (if enabled)

Information About Cloud OnRamp for SaaS Probing Through VPN 0 Interfaces at Gateway Sites

A branch site may connect to the internet through one or more direct internet access (DIA) interfaces at the branch site itself, or through a gateway site, which might use a service VPN or VPN 0 to connect to the internet.

In addition to probing the DIA interfaces at a branch site, Cloud OnRamp for SaaS can probe interfaces at a gateway site, whether they use service VPNs (VPN 1, VPN 2, …) or the transport VPN (VPN 0), when determining the best path to use for the traffic of specified cloud applications. This is helpful when the branch site connects to the internet through a gateway site.

When configuring Cloud OnRamp for SaaS to use the gateway site, specify whether the gateway site uses service VPNs or VPN 0 to connect to the internet, as shown in the following illustrations.

Figure 1: Branch Site Connects to a Gateway Site That Uses Service VPNs to Connect to the Internet

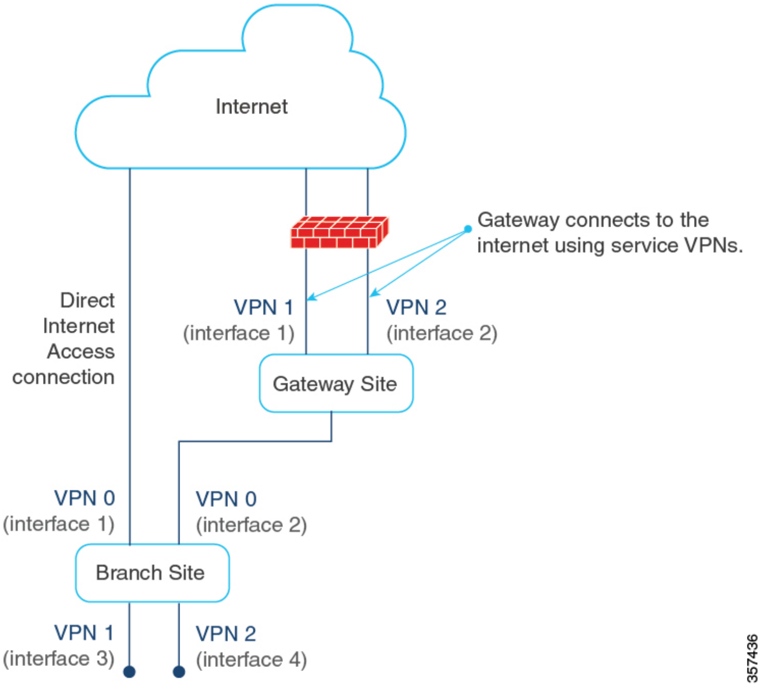
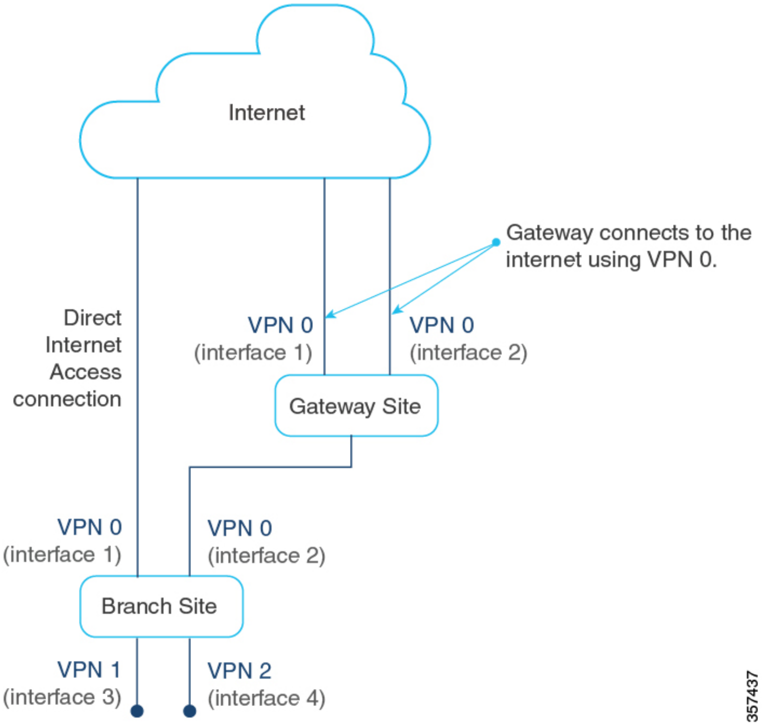


Figure 2: Branch Site Connects to a Gateway Site That Uses VPN 0 to Connect to the Internet



Benefits of Cloud onRamp for SaaS

Benefits of Cloud OnRamp for SaaS Probing Through VPN 0 Interfaces at Gateway Sites

In some network scenarios, a site connects to the internet, entirely or in part, through a gateway site that uses a VPN 0 interface to connect to the internet. This is in contrast to using service VPNs (VPN 1, VPN 2, …).

When the gateway site connects to the internet using VPN 0, the best path to cloud application servers may be through the VPN 0 interface. When Cloud onRamp for SaaS probes for the best path for the traffic of specified cloud applications, it can probe through VPN 0 interfaces at gateway sites. This extends the best path options to include more of the available interfaces connected to the internet.

Note A branch site that connects to the internet through a gateway site may also connect to the internet through one or more DIA interfaces at the branch site itself.

Supported Devices for Cloud onRamp for SaaS

Cisco IOS XE SD-WAN devices and Cisco vEdge devices support Cloud onRamp for SaaS.

The following table describes the device support for specific Cloud onRamp for SaaS features.

Table 2: Device Feature Support

Feature	Cisco IOS XE SD-WAN Device Support	Cisco vEdge Device Support
Basic Cloud onRamp for SaaS functionality	Yes	Yes
Cloud OnRamp for SaaS Probing Through VPN 0 Interfaces at Gateway Sites	Yes	Yes
Webex application support	Yes	No
Application Feedback Metrics for Office 365 Traffic	Yes	No
Microsoft to Provide Traffic Metrics for Office 365 Traffic	Yes	No
SD-AVC Cloud Connector	Yes	No
Viewing Path Scores for Office 365 Traffic	Yes	No
Cloud onRamp for SaaS Over SIG Tunnels	Yes	Yes
SaaS Application Lists	Yes	No
Webex Server-Side Metrics	Yes	No

For information about features supported on Cisco IOS XE SD-WAN devices, see Cloud onRamp for SaaS, Cisco IOS XE Release 17.3.1a and Later.

Prerequisites for Cloud OnRamp for SaaS

The following sections describe the prerequisites for Cloud OnRamp for SaaS features.

Prerequisites for Cloud onRamp for SaaS, General

The prerequisites for using Cloud onRamp for SaaS differ for Cisco vEdge devices and Cisco IOS XE SD-WAN devices. For information about using Cloud onRamp for SaaS with Cisco vEdge devices, see Cloud OnRamp Configuration Guide for vEdge Routers, Cisco SD-WAN Release 20.

For Cisco IOS XE SD-WAN devices, the requirements are:

- The devices must be running Cisco IOS XE Release 17.3.1a or later.
- The devices must be in vManage mode.
- All Cisco vSmart Controller instances must be in vManage mode.
- A centralized policy that includes an application-aware policy must be activated. You can configure more than one centralized policy in Cisco vManage, but only one can be active.

Note This is an important difference from using Cloud onRamp for SaaS with Cisco vEdge devices, which do not have this requirement.

- Cloud onRamp for SaaS is enabled (**Administration** > **Settings**).

To specify traffic by Office 365 traffic category, the following are also required:

- Cisco SD-AVC is enabled (**Administration** > **Cluster Management**).
- Cisco SD-AVC Cloud Connector is enabled (**Administration** > **Settings**). If Cloud Connector is not enabled, policies specifying Office 365 traffic cannot match the Office 365 traffic. The traffic uses the default path, rather than the best path selected by Cloud onRamp for SaaS.

Prerequisites for Cloud OnRamp for SaaS Probing Through VPN 0 Interfaces at Gateway Sites

Cloud onRamp for SaaS probing through VPN 0 interfaces at gateway sites presupposes that a branch site connects to the internet through a gateway site, and that the gateway site connects to the internet using a VPN 0 interface. The branch site may or may not also connect to the internet through one or more DIA connections.

Restrictions for Cloud onRamp for SaaS

The following section(s) describe the restrictions applicable to Cloud OnRamp for SaaS features.

Restrictions for Cloud onRamp for SaaS, General

Configuring Cloud onRamp for SaaS when a site is using a loopback as a transport locator (TLOC) interface is not supported.

Configuring Cloud OnRamp for SaaS on Cisco IOS XE SD-WAN devices is only through centralized app-aware policy using match condition "cloud-saas-app-list" and action "cloud-saas". For mixed deployments including Cisco SD-WAN and Cisco IOS XE SD-WAN devices, we recommend to have different app-aware policies for Cisco SD-WAN and Cisco IOS-XE SD-WAN devices.

Use Cases for Cloud onRamp for SaaS

Use Cases for Cloud OnRamp for SaaS Probing Through VPN 0 Interfaces at Gateway Sites

Enable gateway probing through VPN 0 interfaces if the following conditions apply:

- A branch site connects to the internet through a gateway site. The branch site may or may not also connect to the internet through one or more DIA interfaces.
- The gateway site has internet exits that use the transport VPN (VPN 0) through one or more interfaces.

Configure Cloud onRamp for SaaS

The following sections describe configuration procedures for Cloud OnRamp for SaaS features.

Enable Cloud OnRamp for SaaS, Cisco IOS XE SD-WAN Devices

You can enable Cloud OnRamp for SaaS in your Cisco SD-WAN overlay network on sites with Direct Internet Access (DIA) and on DIA sites that access the internet. You can also enable Cloud OnRamp for SaaS on client sites that access the internet through another site in the overlay network, called a gateway site. Gateway sites can include regional data centers or carrier-neutral facilities. When you enable Cloud OnRamp for SaaS on a client site that accesses the internet through a gateway, you also enable Cloud OnRamp for SaaS on the gateway site.

Note You can only enable Cloud OnRamp for SaaS features using the Cisco vManage procedures described in this document. We do not support configuring Cloud OnRamp for SaaS using CLI templates. Even when you configure other features on a device using a CLI template, you must nevertheless use Cisco vManage for configuring Cloud OnRamp for SaaS features.

Enable Cloud OnRamp for SaaS

1. From the Cisco vManage menu, choose **Administration** > **Settings**.
2. Click **Edit**, next to **Cloud onRamp for SaaS**.

3. In the **Cloud onRamp for SaaS** field, click **Enabled**.
4. Click **Save**.

Configure Applications for Cloud onRamp for SaaS Using Cisco vManage

1. Open Cloud onRamp for Saas.
   - From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**.

     or

   - In Cisco vManage, click the cloud icon near the top right and choose **Cloud onRamp for SaaS**.

2. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**.

   The **Applications and Policy** window displays all SaaS applications.

3. Optionally, you can filter the list of applications by clicking an option in the **App Type** field.
   - **Standard**: Applications included by default for Cloud onRamp for SaaS.
   - **Custom**: User-defined SaaS application lists (see Information About SaaS Application Lists).

4. Enable applications and configure.

Column	Description
Applications	Applications that can be used with Cloud onRamp for SaaS.
Monitoring	**Enabled**: Enables Cloud OnRamp for SaaS to initiate the Quality of Experience probing to find the best path. **Disabled**: Cloud onRamp for SaaS stops the Quality of Experience probing for this application.
VPN	(Cisco vEdge devices) Specify one or more VPNs.

Column	Description
Policy/Cloud SLA	(Cisco IOS XE SD-WAN devices) Select **Enable** to enable Cloud onRamp for SaaS to use the best path for this application. **Note** You can select **Enable** only if there is a centralized policy that includes an application-aware policy has been activated.
	(Cisco IOS XE SD-WAN devices) For Microsoft 365 (M365), select one of the following to specify which types of M365 traffic to include for best path determination: • **Optimize**: Include only M365 traffic categorized by Microsoft as “optimize” – the traffic most sensitive to network performance, latency, and availability. • **Optimize and Allow**: Include only M365 traffic categorized by Microsoft as “Optimize” or “Allow”. The “Allow” category of traffic is less sensitive to network performance and latency than the “Optimize” category. • **All**: Include all M365 traffic.
	Starting from Cisco IOS XE Release 17.5.1a, you can choose the service area that your M365 application belongs to. This allows you to apply the policy to only those applications in the specified service area. Microsoft allows the following service area options: • **Common**: M365 Pro Plus, Office in a browser, Azure AD, and other common network endpoints. • **Exchange**: Exchange Online and Exchange Online Protection. • **SharePoint**: SharePoint Online and OneDrive for Business. • **Skype**: Skype for Business and Microsoft Teams. See the Microsoft documentation for information about updates to the service areas.

5. Click **Save Applications and Next**.

   The **Application Aware Routing Policy** window appears, showing the application-aware policy for the current active centralized policy.

   - You can select the application-aware policy and click **Review and Edit** to view the policy details. The match conditions of the policy show the SaaS applications for which monitoring has been enabled.
   - For an existing policy, you cannot edit the site list or VPN list.
   - You can create a new policy for sites that are not included in existing centralized policies. If you create a new policy, you must add a VPN list for the policy.
   - You can delete one or more new sequences that have been added for the SaaS applications, or change the order of the sequences.

6. Click **Save Policy and Next**. This saves the policy to the Cisco vSmart Controller.

Configure Sites for Cloud onRamp for SaaS Using Cisco vManage

Configure two types of sites:

- Client sites
- Direct internet access (DIA) sites

Configure Client Sites

To configure Cloud OnRamp for SaaS on client sites that access the internet through gateways, configure Cloud OnRamp for SaaS both on the client sites and on the gateway sites.

Note You cannot configure Cloud OnRamp for SaaS with Point-to-Point Protocol (PPP) interface on the gateway sites.

Client sites in the Cloud onRamp service choose the best gateway site for each application to use for accessing the internet.

1. From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**. The **Cloud OnRamp for SaaS** Dashboard appears.
2. Click **Manage Cloud OnRamp for SaaS** and choose **Client Sites**. The page displays the following elements:
   - Attach Sites: Add client sites to Cloud onRamp for SaaS service.
   - Detach Sites: Remove client sites from Cloud onRamp for SaaS service.
   - Client sites table: Display client sites configured for Cloud onRamp for SaaS service.
3. On the **Cloud onRamp for SaaS** > **Manage Sites** window, click **Attach Sites**. The **Attach Sites** dialog box displays all sites in the overlay network with available sites highlighted. For a site to be available, all devices at that site must be running in vManage mode.
4. Choose one or more client sites from **Available Sites** and move them to **Selected Sites**.
5. Click **Attach**. The Cisco vManage NMS saves the feature template configuration to the devices. The Task View window displays a Validation Success message.
6. From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS** to return to the Cloud OnRamp for SaaS Dashboard screen.
7. Click **Manage Cloud OnRamp for SaaS** and choose **Gateways**. The page displays the following elements:
   - Attach Gateways: Attach gateway sites.
   - Detach Gateways: Remove gateway sites from the Cloud onRamp service.
   - Edit Gateways: Edit interfaces on gateway sites.

- Gateways table: Display gateway sites configured for Cloud onRamp service.

8. In the **Manage Gateways** window, click **Attach Gateways**. The **Attach Gateways** dialog box displays all sites in your overlay network with available sites highlighted. For a site to be available, all devices at that site must be running in vManage mode.

9. In the **Device Class** field, choose one of the following operating systems:

   - **Cisco OS**: Cisco IOS XE SD-WAN devices

   - **Viptela OS (vEdge)**: Cisco vEdge devices

10. Choose one or more gateway sites from **Available Sites** and move them to **Selected Sites**.

11. (Cisco vEdge devices for releases before Cisco IOS XE Release 17.7.1a) To specify GRE interfaces for Cloud OnRamp for SaaS to use, perform the actions in Steps 11a through 11d.

    (Cisco vEdge devices for releases from Cisco IOS XE Release 17.7.1a) To specify the VPN 0 interfaces or service VPN interfaces in gateway sites for Cloud OnRamp for SaaS to use, perform the actions in Steps 11a through 11d.

Note If you do not specify interfaces for Cloud OnRamp for SaaS to use, the system selects a NAT-enabled physical interface from VPN 0.

   a. Click **Add interfaces** to selected sites (optional), located in the bottom-right corner of the **Attach Gateways** window.

   b. Click **Select Interfaces**.

   c. From the available interfaces, choose the GRE interfaces to add (for releases before Cisco IOS XE Release 17.7.1a), or the VPN 0 interfaces or service VPN interfaces to add (for releases from Cisco IOS XE Release 17.7.1a).

   d. Click **Save Changes**.

12. (Cisco IOS XE SD-WAN devices) To configure the routers at a gateway site, perform the following steps.

Note If you don’t specify interfaces for Cloud OnRamp for SaaS, an error message indicates that the interfaces aren’t VPN 0.

   a. Click **Add interfaces to selected sites**.

   b. The **Attach Gateways** window shows each WAN edge router at the gateway site.

      Beginning with Cisco IOS XE Release 17.6.1a, you can choose Service VPN or VPN 0 if the gateway uses Cisco IOS XE SD-WAN devices.

      - If the routers at the gateway site connect to the internet using service VPN connections (VPN 1, VPN 2, …), choose **Service VPN**.

      - If the routers at the gateway site connect to the internet using VPN 0, choose **VPN 0**.

Note

- Correctly choosing **Service VPN** or **VPN 0** requires information about how the gateway site connects to the internet.
- All WAN edge routers at the gateway site must use either service VPN or VPN 0 connections for internet access. Cloud OnRamp for SaaS does not support a mix of both.

c. Do one of the following:

- If you chose **Service VPN**, then for each WAN edge router, choose the interfaces to use for internet connectivity.
- If you chose **VPN 0**, then either choose **All DIA TLOC**, or choose **TLOC list** and specify the colors to include in the TLOC list.

d. Click **Save Changes**.

13. Click **Attach**. Cisco vManage saves the feature template configuration to the devices. The Task View window displays a Validation Success message.
14. To return to the Cloud OnRamp for SaaS Dashboard, from the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**.

Edit Interfaces on Gateway Sites

1. Select the sites you want to edit and click **Edit Gateways**.
2. In the **Edit Interfaces of Selected Sites** window, select a site to edit.
   - To add interfaces, click the **Interfaces** field to select available interfaces.
   - To remove an interface, click the **X** beside its name.
3. Click **Save Changes** to push the template to the device(s).

Configure Direct Internet Access (DIA) Sites

Note Cloud onRamp for SaaS requires an SD-WAN tunnel to each physical interface to enable SaaS probing through the interface. For a physical interface configured for DIA only, without any SD-WAN tunnels going to the SD-WAN fabric, configure a tunnel interface with a default or any dummy color in order to enable use of Cloud onRamp for SaaS. Without a tunnel interface and color configured, no SaaS probing can occur on a DIA-only physical interface.

1. From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**.
2. From the **Manage Cloud OnRamp for SaaS** drop-down list, located to the right of the title bar, choose **Direct Internet Access (DIA) Sites**.

   The **Manage DIA**window provides options to attach, detach, or edit DIA sites, and shows a table of sites configured for the Cloud onRamp service.

3. Click **Attach DIA Sites**. The **Attach DIA Sites** dialog box displays all sites in your overlay network with available sites highlighted. For a site to be available, all devices at that site must be running in vManage mode.

4. In the **Device Class** field, select one of the following:
   - **Cisco OS**: Cisco IOS XE SD-WAN devices
   - **Viptela OS (vEdge)**: Cisco vEdge devices

5. Choose one or more DIA sites from **Available Sites** and move them to **Selected Sites**.

6. (For Cisco vEdge devices) By default, if you don't specify interfaces for Cloud OnRamp for SaaS to use, the system selects all NAT-enabled physical interfaces from VPN 0. Use the following steps to specify particular interfaces for Cloud OnRamp for SaaS.

   Note You can't select a loopback interface.

   a. Click the link, **Add interfaces to selected sites** (optional), located in the bottom-right corner of the window.

   b. In the **Select Interfaces** drop-down list, choose interfaces to add.

   c. Click **Save Changes**.

7. (For Cisco IOS XE SD-WAN devices, optional) Specify TLOCs for a site.

   Note Configuring Cloud onRamp for SaaS when using a loopback as a TLOC interface is not supported.

   Note If you do not specify TLOCs, the **All DIA TLOC** option is used by default.

   a. Click the **Add TLOC to selected sites** link at the bottom-right corner of the **Attach DIA Sites** dialog box.

   b. In the **Edit Interfaces of Selected Sites** dialog box, choose **All DIA TLOC**, or **TLOC List** and specify a TLOC list.

   c. Click **Save Changes**.

8. Click **Attach**. The Cisco vManage NMS saves the feature template configuration to the devices. The **Task View** window displays a Validation Success message.

9. To return to the Cloud OnRamp for SaaS Dashboard, from the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**.

Edit Interfaces on Direct Internet Access (DIA) Sites

1. Select the sites to edit and click **Edit DIA Sites**.

2. (Cisco vEdge devices) On the **Edit Interfaces of Selected Sites** screen, select a site to edit.
    - To add interfaces, click the **Interfaces** field to select available interfaces.
    - To remove an interface, click the **X** beside its name.

3. (Cisco IOS XE SD-WAN devices) In the **Edit Interfaces of Selected Sites** dialog box, do the following:
    a. Click **All DIA TLOC** to include all TLOCs, or click **TLOC List** to select specific TLOCs.

4. Click **Save Changes** to push the new template to the devices.

To return to the Cloud OnRamp for SaaS Dashboard, select **Configuration** > **Cloud onRamp for SaaS**.

Verify Cloud onRamp for SaaS

The following section(s) describe the procedures for verifying Cloud OnRamp for SaaS features.

Verify That an Application is Enabled for Cloud onRamp for SaaS

1. From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**.
2. Click **Manage Cloud OnRamp for SaaS** and choose **Applications and Policy**.

    The **Applications and Policy** window displays all SaaS applications.
3. In the row of the application that you are verifying, check that the **Monitoring** column and the **Policy/Cloud SLA** column both show **Enabled**.

Monitor Cloud onRamp for SaaS

The following section(s) describe the procedures for monitoring Cloud OnRamp for SaaS features.

View Details of Monitored Applications

1. Open Cloud onRamp for SaaS.
    - From the Cisco vManage menu, choose **Configuration** > **Cloud onRamp for SaaS**.

      or
    - In Cisco vManage, click the cloud icon at the top right and click **Cloud onRamp for SaaS**.

    The page includes a tile for each monitored application, with the following information:
    - How many sites are operating with Cloud onRamp for SaaS.
    - A color-coded rating of the Quality of Experience (vQoE) score for the application (green=good score, yellow=moderate score, red=poor score) on the devices operating at each site.

2. Optionally, you can click a tile to show details of Cloud onRamp for SaaS activity for the application, including the following:

Field	Description
vQoE Status	A green checkmark indicates that the vQoE score for the best path meets the criteria of an acceptable connection. The vQoE is calculated based on average loss and average latency. For Office 365 traffic, other connection metrics are also factored in to the vQoE score.
vQoE Score	For each site, this is the vQoE score of the best available path for the cloud application traffic. The vQoE score is determined by the Cloud onRamp for SaaS probe. Depending on the type of routers at the site, you can view details of the **vQoE Score** as follows: • Cisco IOS XE SD-WAN devices: To show a chart of the vQoE score history for each available interface, click the chart icon. In the chart, each interface vQoE score history is presented as a colored line. A solid line indicates that Cloud onRamp for SaaS has designated the interface as the best path for the cloud application at the given time on the chart. You can place the cursor over a line, at a particular time on the chart, to view details of the vQoE score of an interface at that time. From Cisco vManage Release 20.8.1, for the Office 365 application, the chart includes an option to show the vQoE score history for a specific service area, such as Exchange, Sharepoint, or Skype. For each service area, a solid line in the chart indicates the interface chosen as the best path at a given time. If you have enabled Cloud onRamp for SaaS to use Microsoft traffic metrics for Office 365 traffic, the choice of best path takes into account the Microsoft traffic metrics. • Cisco vEdge devices: To show a chart of the vQoE score history, click the chart icon. The chart shows the vQoE score for the best path chosen by Cloud onRamp for SaaS.
DIA Status	The type of connection to the internet, such as local (from the site), or through a gateway site.
Selected Interface	The interface providing the best path for the cloud application. **Note** If the DIA status is Gateway, this field displays **N/A**.
Activated Gateway	For a site that connects to the internet through a gateway site, this indicates the IP address of the gateway site. **Note** If the DIA status is Local, this field displays **N/A**.

Field	Description
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. **Note** If the DIA status is Local, this field displays **N/A**.
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. **Note** If the DIA status is Local, this field displays **N/A**.
SDWAN Computed Score	This field is applicable only if the site uses Cisco IOS XE SD-WAN devices. It does not apply for Cisco vEdge devices. From Cisco vManage Release 20.8.1, for the Microsoft Office 365 application, an **SDWAN Computed Score** column provides links to view charts of the path scores (OK, NOT-OK, or INIT) provided by Microsoft telemetry for each Microsoft service area, including Exchange, Sharepoint, and Skype. The chart shows the scores over time for each available interface. The scores are defined as follows: • **OK**: Acceptable path • **NOT-OK**: Unacceptable path • **INIT**: Insufficient data These charts provide visibility into how Cloud onRamp for SaaS chooses a best path for each type of Microsoft Office 365 traffic. A use case for viewing the path score history is for determining whether Microsoft consistently rates a particular interface as NOT-OK for some types of traffic, such as Skype traffic.