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 Release 20.3.1 to Cisco Catalyst SD-WAN Release 20.14.x

Table 1: Feature History

Feature Name	Release Information	Description
Support for Specifying Office 365 Traffic Categories for Cloud OnRamp for SaaS on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature updates the existing Cloud OnRamp for SaaS configuration workflow for Cisco IOS XE Catalyst SD-WAN devices. The feature allows you to limit the use of best path selection to some or all Office 365 traffic, according to the Office 365 traffic categories defined by Microsoft.

Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Release 20.3.1 to Cisco Catalyst SD-WAN Release 20.14.x

Feature Name	Release Information	Description
Application Feedback Metrics for Office 365 Best Path Selection on Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a Cisco vManage Release 20.4.1	This feature adds new metrics as inputs to the best-path selection algorithm for Office 365 traffic. The new inputs include best-path metrics from Microsoft Cloud Services. The feature also provides a new page for viewing detailed logs of the input data used by the best path algorithm.
Load Balancing Across Multiple Interfaces	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco vManage Release 20.5.1	This feature adds the ability to balance traffic for cloud applications across multiple DIA interfaces.
Support for Cloud OnRamp for SaaS Probing through VPN 0 Interfaces at Gateway Sites	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	Cloud OnRamp for SaaS tests the performance of (probes) routing paths to find the best routing path for specific cloud application traffic. Using the best routing path for the traffic of a cloud application optimizes the performance of the application. This feature enables Cloud OnRamp for SaaS to probe through VPN 0 interfaces at gateway sites as part of determining the best path to use for the traffic of specified cloud applications. This extends the best path probing to include more of the available interfaces connected to the internet. Using this feature, Cloud OnRamp for SaaS can probe interfaces at a gateway site, whether they use service VPNs (VPN 1, VPN 2, and so on) or the transport VPN (VPN 0). This is helpful when a branch site connects to the internet, exclusively or in part, through a gateway site that uses a VPN 0 interface to connect to the internet.
Cloud OnRamp for SaaS Support for Webex	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco vManage Release 20.7.1	This feature adds Webex to the list of cloud applications supported by Cloud OnRamp for SaaS. Cloud OnRamp for SaaS can determine the best network path to Webex cloud servers. Cisco SD-WAN Manager periodically downloads a list of Webex servers organized by geographic region. Cloud OnRamp for SaaS uses this server list to help calculate the best network path for Webex traffic in different regions.
Support for Using Microsoft Telemetry Metrics for Microsoft 365 SharePoint and Teams Traffic.	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1	This feature adds support for using Microsoft telemetry metrics for Microsoft 365 SharePoint and Teams. Cloud OnRamp for SaaS uses the metrics data when determining the best path for Office 365 traffic.

Cloud OnRamp for SaaS, Cisco Catalyst SD-WAN Release 20.3.1 to Cisco Catalyst SD-WAN Release 20.14.x

Feature Name	Release Information	Description
View Details of Microsoft Telemetry and View Application Server Information for Office 365 Traffic	Cisco IOS XE Catalyst SD-WAN Release 17.8.1a 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 Catalyst SD-WAN receives from Microsoft Cloud.
Configure the Traffic Category and Service Area for Specific Policies	Cisco vManage Release 20.9.1 Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	You can edit AAR policies individually to change the specified Microsoft 365 traffic category and service area for specific AAR policies.
Enable Cloud OnRamp for SaaS Operation for Specific Applications at Specific Sites	Cisco vManage Release 20.9.1 Cisco IOS XE Release 17.2.1	This feature allows you to selectively delete AAR policy sequences to exclude Cloud OnRamp for SaaS operation on specific applications at specific sites.
Improved Visibility for Microsoft 365 Traffic	Cisco vManage Release 20.9.1 Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This feature provides improved visibility to allow you to monitor the details of Microsoft 365 traffic processed by Cloud OnRamp for SaaS.
Option to Include or Exclude Microsoft Telemetry Data from Best Path Decision for Microsoft 365 Traffic	Cisco vManage Release 20.9.1	This feature allows you to choose whether Cloud OnRamp for SaaS should factor in the Microsoft telemetry data in the best path decision. If you disable this option, you can still view the Microsoft telemetry data in the Cisco SD-WAN Analytics dashboard, but it does not affect the best path decision.

Feature Name	Release Information	Description
Improved Visibility and Control of Webex Traffic	Cisco vManage Release 20.10.1 Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This feature introduces several improvements to the visibility and control of Webex traffic, including the following: • Using Cisco SD-AVC to manage deep packet inspection (DPI) of Webex traffic • Receiving server-side Webex metrics to provide detailed information about Webex traffic performance • Adding only a single sequence to application-aware routing (AAR) policies to enable Cloud OnRamp for SaaS for Webex traffic
Add Cloud OnRamp for SaaS Support for Loopback, Dialer, and Subinterfaces	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Control Components Release 20.13.1	This feature extends the Cloud OnRamp for SaaS support to SD-WAN supported WAN interfaces that includes loopback, dialer, and subinterfaces. It also adds support for TLOC-extension and SIG on loopback, dialer, and subinterfaces.
Option to Exclude Data Prefixes from Cloud OnRamp for SaaS Optimization	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Control Components Release 20.13.1	You can define a list of IP prefixes to exclude from Cloud OnRamp for SaaS optimization. This is useful when SaaS applications are hosted on-premises or in a private cloud.
Enable Faster Failover by Associating a DIA Tracker with Cloud OnRamp for SaaS	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Control Components Release 20.13.1	To enable faster failover from a failed route, you can associate a tracker to a DIA or gateway site. The tracker detects internet connectivity failure on an interface faster than Cloud OnRamp for SaaS probing.

Information About Cloud OnRamp for SaaS

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 Catalyst 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.

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.

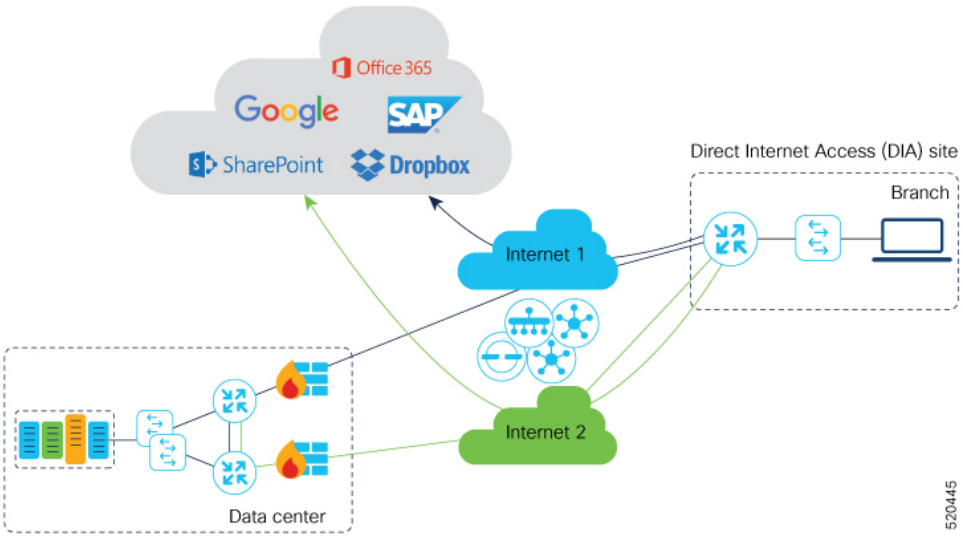
- Cloud OnRamp determining best path

  Cloud OnRamp for SaaS selects the best connection for each SaaS application through the local DIA links that are configured and available. For Cloud OnRamp for SaaS, a DIA link is considered unavailable in various conditions—for example, loss of more than 90% of probe packets.

- Cloud OnRamp not determining best path

  If Cloud OnRamp for SaaS determines that no local DIA paths are available for an application, the traffic follows the path determined by other routing features on the site.

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.



Overview of the configuration tasks:

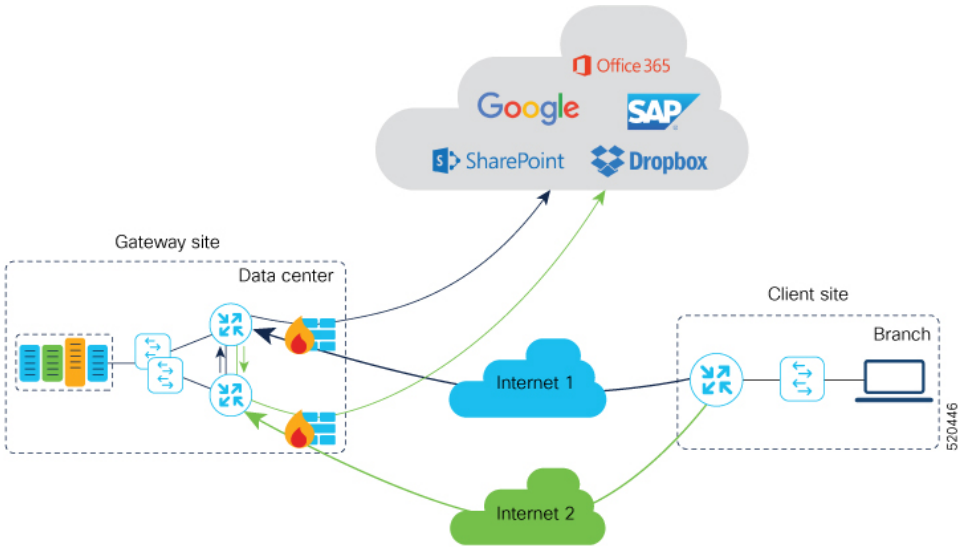
Enable Cloud OnRamp for SaaS, select the applications for which Cloud OnRamp for SaaS will find the best-performing path, choose the policy to steer traffic through the best-performing path, and associate the policy with DIA sites.

1. Enable Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Devices, on page 24
2. Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager, on page 24
3. Configure Direct Internet Access (DIA) Sites, on page 34

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, Cisco Catalyst 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.



Overview of the configuration tasks:

Enable Cloud OnRamp for SaaS, select the applications for which Cloud OnRamp for SaaS will find the best-performing path, choose the policy to steer traffic through the best-performing path, and associate the policy with client sites and gateway sites.

1. Enable Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Devices, on page 24
2. Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager, on page 24
3. Configure Client Sites, on page 29
4. Edit Interfaces on Gateway Sites, on page 32

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

Overview of the configuration tasks:

Enable Cloud OnRamp for SaaS, select the applications for which Cloud OnRamp for SaaS will find the best-performing path, choose the policy to steer traffic through the best-performing path, and associate the policy with DIA sites and gateway sites.

1. Enable Cloud OnRamp for SaaS, Cisco IOS XE Catalyst SD-WAN Devices, on page 24
2. Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager, on page 24
3. Configure Direct Internet Access (DIA) Sites, on page 34
4. Edit Interfaces on Gateway Sites, on page 32

Specify Office 365 Traffic Category

When enabling Cloud OnRamp for SaaS to manage Office 365 traffic, you can limit Cloud OnRamp for SaaS path selection to apply to some or all Office 365 traffic, with the following options:

- **Optimize** traffic
- **Optimize** and **Allow** traffic
- All Office 365 traffic

These options correspond to the three categories of Office 365 traffic that Microsoft defines as follows:

- **Optimize**: Traffic most sensitive to network performance, latency, and availability.
- **Allow**: Traffic less sensitive to network performance, latency, and availability.
- **Default**: Traffic not sensitive to network performance.

Specifying traffic by Office 365 category requires enabling the Cisco SD-AVC Cloud Connector component in **Administration** > **Settings**.

Best path determination

Cloud OnRamp for SaaS selects the best path for each application using an algorithm that takes input from the sources shown in the table. The algorithm chooses among the configured and available Cloud OnRamp internet egress options for an application, such as local DIA egress or gateway site internet egress. The vQoE status and vQoE score displayed on the monitoring page are monitoring indicators and are not failover thresholds. They do not directly influence the Cloud OnRamp for SaaS determination of best path.

	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)

For Office 365 traffic, you can view a log of the metrics that factor into the best-path determination. The metrics appear in a Cisco SD-WAN Analytics page specifically designed to display only this information, and available directly from Cisco SD-WAN Manager.

Load Balancing Across Multiple Interfaces

Cloud OnRamp for SaaS can determine the best network path for each type of cloud traffic. However, if multiple direct internet access (DIA) interfaces on a WAN edge device at a branch site provide acceptable performance for a cloud application, Cloud OnRamp for SaaS can employ load balancing across up to three interfaces to further improve performance.

When you enable load balancing across multiple interfaces of a WAN edge device, load balancing is enabled for all cloud applications that are managed by Cloud OnRamp for SaaS. After determining the best path

interface for a cloud application, Cloud OnRamp compares the performance statistics for other interfaces. To use another interface for load balancing, the following must be true:

- The packet loss value of the interface cannot vary from the packet loss value of the best path interface by more than a configured value (%). You can configure a smaller value to restrict load balancing only to interfaces with a packet loss value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher packet loss than the best path interface.
- The latency value of the interface cannot vary from the latency value of the best path interface by more than a configured value (milliseconds). You can configure a smaller value to restrict load balancing only to interfaces with a latency value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher latency than the best path interface.

If required, you can select an option to ensure that all traffic from a single host uses a single interface – for example, to ensure that DNS and application traffic use the same path.

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

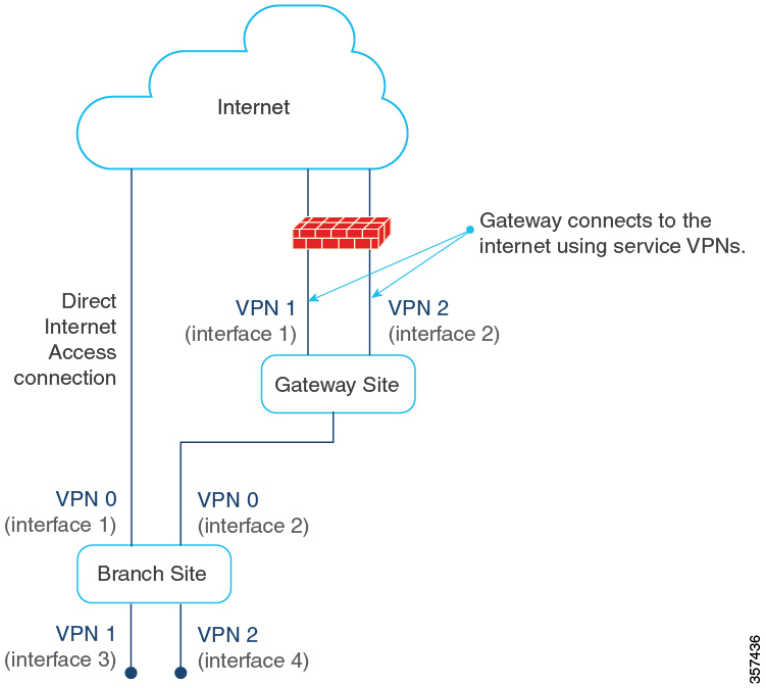
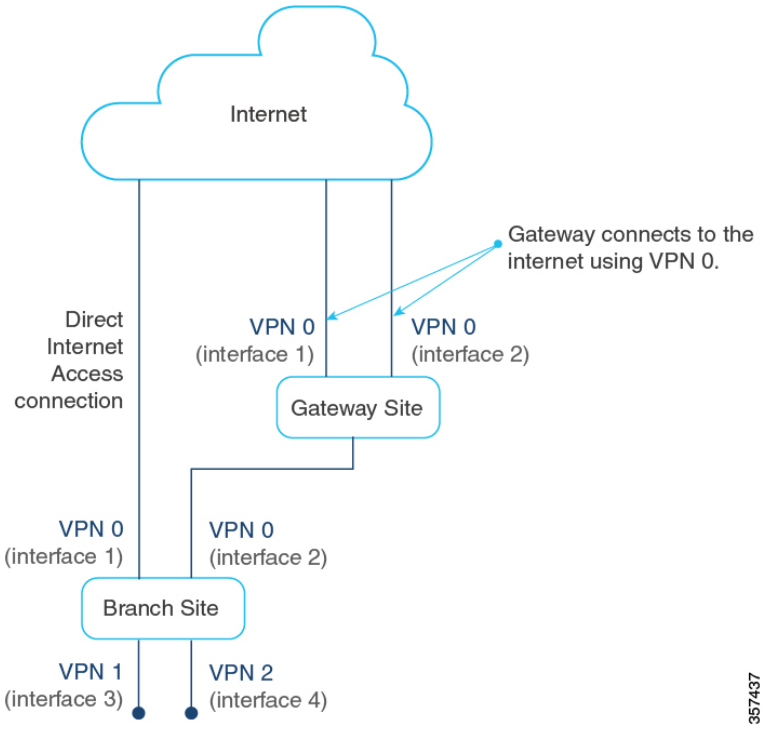


Figure 2: Branch Site Connects to a Gateway Site That Uses VPN 0 to Connect to the Internet



Information About Cloud OnRamp for SaaS Support for Webex

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

When you enable Cloud OnRamp for SaaS best path determination for an application, Cisco SD-WAN Manager updates match conditions in the application-aware policy in the active centralized policy to support Cloud OnRamp for SaaS functionality for the application. For most applications, the match conditions do not require any later update.

For Webex, Cloud OnRamp for SaaS uses a more complex method than for most other applications. Cloud OnRamp for SaaS maintains a list of worldwide Webex servers. When you enable Cloud OnRamp for SaaS best path determination for Webex, Cloud OnRamp for SaaS determines the best path for each Webex server worldwide. It adds match conditions in the application-aware policy to address each of the regional Webex servers. This provides the Webex application with the best path to any Webex server worldwide that it may need to connect to.

In the Cisco SD-WAN Release 20.9.1 Cloud OnRamp for SaaS Support for Webex, when a Webex API response contains `provider_reserved`, it will result in a `sync push failed` response.

When this issue occurs in a customer deployment:

- New Deployments: Customers need to upgrade to the latest 20.9 version or 20.12+.
- Existing Deployments: Customers need to upgrade to the latest 20.9 version or 20.12+. If an upgrade is not an option, please contact TAC.

Table 2: Best Path Determination Method for Webex, Compared with the Method for Other Applications

Application	Cloud OnRamp for SaaS Method
Most cloud applications	Cloud OnRamp for SaaS determines the best path to the most relevant server for the cloud application, as determined by the DNS response, using the DNS server configured for the device.
Webex	Cloud OnRamp for SaaS maintains a list of worldwide Webex servers, and determines the best path for all available Webex servers.

Maintaining an Up-to-Date List of Webex Servers

To maintain an up-to-date list of Webex servers, Cisco SD-WAN Manager periodically retrieves the latest server information and determines whether there are any changes to the information. If Cisco SD-WAN Manager detects that there are changes to the Webex server information, it displays notifications on the Cloud OnRamp for SaaS dashboard, prompting you to synchronize the Webex server information. The notifications are shown in a dialog box that appears on the Cloud OnRamp for SaaS dashboard page, and in a message in the Webex application pane that appears on the dashboard.

Classifying Traffic with SD-AVC

Beginning with Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Cloud OnRamp for SaaS uses Cisco SD-AVC to manage deep packet inspection (DPI) of Webex traffic, enabling first-packet classification of the traffic. This requires enabling SD-AVC in **Administration** > **Settings**.

Classifying Webex traffic flows from the first packet enables Cloud OnRamp for SaaS control policy to act on more of the Webex traffic handled by a router.

One benefit to using SD-AVC for DPI is that it resolves a known issue that could cause some Webex traffic to use a sub-optimal path to cloud servers. The scenario is that Webex servers in one geographical region might use some of the same IP addresses as Webex servers in a different region. In previous releases, this IP overlap could cause Webex traffic destined for one geographical region to use the edge device interface that is optimal for traffic to a different region. The traffic flow operated correctly, reaching the correct destination, but the traffic used a non-optimal path. In Cisco vManage Release 20.10.1, this is resolved.

Simplified Application-Aware Routing Policy

Beginning with Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, when you enable Cloud OnRamp for SaaS to operate on Webex traffic, Cisco SD-WAN Manager adds only a single sequence to application-aware routing (AAR) policies, rather than a series of sequences, as in earlier releases. Cisco Catalyst SD-WAN continues to support existing legacy AAR policies that use more sequence statements to enable Cloud OnRamp for SaaS for Webex.

If you are using a legacy AAR policy (that uses numerous sequences to enable Cloud OnRamp for SaaS for Webex traffic), disabling Webex in Cloud OnRamp for SaaS removes the series of sequences that address Webex traffic from the AAR policy. If you re-enable Webex, Cloud OnRamp for SaaS uses the newer, more efficient method of adding only a single sequence to the AAR policy.

For information about restrictions related to the new policy model, see Restrictions for the Webex Application, on page 22.

Webex Server-Side Metrics

Beginning with Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, Webex servers can provide metrics to Cisco SD-WAN Analytics describing the the performance of different facets of Webex traffic, such as audio, video, and so on. The metrics augment the traffic metrics that Cloud OnRamp for SaaS collects using path probes to determine metrics such as loss and latency. The aggregated information from Webex servers and from probing provides a valuable tool for understanding Webex traffic performance in your network. For information about viewing the aggregated metrics, see View Details of Monitored Applications, on page 46.

Cloud OnRamp for SaaS does not use the metrics data when determining the best path for Webex traffic. See Prerequisites for Webex Server-Side Metrics, on page 19, and Enable Webex Server-Side Metrics.

Information About the SD-AVC Cloud Connector

Minimum supported release: Cisco vManage Release 20.8.1

Cisco Catalyst SD-WAN uses a component called SD-AVC Cloud Connector to collect information from Microsoft Cloud about the Microsoft application servers that handle Office 365 traffic. The information includes the transport protocols for the traffic; and the domain names, IP addresses, and ports of the application servers that manage the traffic. This server information improves the process of identifying network traffic—for example, making it possible to identify traffic from the first packet. Improving traffic identification enhances the effectiveness of application-aware routing policies because policies can often match all traffic, from the first packet.

The **SD-AVC Cloud Connector** page provides visibility into the application servers that are used for Office 365 traffic. It provides a table of the server information that Cisco Catalyst SD-WAN has collected for Office 365 traffic. For example, the table may indicate that the domains represented by *-admin.sharepoint.com correspond to Sharepoint traffic. In this case, any traffic flow with a destination domain included in those domains, such as connect-admin.sharepoint.com, can be identified as Sharepoint traffic from the first packet of the flow.

Information About Viewing Path Scores for Office 365 Traffic

Minimum supported release: Cisco vManage Release 20.8.1

For Office 365 traffic, you can view charts showing 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 path scores over time for each available interface.

Viewing the path score history can be useful when troubleshooting network performance issues for Office 365 traffic—for example, to determine whether Microsoft consistently rates a particular interface as NOT-OK for some types of traffic, such as Skype traffic. If that occurs, you can investigate why the interface is consistently receiving a low path score.

Information About Configuring the Traffic Category and Service Area for Specific Policies

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

When you enable Microsoft 365 on the **Applications and Policy** page, and choose a traffic category, Cloud OnRamp for SaaS adds sequences to all application-aware routing (AAR) policies to enable Cloud OnRamp for SaaS operation on Microsoft 365 traffic, in accordance with the traffic category that you have chosen. Adding these sequences to the AAR policies enables Cloud OnRamp for SaaS operation on this traffic, with the selected traffic category.

Starting from Cisco vManage Release 20.9.1, you can edit the sequences in AAR policies individually to change the specified Microsoft 365 traffic category and service area for specific AAR policies.

Note This feature is only available for the Microsoft 365 application.

Benefits of Configuring the Traffic Category and Service Area for Specific Policies

By editing individual AAR policies, you can enable Cloud OnRamp for SaaS to operate on different Microsoft 365 service areas and traffic categories in different policies.

Information About Enabling Cloud OnRamp for SaaS Operation for Specific Applications at Specific Sites

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Release 17.2.1

Starting from Cisco vManage Release 20.9.1, you can selectively enable Cloud OnRamp for SaaS to operate for a particular application at specific sites, while excluding other sites. When you enable an application on the **Applications and Policy** page, Cloud OnRamp for SaaS adds AAR policy sequences that match traffic for the selected application and direct the traffic in accordance with the Cloud OnRamp for SaaS best path calculation. This has the effect of enabling Cloud OnRamp for SaaS operation at all sites.

To exclude Cloud OnRamp for SaaS operation for applications at specific sites, you can edit an AAR policy and delete a specific application within the AAR policy. This disables Cloud OnRamp for SaaS activity for that application on sites that use the AAR policy.

In contrast to editing the traffic category or service area for specific policies (see Information About Configuring the Traffic Category and Service Area for Specific Policies), which works only with Microsoft 365 traffic, you can use this feature to enable or exclude any SaaS application.

Benefits of Enabling Cloud OnRamp for SaaS Operation for Specific Applications at Specific Sites

This feature enables granular, site-level control of applications that Cloud OnRamp for SaaS operates on at each site in the network.

Information About Visibility for Microsoft 365 SaaS Traffic

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Cisco vManage Release 20.9.1 introduces improved application visibility, enabling you to monitor Microsoft 365 traffic processed by Cloud OnRamp for SaaS in more detail. You can view, in graph or table formats, the volume of Microsoft 365 traffic over time, with details as to how much traffic used a direct internet access (DIA) link, and how much was routed through a gateway site. The monitoring page also shows the volume of traffic that Cloud OnRamp for SaaS does not affect.

Benefits of Visibility for Microsoft 365 SaaS traffic

Visibility into the details of how Cloud OnRamp for SaaS is routing traffic can be helpful when troubleshooting traffic routing issues.

Information About Including or Excluding Microsoft Telemetry Data from the Best Path Decision for Microsoft 365 Traffic

Minimum releases: Cisco vManage Release 20.9.1

From Cisco vManage Release 20.9.1, you can control whether the Cloud OnRamp for SaaS best path decision includes Microsoft telemetry data as a factor for Microsoft 365 traffic. When enabling telemetry for Microsoft 365 (Office 365) traffic, the **Application Feedback** dialog box contains a **Traffic Steering** check box. Check this check box to enable the use of Microsoft telemetry data in best path decisions. For information, see Enable Application Feedback Metrics for Office 365 Traffic.

Even when you elect not to use Microsoft telemetry data in best path decisions, you can view the telemetry data. You can view the telemetry data related to the Microsoft 365 application, as well as detailed information about the best path decisions made on devices, using Cisco vAnalytics. For information about Cisco SD-WAN Analytics, see Cisco vAnalytics.

For information about enabling Microsoft to provide telemetry for Microsoft 365 traffic, see Enable Microsoft to Provide Telemetry for Office 365 Traffic.

After Upgrading Cisco SD-WAN Manager

If you have enabled Microsoft telemetry on a previous release of Cisco SD-WAN Manager, and are now upgrading to Cisco vManage Release 20.9.1, Cloud OnRamp for SaaS does not automatically enable the use of Microsoft telemetry data in best path decisions. To ensure that devices use Microsoft telemetry for best path decisions, if you have configured that option, perform one of the following:

- Disable and enable Microsoft telemetry for Microsoft 365 traffic. See Enable Application Feedback Metrics for Office 365 Traffic

- Disable and enable monitoring for Microsoft 365 traffic. See Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager
- Perform the following steps:
  1. Detach and attach sites and gateways. See Configure Client Sites.
  2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.
  3. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**. The **Applications and Policy** page displays all SaaS applications.
  4. Click **Save Applications and Next**. This sends the traffic steering values to devices at each site.

Note From Cisco vManage Release 20.9.1, you can enter the public system IP of edge devices, on the Microsoft portal. For details, see step 2-c under Enable Microsoft to Provide Telemetry for Office 365 Traffic.

Information About Cloud OnRamp for SaaS Support for Loopback, Dialer, and Subinterfaces

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

Cloud OnRamp for SaaS supports loopback, dialer, and subinterfaces. You can configure TLOC-extension and SIG on these interfaces.

You can configure different interfaces on a Cisco IOS XE Catalyst SD-WAN device based on your requirements. For more information about configuring network interfaces, see Configure Network Interfaces.

For more information about supported Network Address Translation (NAT) configuration on loopback and dialer interfaces, see Configure NAT.

Information About Excluding Data Prefixes

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a , Cisco Catalyst SD-WAN Manager Release 20.13.1

You can define a list of destination IP prefixes to exclude from Cloud OnRamp for SaaS optimization. You can apply a data prefix exclusion list to all SaaS applications or individually to a specific application.

A common use is to exclude the prefixes of on-premises SaaS application servers or private-cloud-hosted SaaS application servers. For example, if you have local on-premises SharePoint servers and configure Cloud OnRamp for SaaS to optimize SharePoint traffic, you can exclude the prefixes for the local SharePoint servers from Cloud OnRamp for SaaS optimization. This enables the SharePoint traffic to be routed internally, unaffected by Cloud OnRamp for SaaS.

Information About Using a Tracker for Faster Failover

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

Cloud OnRamp for SaaS performs best-path determination using probes on all available interfaces. If internet connectivity on an interface fails, Cloud OnRamp for SaaS reroutes to another path, which is called failover. Detecting the failure might take some time. When relying on probes, it takes two to four minutes to detect internet connectivity failure on an interface.

To achieve a faster failover, you can configure a DIA tracker and associate it with a DIA or gateway site configured for Cloud OnRamp for SaaS. The tracker probes the transport interface periodically to determine if the internet or external network is unavailable. Associating a tracker with Cloud OnRamp for SaaS allows faster switching to an alternate path when the primary link for an application is unavailable.

The speed of a tracker or tracker group depends on the configuration of parameters such as threshold, interval, multiplier, and so on. For more information about the DIA tracker, see NAT DIA Tracker.

For information about previous support for faster failover when using Cloud OnRamp for SaaS over a SIG tunnel, see Information About Cloud OnRamp for SaaS Over SIG Tunnels, on page 52.

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.

Benefits of Cloud OnRamp for SaaS Support for Webex

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

By maintaining a list of worldwide Webex servers, and determining the best path for all available Webex servers, Cloud OnRamp for SaaS provides a high degree of path optimization for Webex traffic. Even if the Webex application connects to a distant cloud server, or connects to different servers at different times, Cloud OnRamp for SaaS always provides the best path to any Webex server worldwide.

Supported Devices for Cloud OnRamp for SaaS

Cisco IOS XE Catalyst 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 3: Device Feature Support

Feature	Cisco IOS XE Catalyst 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 vEdge devices, see Cloud OnRamp for SaaS, Cisco SD-WAN Release 20.3.1 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 Catalyst 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 Catalyst SD-WAN devices, the requirements are:

- The devices must be running Cisco IOS XE Catalyst SD-WAN Release 17.3.1a or later.
- The devices must be in Manager mode.
- All Cisco Catalyst SD-WAN Controller instances must be in Manager mode.
- A centralized policy that includes an application-aware policy must be activated. You can configure more than one centralized policy in Cisco SD-WAN Manager, 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**).

  From Cisco Catalyst SD-WAN Manager Release 20.13.1, Cloud OnRamp for SaaS is enabled by default. (**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.

Prerequisites for Cloud OnRamp for SaaS Support for Webex

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

- To download the latest information about Webex servers, as described in "Maintaining an Up-to-Date List of Webex Servers" in Information About Cloud OnRamp for SaaS Support for Webex, Cisco SD-WAN Manager requires access to the internet.
- When you enable Cloud OnRamp for SaaS to optimize Webex traffic, ensure that for each router, the service VPN has a default route configured. This default route is required for the Webex DNS and control traffic, which are components of Webex traffic that are not optimized by Cloud OnRamp for SaaS.
- Verify that SD-WAN Manager can reach this domain:

  https://info.net-int.infra.webex.com/v1/prefixes/regions

Prerequisites for Configuring the Traffic Category and Service Area for Specific Policies

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

- You must have multiple active AAR policies.
- To edit the service area and traffic category, you must enable **Monitoring** and **Policy/Cloud SLA** for the Microsoft 365 application. For information, see Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager.

Prerequisites for Enabling Cloud OnRamp for SaaS Operation for Specific Applications at Specific Sites

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Release 17.2.1

Availability of multiple AAR policies associated with different sets of sites.

Prerequisites for Visibility for Microsoft 365 SaaS Traffic

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

- Enable application visibility and flow visibility. For information, see Enable Application Visibility and Flow Visibility, on page 42.
- To view the graphical visualizations of traffic, and to view logs, enable on-demand troubleshooting. For information, see On Demand Troubleshooting in the *Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*.

Prerequisites for Including or Excluding Microsoft Telemetry Data from the Best Path Decision for Microsoft 365 Traffic

Minimum releases: Cisco vManage Release 20.9.1

Enable Microsoft traffic metrics.

See Enable Microsoft to Provide Traffic Metrics for Office 365 Traffic.

Prerequisites for Webex Server-Side Metrics

Minimum releases: Cisco vManage Release 20.10.1, Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

- Enable SD-AVC in **Administration** > **Settings**.
- Enable Cloud Services in **Administration** > **Settings**.
- Webex account (This is usually an account for your organization).
- Enable server-side metrics. See Enable Webex Server-Side Metrics, on page 38.

Prerequisites for Cloud OnRamp for SaaS Support on Loopback, Dialer, and Subinterfaces

Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a

To use a dialer interface for Cloud OnRamp for SaaS, the Point-to-Point Protocol (PPP) models associated with the DIA interface must support NAT DIA.

Prerequisites for Excluding a Data Prefix List for a Cloud OnRamp for SaaS Application

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

Before using or creating a destination data prefix list for a Cloud OnRamp for SaaS application, perform the following on the **Applications and Policy** page, for the application or applications for which you are excluding specific prefixes:

- Enable monitoring for the application.
- Enable Policy/Cloud SLA for the application.

Prerequisites for Faster Failover with a DIA Tracker

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

- Configure a tracker with a DNS name or an IP address of the endpoint on the DIA or gateway site where Cloud OnRamp for SaaS is enabled.
  - To configure a DIA tracker using a Cisco System feature template, see Configure NAT DIA Tracker on IPv4 Interfaces Using Feature Templates in Cisco SD-WAN Manager.
  - Devices on the site must have a tracker or tracker group associated with them.
  - You can configure an ICMP tracker using a CLI template. For more information about configuring an ICMP tracker, see Information About NAT DIA Tracking.
- Ensure the DIA interfaces are configured for Cloud OnRamp for SaaS before associating a tracker.

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

Restriction	Description
Loopback interface TLOC	Configuring Cloud OnRamp for SaaS when a site is using a loopback as a transport locator (TLOC) interface is not supported. From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cloud OnRamp for SaaS supports using loopback as a TLOC interface.
DNS server	Cloud OnRamp doesn't support if the name-server is reachable over SD-WAN tunnel (through OMP), DNS resolution will fail.

Restriction	Description
Dialer interface TLOC	From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cloud OnRamp for SaaS supports using dialer as a TLOC interface. For resctrictions related to dialer interfaces, see Restrictions for Using a Dialer Interface with NAT DIA.
VLAN interface TLOC	Configuring Cloud OnRamp for SaaS when a site is using VLAN as a TLOC interface is not supported.
Cellular interface TLOC	Configuring Cloud OnRamp for SaaS when a site is using cellular as a TLOC interface is not supported.
Application-aware policy	Configuring Cloud OnRamp for SaaS on Cisco IOS XE Catalyst SD-WAN device devices is only through centralized app-aware policy using match condition "cloud-saas-app-list" and action "cloud-saas". For mixed deployments including Cisco vEdge devices and Cisco IOS XE Catalyst SD-WAN devices, we recommend to have different app-aware policies for Cisco vEdge devices and Cisco IOS XE Catalyst SD-WAN devices.
ICMP traffic	Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and Cisco SD-WAN Release 20.8.1, Cloud OnRamp for SaaS does not support ICMP traffic. This has a minor effect on Webex traffic counters, as compared with Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco SD-WAN Release 20.7.1.
Configuration groups	You can configure Cloud OnRamp for SaaS using the methods described in the Configure Cloud OnRamp for SaaS, on page 24 section. Cloud OnRamp for SaaS does not support configuration using configuration groups.
NAT pool	Configuring Cloud OnRamp for SaaS with NAT pool mapping on DIA interface is not supported. Configuring Cloud OnRamp for SaaS with NAT pool mapping on DIA interface is supported from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and later.

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.

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.

Restrictions for the Webex Application

Beginning with Cisco vManage Release 20.10.1 and Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, when you enable Cloud OnRamp for SaaS to operate on Webex traffic, Cisco SD-WAN Manager uses a more efficient policy model, while still supporting existing legacy control policies that enable Cloud OnRamp for SaaS for Webex. If you disable the Webex application in Cloud OnRamp for SaaS, and then re-enable the Webex application, Cisco SD-WAN Manager can only use the newer policy model. Before disabling and then re-enabling the Webex application, ensure that devices in the network are using Cisco IOS XE Catalyst SD-WAN Release 17.10.1a or later, and that SD-AVC is enabled (in **Administration** > **Settings**).

Restrictions for Associating a Tracker with DIA and Gateway Sites

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

You can associate a tracker with a gateway site only if connectivity to the gateway site uses VPN 0, not a service VPN.

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.

Use Cases for the SD-AVC Cloud Connector

Minimum supported release: Cisco vManage Release 20.8.1

Visibility into server information is helpful when troubleshooting. For example, after creating a policy that applies Cloud OnRamp for SaaS only to Office 365 traffic in the Sharepoint service area, you might find that Cisco Catalyst SD-WAN is not routing the first few flows of Sharepoint traffic on the best path determined by Cloud OnRamp for SaaS, and Sharepoint performance is below expectations.

To troubleshoot, you can do the following:

1. Determine which server the Sharepoint traffic is using.
2. Open the SD-AVC Cloud Connector page and filter for the term, “sharepoint”.
3. Look for the Sharepoint server you found in the first step. If that server does not appear in the list, it means that Cloud OnRamp for SaaS is not classifying the traffic to that server as Sharepoint traffic. If it is not classified as Sharepoint traffic, it does not use the best path determined by Cloud OnRamp for SaaS for the first few flows.

Use Case for Configuring the Traffic Category and Service Area

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

An organization relies heavily on Microsoft 365 for its office applications and has configured Cloud OnRamp for SaaS to optimize Microsoft 365 traffic at its headquarters and at each branch office. In addition, it uses an on-premises Outlook server at a data center to handle its company email.

Microsoft distinguishes different types of Microsoft 365 traffic using the following service areas:

- Common: Microsoft 365 ProPlus, Office in a browser, Azure Active Directory (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

Because the organization uses an on-premises Outlook server, the network administrator chooses to exclude Outlook traffic from the Cloud OnRamp for SaaS optimization of Microsoft 365 traffic. By modifying the AAR policies, they exclude the Exchange service area (for Outlook) from the Microsoft 365 traffic that Cloud OnRamp for SaaS operates on, thereby ensuring the best performance for the email traffic using the on-premises Outlook server.

Use Case for Enabling Specific Applications at Specific Sites

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.2.1r

An organization's network spans numerous sites. Most of the sites utilize the Box.com cloud storage application, but a subset of sites does not use Box.com.

First, the network administrator creates an AAR policy that serves the subset of sites that do not use Box.com. Next, the network administrator enables Cloud OnRamp for SaaS for Box.com traffic, which enables Cloud OnRamp for SaaS operation at all sites in the network.

To exclude the subset of sites that do not use Box.com, the network administrator edits the AAR policy for that subset of sites, to disable Cloud OnRamp for SaaS operation for Box.com traffic. This has the effect of disabling Cloud OnRamp for SaaS operation for Box.com traffic at that subset of sites only.

Use Case for Excluding Data Prefixes from Cloud OnRamp for SaaS Optimization

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1

Some organizations host SaaS applications in private data centers that are reachable only through the organization's internal network. If you enable Cloud OnRamp for SaaS to optimize traffic for one of these SaaS applications, then Cloud OnRamp for SaaS might attempt to route the SaaS traffic to a server outside the organization's internal network. This inadvertently prevents the SaaS traffic from reaching the private data center.

For example, an organization hosts a private on-premises SharePoint server for its internal SharePoint traffic. At the same time, the organization has enabled Cloud OnRamp for SaaS optimization for several SaaS applications, including SharePoint. This can inadvertently interfere with the SharePoint traffic.

To prevent Cloud OnRamp for SaaS optimization of the internal SharePoint traffic, network administrators configure Cloud OnRamp for SaaS to exclude the IP prefixes of the internal SharePoint servers. Consequently, internal SharePoint traffic flows correctly to the on-premises SharePoint server at the private data center.

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 Catalyst SD-WAN Devices

You can enable Cloud OnRamp for SaaS in your Cisco Catalyst 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 SD-WAN Manager 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 SD-WAN Manager for configuring Cloud OnRamp for SaaS features.

Enable Cloud OnRamp for SaaS

Before You Begin

From Cisco Catalyst SD-WAN Manager Release 20.13.1, Cloud OnRamp for SaaS is enabled by default.

Enable Cloud OnRamp for SaaS

1. From the Cisco SD-WAN Manager 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 SD-WAN Manager

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

   or

- In Cisco SD-WAN Manager, 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. (Optional) (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) To exclude specific data prefixes for all SaaS applications, click **Exclude Destination Data Prefix**.

   In the drop-down list, choose an existing data prefix list or click **New Data Prefix List** to define a new data prefix list.

   For more information about configuring a data prefix, see the Configure Data Prefix section in Centralized Policy in the *Cisco Catalyst SD-WAN Policies Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x*.

Note To exclude data prefixes for a specific SaaS application, see a later step in this procedure.

   For information about excluding data prefixes, see Information About Excluding Data Prefixes, on page 15.

5. Enable applications and configure.

Column	Description
Applications	Applications that can be used with Cloud OnRamp for SaaS. If you enable the **Office 365** application, you can click the **Enable Application Feedback** link to enable Cloud OnRamp for SaaS to receive server-side metrics from Microsoft. For information, see Enable Application Feedback Metrics for Office 365 Traffic. If you enable the **Webex** application, you can click the **Enable Application Telemetry** link to enable Cloud OnRamp for SaaS to receive server-side metrics from Webex. **Note** Enabling application feedback metrics opens a Microsoft site that requests various permissions to access your application telemetry data. These permissions enable Cisco Catalyst SD-WAN to receive application telemetry data from Microsoft and correlate it with network telemetry data. This is part of the process of computing best paths to optimally route Microsoft 365 traffic. The Bcos.IsvPartner permission provides access to the Branch Connect Web Services APIs, which Cisco uses to manage opt-in, get connectivity information about branch sites, and store location information, such as IP addresses. These APIs enable correlating traffic to branch sites. The Bcos.ReadOnly and Bcos.ReadWrite permissions are storage permissions for the tenant-specific portion of the Branch Connect Optics Store. This is an Azure storage located in the region that you select when opting in. Cisco and Microsoft use this storage location to exchange telemetry information for processing.
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 Catalyst 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 Catalyst 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 Catalyst SD-WAN 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.

Column	Description
Exclude Destination Data Prefix	(Optional) From Cisco Catalyst SD-WAN Manager Release 20.13.1, you can exclude a data prefix list for a specific SaaS application: **a.** Click **Select Destination Data Prefix**. **b.** In the drop-down list, choose a data prefix list or click **New Data Prefix List** to define a new list. **c.** Click **Save**. **Note** To exclude data prefixes for all SaaS applications, see a previous step in this procedure. For information about excluding data prefixes, see Information About Excluding Data Prefixes, on page 15.

6. 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.

7. Click **Save Policy and Next**. This saves the policy to the Cisco Catalyst SD-WAN Controller.
8. To activate the modified policy, click **Activate**.

Note You can choose a simple workflow under application and SLA priority to create a data prefix using exclusion of RFC1918 data prefix lists (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). When you switch from already created simple workflow to advanced workflow layout, you can see the default RFC1918 data prefix list sequences in proper order and can proceed to add any additional prefix lists on top of that.

Configure Sites for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager

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 SD-WAN Manager 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 Manager mode.
4. Choose one or more client sites from **Available Sites** and move them to **Selected Sites**.
5. Click **Attach**. The Cisco SD-WAN Manager saves the feature template configuration to the devices. The Task View window displays a Validation Success message.
6. From the Cisco SD-WAN Manager 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 Manager mode.
9. In the **Device Class** field, choose one of the following operating systems:
   - **Cisco OS**: Cisco IOS XE Catalyst 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 Catalyst SD-WAN 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 Catalyst SD-WAN 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 Catalyst SD-WAN Release 17.7.1a), or the VPN 0 interfaces or service VPN interfaces to add (for releases from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a).
    d. Click **Save Changes**.

12. (Cisco IOS XE Catalyst 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 Catalyst SD-WAN Release 17.6.1a, you can choose Service VPN or VPN 0 if the gateway uses Cisco IOS XE Catalyst 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. From Cisco Catalyst SD-WAN Manager Release 20.13.1, if you chose **All DIA TLOC**, or **TLOC list** and specified the colors to include in the TLOC list, you can associate a tracker or tracker group for the gateway site by checking the **Enable Tracker Association** check box.

For more information about configuring a tracker, see Prerequisites for Faster Failover with a DIA Tracker, on page 20.

e. To enable load balancing for cloud application traffic across multiple interfaces on the WAN edge device, check the **Enable Load Balancing** check box. (See Load Balancing Across Multiple Interfaces.)

f. Configure the load-balancing options:

Option	Description
Loss (%)	After determining the best path interface for a cloud application, Cloud OnRamp compares the performance statistics for other interfaces. To use another interface for load balancing, the packet loss value of the interface cannot vary from the packet loss value of the best path interface by more than this configured value. You can configure a smaller value to restrict load balancing only to interfaces with a packet loss value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher packet loss than the best path interface. For example, if the best path interface has a packet loss value of 2% and the **Loss** value is 10, then another interface can be used for load balancing only if its packet loss value is no more than 12%. Range: 0 to 100 Default: 10
Latency (milliseconds)	To use another interface for load balancing, the latency value of the interface can't vary from the latency of the best path interface by more than this number of milliseconds. You can configure a smaller value to restrict load balancing only to interfaces with a latency value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher latency than the best path interface. For example, if the best path interface has a latency of 5 milliseconds, and the **Latency** value is set to 50, then another interface can be used for load balancing only if its latency is no more than 55 milliseconds. Range: 1 to 1000 Default: 50

Option	Description
Source IP based Load Balancing	To ensure that all traffic from a single host uses a single interface, enable this option. For example, to ensure that DNS and application traffic use the same path, enable this option.

g. Click **Save Changes**.

13. Click **Attach**. Cisco SD-WAN Manager 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 SD-WAN Manager 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.
   - Choose **Service VPN** or **VPN 0** based on how the gateway site connects to the internet.
   - 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.
   - From Cisco Catalyst SD-WAN Manager Release 20.13.1, when you choose **VPN 0**, you can associate a tracker with the gateway sites by checking the **Enable Tracker Association** check box.

     For more information about configuring a tracker, see Prerequisites for Faster Failover with a DIA Tracker, on page 20.
   - To add interfaces, click the **Interfaces** field to select available interfaces.
   - To remove an interface, click the **X** beside its name.
   - To enable load balancing for cloud application traffic across multiple interfaces on the WAN edge device, check the **Enable Load Balancing** check box, and configure the load balancing options. (See Load Balancing Across Multiple Interfaces, on page 8.)

Option	Description
Loss (%)	After determining the best path interface for a cloud application, Cloud OnRamp compares the performance statistics for other interfaces. To use another interface for load balancing, the packet loss value of the interface cannot vary from the packet loss value of the best path interface by more than this configured value. You can configure a smaller value to restrict load balancing only to interfaces with a packet loss value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher packet loss than the best path interface. For example, if the best path interface has a packet loss value of 2% and the **Loss** value is 10, then another interface can be used for load balancing only if its packet loss value is no more than 12%. Range: 0 to 100 Default: 10
Latency (milliseconds)	To use another interface for load balancing, the latency value of the interface cannot vary from the latency of the best path interface by more than this number of milliseconds. You can configure a smaller value to restrict load balancing only to interfaces with a latency value very close to that of the best path interface, or you can configure a larger value to be more inclusive of interfaces that might have a higher latency than the best path interface. For example, if the best path interface has a latency of 5 milliseconds, and the **Latency** value is set to 50, then another interface can be used for load balancing only if its latency is no more than 55 milliseconds. Range: 1 to 1000 Default: 50
Source IP based Load Balancing	To ensure that all traffic from a single host uses a single interface, enable this option. For example, to ensure that DNS and application traffic use the same path, enable this option.

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 SD-WAN Manager 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 Manager mode.
4. In the **Device Class** field, select one of the following:
   - **Cisco OS**: Cisco IOS XE Catalyst 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 Catalyst 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.

From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cloud OnRamp for SaaS supports using loopback as a TLOC interface.

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. From Cisco Catalyst SD-WAN Manager Release 20.13.1, if you chose **All DIA TLOC**, or **TLOC list** and specified the colors to include in the TLOC list, you can associate a tracker or tracker group for the DIA site by checking the **Enable Tracker Association** check box.

For more information about configuring a tracker, see Prerequisites for Faster Failover with a DIA Tracker, on page 20.

d. Click **Save Changes**.

8. Click **Attach**. The Cisco SD-WAN Manager 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 SD-WAN Manager 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 Catalyst 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.

   b. From Cisco Catalyst SD-WAN Manager Release 20.13.1, you can associate a tracker on DIA sites by checking the **Enable Tracker Association** check box.

   For more information about configuring a tracker, see Prerequisites for Faster Failover with a DIA Tracker, on page 20.
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**.

Enable Application Feedback Metrics for Office 365 Traffic

Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, you can enable the following types of application feedback from additional sources. Cloud OnRamp for SaaS can use these metrics to help determine the best path for Office 365 traffic. See Best path determination, on page 8.

- Enable telemetry with Microsoft Exchange cloud servers, which can provide best path metrics for Office 365 traffic on specifically configured interfaces. This involves use of a Microsoft service called Microsoft 365 informed network routing. To understand this feature better, see the information available in the Microsoft 365 informed network routing document.
- Enable application response time (ART) metrics, which configures network devices to report ART metrics.

Before You Begin

- Enable monitoring for Office 365 traffic.

  See Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager, on page 24.
- Configure a policy for Office 365, for Cisco IOS XE SD-WAN devices.

  See the Policy/Cloud SLA options in Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager, on page 24.
- To enable NetFlow metrics, enable Cloud Services.

  (From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings** > **Cloud Services**)
- To enable NetFlow metrics for devices in the network, enable the **NetFlow** and **Application** options in the localized policy for each device.

  (From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies** > **Localized Policy** > **Policy template**, **Policy Settings** section)
- Enable Cisco SD-WAN Analytics. See Cisco vAnalytics Insights.

Enable Application Feedback Metrics for Office 365 Traffic

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.
2. In the **Manage Cloud OnRamp for SaaS** drop-down list, choose **Applications and Policy**.
3. In the **Office 365** row, click the **Enable Application Feedback for Path Selection** link.

   The **Application Feedback** dialog box opens.
4. In the **Application Feedback** dialog box, enable traffic metrics:
   - **Telemetry**: Enable Telemetry with Microsoft Exchange cloud servers to receive traffic metrics for Office 365 traffic over specific configured interfaces. For information about configuring interfaces for these metrics, see Enable Microsoft to Provide Telemetry for Office 365 Traffic, on page 37.

     If the option is disabled and the dialog box shows a message requesting sign-in to a Microsoft account, copy the code provided in the message and click the link to sign in. Provide the code on the Microsoft page that is displayed and log in with your Microsoft tenant account credentials when prompted. After signing in, the **Telemetry** option in the dialog box is enabled.

See Enable Microsoft to Provide Telemetry for Office 365 Traffic, on page 37.

- **Traffic Steering**: From Cisco vManage Release 20.9.1, check this check box to allow Cloud OnRamp for SaaS to factor in the Microsoft telemetry data in the best path decision. If you disable this, you can still view the Microsoft telemetry data in the Cisco SD-WAN Analytics dashboard, but the telemetry does not affect the best path decision.
- (Optional) **Application Response Time (ART)**: Enable ART metrics.

Note Enabling ART automatically configures devices to report ART metrics.

5. Click **Save**.

Enable Microsoft to Provide Telemetry for Office 365 Traffic

You can enable Microsoft Exchange cloud servers to calculate traffic metrics for Microsoft Exchange traffic coming from specific interfaces in the Cisco Catalyst SD-WAN overlay. Using the Microsoft Azure portal, you specify which interfaces to include, indicating the interfaces by their public IP addresses. This is called opting in the interfaces.

For the specified interfaces, Microsoft identifies the Office 365 traffic by packet source ID and provides metrics that Cloud OnRamp for SaaS can use to determine the best path for the Office 365 traffic.

Before You Begin

- Enable Cloud OnRamp for SaaS

  (**Administration** > **Settings** > **Cloud OnRamp for SaaS**)

  From Cisco Catalyst SD-WAN Manager Release 20.13.1, Cloud OnRamp for SaaS is enabled by default.

- Enable SD-AVC Cloud Connector

  (**Administration** > **Settings** > **SD-AVC Cloud Connector**)

  Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

  Administration > **Settings** > **SD-AVC**

  See Enable Cisco SD-AVC Cloud Connector.

- Enable Cloud Services

  (**Administration** > **Settings** > **Cloud Services**)

- Configure statistics collection interval to 5 minutes.

  (**Administration** > **Settings** > **Statistics Configuration**)

- Enable Microsoft telemetry for Office 365 traffic. See Enable Application Feedback Metrics for Office 365 Traffic, on page 36.
- Activate the Microsoft 365 informed network routing service for your Microsoft 365 tenant account.
- **ip visibility**

To enable telemetry to operate, configure **ip visibility** on each Cisco IOS XE Catalyst SD-WAN device in the network, as follows:

```
policy
app-visibility
ip visibility features
  cxp        enable
  probe-saas enable
```

Enable Microsoft to Provide Telemetry for Office 365 Traffic

Note The functionality of the Microsoft Azure portal is subject to change and is therefore outside the scope of this documentation. These high-level instructions provide some guidance, but see Microsoft 365 documentation for details.

For information about the following steps, see the "Microsoft 365 informed network routing" topic in the Microsoft 365 documentation.

1. Log in to the Microsoft Azure portal. (For information about how to create a Microsoft Azure tenant account, see the Microsoft Azure documentation.)
2. Using the Microsoft Azure portal, specify Cisco Catalyst SD-WAN overlay network interfaces for which to track traffic metrics.
   a. In the Azure portal, access the Microsoft 365 admin center.
   b. On the **Locations** page, add a location entry for each location in the SD-WAN overlay network, as desired.
   c. Within a location entry, do one of the following:
      - For locations using an edge router operating with Cisco IOS XE Release 17.9.1a or later, on the "Add an office location" page (or the equivalent), enable the option to allow an SD-WAN solution to automatically set the LAN subnet and egress address range. Then enter the system IP address of the edge device for the location.
      - For locations using an edge router operating with Cisco IOS XE Release 17.8.x or earlier, add egress IP addresses, using the public IP address of the desired interfaces.

Enable Webex for Cloud OnRamp for SaaS

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

To enable Cloud OnRamp for SaaS to determine the best path for Webex traffic, enable the Webex application in the same way as other applications. See Enable Cloud OnRamp for SaaS, Cisco IOS XE SD-WAN Devices.

Enable Webex Server-Side Metrics

Minimum releases: Cisco vManage Release 20.10.1, Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

Before You Begin

To enable telemetry to operate, configure **ip visibility** on each Cisco IOS XE Catalyst SD-WAN device in the network, as follows:

```
policy
app-visibility
ip visibility features
  cxp        enable
  probe-saas enable
```

Enable Webex Server-Side Metrics

Webex integrations enable an application, such as Cisco SD-WAN Manager, to request information from Webex servers, using an application programming interface (API).

1. Using your Webex account, create an integration for Cisco SD-WAN Manager. For information about creating the integration, see Webex for Developers documentation, Integrations & Authorization.

   Creating the Webex integration requires a redirect URI, which includes the IP address of your Cisco SD-WAN Manager server, in the following format:

   https://*vManage-ip-address*:*port*/dataservice/webex/redirect

   At the end of the process of creating the Webex integration, the Webex for Developers site provides you with a client ID and client secret.

Note The details for creating an integration app in the Webex for Developers site are beyond the scope of this document.

2. When you enable Webex in Cloud OnRamp for SaaS, use the client ID and client secret that you received in the previous step to enable Cisco SD-WAN Manager to use the WebEx integration.

   a. Open Cloud OnRamp for SaaS:

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

        Or

      - In Cisco SD-WAN Manager, click the cloud icon near the top right and choose **Cloud OnRamp for SaaS**.

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

      The **Applications and Policy** page displays the Cloud OnRamp applications.

   c. Adjacent to **Webex**, click **Enable vAnalytics Webex Telemetry**.

   d. In the pop-up window, check the **Enable Webex Telemetry** checkbox.

   e. Enter the client ID and client secret for the Webex integration, and click **Save**.

   f. When prompted, enter your **Webex** account credentials.

Note You must use the credentials for the Webex account associated with the Webex integration you used in the previous step. This enables Webex telemetry for that Webex account.

g. Click **Save Applications and Next** to save the Webex telemetry configuration on Cisco SD-WAN Manager and push the updates to edge devices and to Cisco SD-WAN Analytics.

Update the Webex Server Information for Cloud OnRamp for SaaS

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS** to display the Cloud OnRamp for SaaS dashboard.
2. (This step applies only to releases earlier than Cisco vManage Release 20.10.1.) If the dashboard shows a dialog box prompting you to synchronize Webex server information, click **Yes** in the dialog box.

   Cisco SD-WAN Manager displays the **Application Aware Routing Policy** page, enabling you to review the policy. The policy includes updated match conditions that use the latest Webex server information.
3. Click **Save Policy**.

   Cloud OnRamp for SaaS updates the following, as needed, to reflect the updated information for Webex servers worldwide:

   - Match conditions in the application-aware policy
   - Configuration for probing the cloud application

Configure the Traffic Category and Service Area for Specific Policies Using Cisco SD-WAN Manager

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

Before You Begin

To edit the service area and traffic category, you must enable **Monitoring** and **Policy/Cloud SLA** for the Microsoft 365 application with a minimum of one service area. For information, see Configure Applications for Cloud OnRamp for SaaS Using Cisco SD-WAN Manager.

Configure the Traffic Category and Service Area

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

     Or
   - In Cisco SD-WAN Manager, 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** page displays all the Cloud OnRamp for SaaS applications.

3. Click the edit icon from the **Policy/Cloud SLA** column for the Microsoft 365 application.

   The **Policy/Cloud SLA Settings** pop-up window opens.

4. Perform one of the following in the **Policy/Cloud SLA Settings** pop-up window.

   - Click **Yes**. Select a minimum of one service area and traffic category.
   - If you have already selected a service area and traffic category, click **No** and edit the Microsoft 365 categories or service area.

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

   The **Application Aware Routing Policy** page opens. A list of AAR policies in the current active centralized policy appears.

6. Select the AAR policy that you wish to edit and click **Review and Edit**.

   The **Review Policy** page opens.

7. Select the Microsoft 365 sequence you wish to edit, to change the service area or traffic category, and click the edit icon.

8. Edit the service area and traffic category, and click **Save Match And Actions**.

9. Click **Save Policy and Next**. This saves the policy.

Configure AAR Policy to Enable Cloud OnRamp Operation on Specific Applications at Specific Sites Using Cisco SD-WAN Manager

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.2.1r

1. Open Cloud OnRamp for SaaS.

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

     Or

   - In Cisco SD-WAN Manager menu, 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** page displays all the Cloud OnRamp for SaaS applications.

3. Click **Save Applications and Next**.

   The **Application Aware Routing Policy** page opens, showing the application-aware policies in the current active centralized policy.

4. Select the policy you wish to edit and click **Review and Edit** to view the policy details.

5. You can now delete one or more sequences that have been added by Cloud OnRamp for SaaS for specific applications or change the order of the sequences.

6. Click **Save Policy and Next**. This pushes the updated policy to the Cisco SD-WAN Controller.

Note Note: When you enable an application on the **Applications and Policy** page, by default, Cloud OnRamp for SaaS is enabled for all AAR policies that are part of the current active centralized policy.

Enable Application Visibility and Flow Visibility

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Enable Visibility and Flow Visibility Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. Click **Add Policy**.
4. Continue clicking **Next** until the **Policy Settings** page appears.
5. Check the **Netflow and Applications** check box.
6. Click **Save Policy**.

   Application visibility and flow visibility are now enabled.

Enable Application Visibility and Flow Visibility Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Configure Visibility for Microsoft 365 SaaS traffic Using Cisco SD-WAN Manager

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Enable a Device to Provide Data for the Visualization of Microsoft 365 Traffic

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **On Demand Troubleshooting**. The **On Demand Troubleshooting** page opens.
2. Click the **Select Device** drop-down list and choose a device.
3. Click the **Select Data Type** drop-down list and choose the data type **DPI**.
4. Select a time range from **Data Backfill Time Period**.
5. Click **Add** to queue the device for processing.
6. Wait until the **Status** column shows **Completed**.

View Application Usage

Minimum releases (for Microsoft 365 traffic): Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.9.1a

Minimum releases (for Webex traffic): Cisco vManage Release 20.10.1, Cisco IOS XE Catalyst SD-WAN Release 17.10.1a

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

     Or

   - In Cisco SD-WAN Manager, click the cloud icon near the top right and select **Cloud OnRamp for SaaS**.
2. Click **Manage Cloud OnRamp for SaaS**.
3. Click the **Microsoft 365** application or the **Webex** application. A list of devices that are attached to a DIA or gateway is shown.
4. In the **Application Usage** column of a device, click **View Usage**.

   For the Webex application, the usage information is shown according to Webex region.
5. The **CoR SaaS Application Usage** page displays the information for each type of traffic. To limit the traffic information that is displayed, click the **Search** field, and choose **All CoR SaaS Traffic**, **DIA**, **Gateway**, or **Non CoR SaaS**.

Note

- The information presented in the above graphs or logs is for an individual device. You can view the information related to only one device at a time. The graphs or logs are only shown for those devices for which on-demand troubleshooting is enabled. For information about on-demand troubleshooting, see On-Demand Troubleshooting.
- IP visibility feature commands are supported only through CLI or add-on CLI template.
- If you don't see any application usage for each type of traffic for a particular Cisco IOS XE Catalyst SD-WAN device, add the following configuration to the device using a CLI add-on feature template:

```
policy
 app-visibility
 ip visibility features
  cxp        enable
  probe-saas enable
```

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 SD-WAN Manager 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**.

Verify Changes to the Configuration of the Traffic Category and Service Area for Specific Policies Using Cisco SD-WAN Manager

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Catalyst SD-WAN Release 17.5.1a

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

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

   A list of devices is displayed.
3. For the device you wish to verify, click **…** and click **Running Configuration**. The **Running Configuration** window opens, displaying the running configuration.
4. Verify that the running configuration reflects any changes that you have made to AAR policies.

Or

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

   The **Policies** page displays the policies.
2. For the policy, you wish to verify, click **…** and click **Preview**.

   The **Policy Configuration Preview** pop-up window appears, providing a preview of the running configuration.
3. Verify that the policy preview reflects any changes that you have made to AAR policies.

Verify Which Applications Are Enabled for Specific Devices Using Cisco SD-WAN Manager

Minimum releases: Cisco vManage Release 20.9.1, Cisco IOS XE Release 17.2.1

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

Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

A list of devices is displayed.

3. For the device you wish to verify, click **…** and click **Running Configuration**. The **Running Configuration** window opens, displaying the running configuration.
4. Verify that the running configuration reflects any changes that you have made to AAR policies.

Verify Which Applications Are Enabled for a Specific Policy Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.

   The **Policies** window displays the policies.
2. For the policy, you wish to verify, click **…** and click **Preview**.

   The **Policy Configuration Preview** page appears, providing a preview of the running configuration.
3. Verify that the policy reflects any changes that you have made to AAR policies.

Verify the Excluded Data Prefixes Using Cisco SD-WAN Manager

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

Before You Begin

You can exclude specific data prefixes from Cloud OnRamp for SaaS optimization. For information, see Information About Excluding Data Prefixes, on page 15. The excluded data prefixes appear in the application-aware routing policy. This procedure displays the application-aware routing policy, enabling you to verify the excluded data prefixes.

Verify Excluded Prefixes

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.
2. Click **Manage Cloud OnRamp for SaaS** and choose **Applications and Policy**.

   The **Applications and Policy** page displays all SaaS applications.
3. Click **Save Applications and Next**.

   The **Application Aware Routing Policy** page appears, showing the application-aware policies for the active centralized policies.
4. Choose an application-aware policy and click **Review and Edit** to view the policy details.
5. Click **Preview**.
6. Click **Config Diff**.

7. View the data prefixes that you are excluding.

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 SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.

     or

   - In Cisco SD-WAN Manager, 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.

Field	Description
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 Catalyst 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**. From Cisco Catalyst SD-WAN Manager Release 20.13.1, if the best path is a loopback interface, this field displays the interface bind to the loopback.
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**.
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**.

Field	Description
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 Catalyst 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.

Monitor the Status of Webex for Cloud OnRamp for SaaS

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and Cisco vManage Release 20.7.1

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

   The page displays each monitored application, the relevant sites, with information about each.

2. Optionally, you can click a site to display a chart of the scores for various available paths for the application traffic, and the best path (solid line).

3. Beginning with Cisco vManage Release 20.10.1, for each site and region, you can view information about the interfaces that Webex traffic is using. For information, see View Application Usage, on page 43.

View Server Information Using the SD-AVC Cloud Connector

Before You Begin

- Enable SD-AVC (**Administration** > **Cluster Management**, click **…** and choose **Edit**, and choose **Enable SD-AVC**).

- Enable the SD-AVC Cloud Connector. See Enable Cisco SD-AVC Cloud Connector in the *Cisco Catalyst SD-WAN Getting Started Guide*.

View Server Information

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **SD-AVC Cloud Connector**.
2. In the **Application** field, choose an application.
   - For the Office 365 application, the **SD-AVC Cloud Connector** page shows the following information collected from Microsoft Cloud about the Microsoft application servers that handle Office 365 traffic:

Field	Description
Domain tab	
Application Name	Name of the application producing the traffic. Network-Based Application Recognition (NBAR), a component of Cisco IOS XE, provides the application name.
Domain	Destination domain of the traffic. This is the application server handling the cloud application traffic.
Service Area	The service area categorization, as determined by Microsoft, including **exchange**, **sharepoint**, **skype**, and **common**.
Category	Traffic categorization by Microsoft as **optimize**, **allow**, or **default**. A dash in this field indicates traffic that does not have a defined category.
Service Instance	Service instance information, as defined by Microsoft, for the server. Examples of service instances are China, Germany, USGovGCCHigh, and USGovDoD.
IP Address tab	
IP	Destination IP of the traffic. This is the IP address of the application server handling the cloud application traffic.
Port	Destination port of the traffic.
L4 Protocol	Transport protocol of the traffic, such as TCP or UDP.
Application	Name of the application producing the traffic. NBAR, a component of Cisco IOS XE, provides the application name.
Category	Traffic categorization by Microsoft as **optimize**, **allow**, or **default**. A dash in this field indicates that traffic does not have a defined category.
Service Area	The service area categorization, as determined by Microsoft, including **exchange**, **sharepoint**, **skype**, and **common**.
Service Instance	Service instance information, as defined by Microsoft, for the server. Examples of service instances are China, Germany, USGovGCCHigh, and USGovDoD.

- (Minimum release: Cisco vManage Release 20.10.1) For the Webex application, the **SD-AVC Cloud Connector** page shows the following information collected from Webex cloud servers:

Field	Description
IP Address tab	
Application Name	Name of the application producing the traffic.
Service Area	Type of Webex traffic: meeting, calling, or teams.
IP Address	Destination IP address of the traffic. This is the IP address of the application server handling the cloud application traffic.
Port	Destination port or ports of the traffic.
L4 Protocol	Transport protocol of the traffic, such as TCP or UDP.
Quality of Service	QoS classification for the Webex traffic, as defined by Webex, such as default or optimizemedia.
Primary or Fallback	Category of Webex traffic.
Region	Region of the Webex server data center, such as ap-south-1, ap-northeast-1, and ap-southeast-1.

3. Optionally, you can use the search field to filter the information in the table. For example, you can filter by an application name or by a domain name.

Monitor an Excluded Data Prefix List for Cloud OnRamp for SaaS

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Click on the device to select it.
3. Click **Real Time** in the left pane.
4. Click the **Device Options** drop-drop list, and choose **Policy App Route Filter**.

A table displays real-time statistics, including the packet counter name that represents the data prefix list for an application.

View Logs in Syslog And Console Log

The Cisco Cloud OnRamp for SaaS notifications and alarms are populated in the syslog. These notifications and alarms are not populated in the console log. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the Cisco Cloud OnRamp for SaaS notifications and alarms are displayed both in syslog and console logs. However, to avoid flooding of notifications and alarms on both syslog and console logs, Cisco SD-WAN Manager generates NETCONF by default, the syslogs on demand and the console logs when you add a CLI template. For more information about using CLI templates, see CLI Add-on Feature Templates and CLI Templates.

1. Use the **system** *alarms alarm cloud-express-score change syslog* command using a CLI template to print the cloud express score change notifications both in syslogs and console logs.
2. Use the **system** *alarms alarm cloud-express-application-change syslog* command using a CLI template to print the cloud express application change notifications both in syslogs and console logs.

Cloud OnRamp for SaaS Over SIG Tunnels

Table 4: Feature History

Feature Name	Release Information	Description
Cloud OnRamp for SaaS Over SIG Tunnels	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco vManage Release 20.6.1	This feature allows you to connect to Cloud OnRamp for SaaS by means of a SIG tunnel. The Cloud OnRamp for SaaS Over SIG Tunnels feature provides you with secure access to the SaaS applications, and the capability to automatically select the best possible SIG tunnel for accessing the SaaS applications.

Prerequisites for Cloud OnRamp for SaaS Over SIG Tunnels

- The SIG tunnels created using the Secure Internet Gateway (SIG) template must have a valid Tracker Source IP address. Cloud OnRamp for SaaS uses the Tracker Source IP address in the SIG template for probing purposes.
- Configure the device to use an internet-based DNS server with an IP address that can be reached through the SIG tunnel.

Restrictions for Cloud OnRamp for SaaS Over SIG Tunnels

- Application identification:

  An application must be identified by Cloud OnRamp for SaaS from the very first packet in a flow going through the edge routers, between a branch and Cloud OnRamp for SaaS. If an application cannot be identified in the first packet of a flow, the best path that is selected by Cloud OnRamp cannot be implemented for the subsequent packets in that given flow. After an application is classified, the subsequent traffic flow goes through the best path selected by Cloud OnRamp for SaaS.

- Gateway exit and DIA:

  Cloud OnRamp for SaaS comparison logic between a gateway exit and a Direct Internet Access (DIA) exit cannot determine if the Cloud OnRamp for SaaS in the remote gateway is executing a computation with an underlay interface or a SIG interface.

- IPv6 support:

IPv6 is not supported with Cloud OnRamp for SaaS.

- Support for telemetry:
  - You cannot enable Microsoft 365 telemetry or Webex server-side metrics on a site that uses Cloud OnRamp for SaaS over SIG tunnels.
  - From Cisco Catalyst SD-WAN Manager Release 20.14.1, in a scenario that includes (a) sites that use Cloud OnRamp for SaaS over SIG tunnels, and also (b) sites that use Cloud OnRamp for SaaS without SIG tunnels, Microsoft 365 telemetry and Webex server-side metrics are supported only on the sites that do not use a SIG tunnel.

    When you enable Microsoft 365 telemetry or Webex server-side metrics globally, they are active only on sites that do not use Cloud OnRamp for SaaS over SIG tunnels.
  - From Cisco vManage Release 20.6.1 through Cisco Catalyst SD-WAN Manager Release 20.13.x, in a scenario that includes (a) sites that use Cloud OnRamp for SaaS over SIG tunnels, and also (b) sites that use Cloud OnRamp for SaaS without SIG tunnels, Microsoft 365 telemetry and Webex server-side metrics are not supported on any of the sites in the network.

    If you attempt to enable Microsoft 365 telemetry or Webex server-side metrics in this scenario, an error appears in the task list, associated with the push feature template configuration task.

Information About Cloud OnRamp for SaaS Over SIG Tunnels

Using Cloud OnRamp for SaaS, a site can connect to SaaS applications through the following:

- Through the best performing SIG tunnel
- Through a gateway site in which the traffic is sent through the best-performing overlay tunnel from the branch to the gateway, and then from the gateway site through the best-performing SIG tunnel.

When you configure Cloud OnRamp for SaaS for a site to connect over SIG tunnels, you have secure access to the SaaS applications over the internet.

From Cisco Catalyst SD-WAN Control Components Release 20.6.1 and Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, Cloud OnRamp for SaaS supports faster failover on SIG tunnels by default, if the SIG tunnels are configured with Layer 7 health check. For more information about configuring Layer 7 health check, see Support for Layer 7 Health Check.

Benefits of Cloud OnRamp for SaaS Over SIG Tunnels

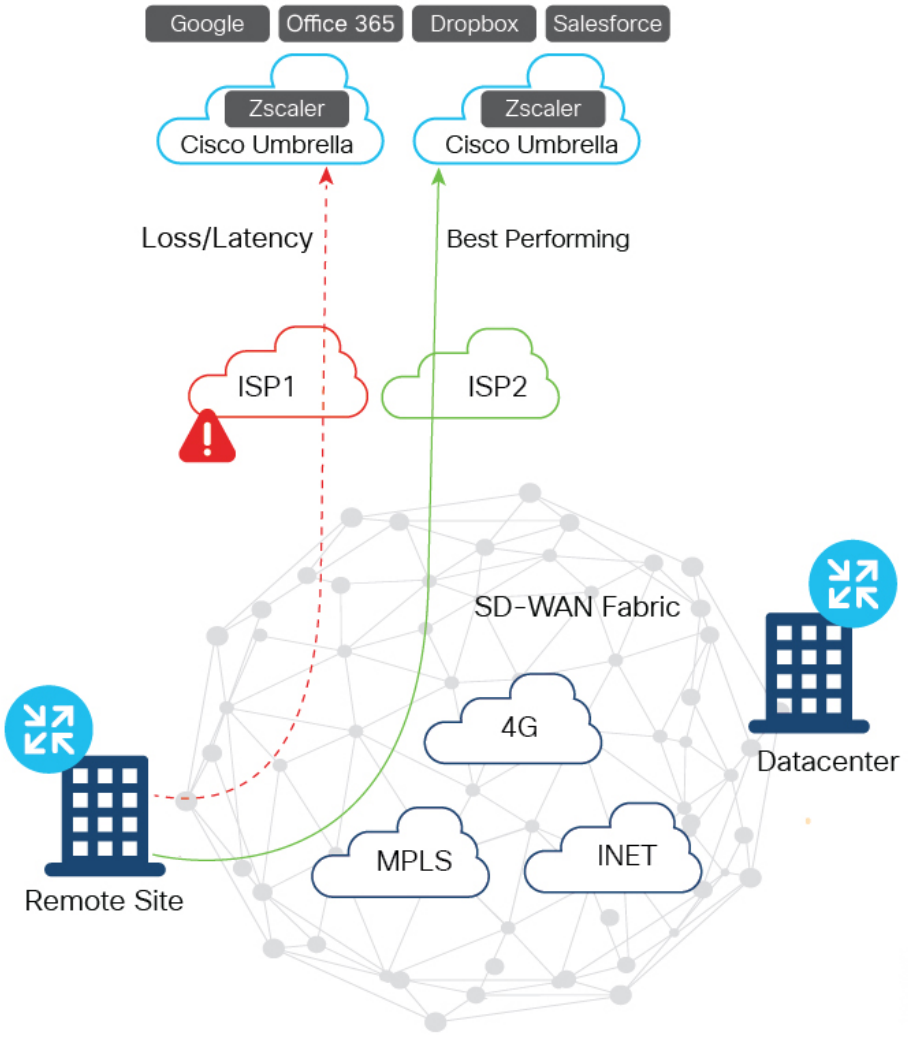
Connecting to Cloud OnRamp for SaaS over SIG tunnels has the following benefits:

- You have secure access to the SaaS applications over SIG tunnels.
- Cloud OnRamp for SaaS over SIG tunnels provides best path performance where access to the SaaS applications is enabled through the best-performing tunnel.

Use Cases for Cloud OnRamp for SaaS Over SIG Tunnels

There are different ways through which you can access the SaaS applications over SIG tunnels:

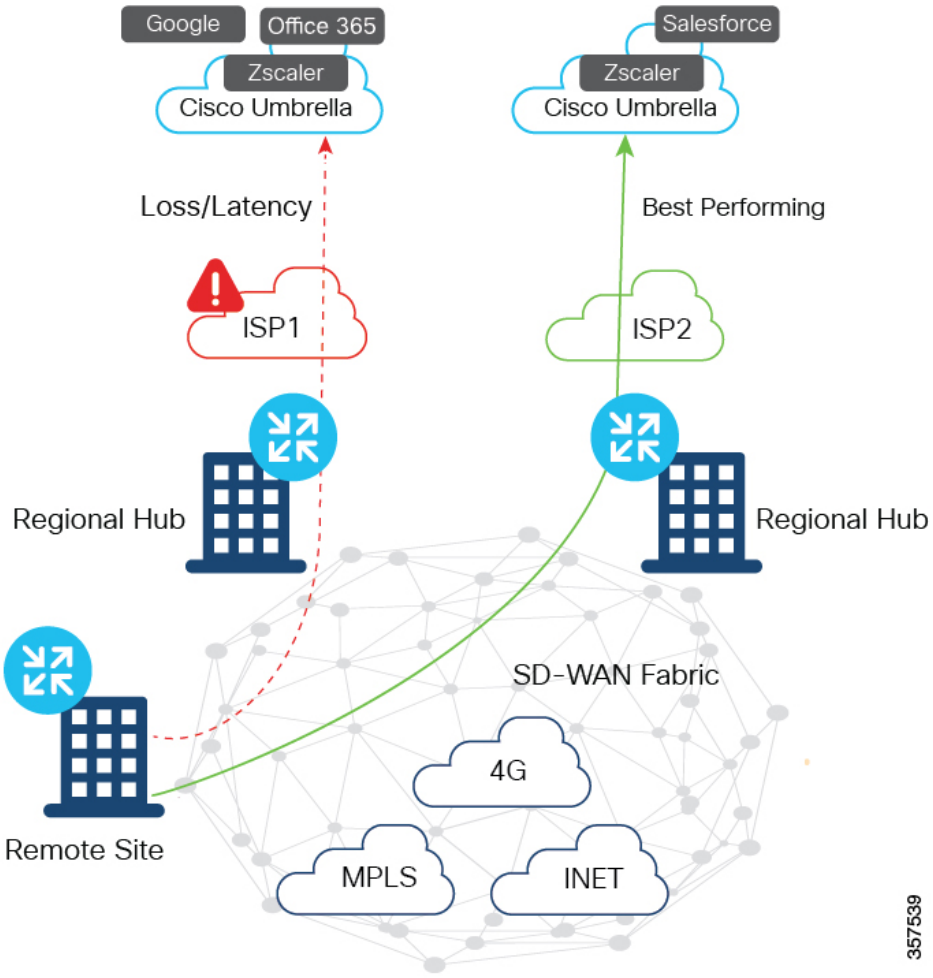
Direct Access to SaaS Applications with Multiple SIG Tunnels from Branch Using DIA



In this scenario:

- Multiple VPN0 tunnels over GRE or IPSec are set up from a branch to Zscaler and Cisco Umbrella.
- Traffic from the branch is forwarded through the best-performing tunnel for a given SaaS application, and is terminated at Zscaler and Cisco Umbrella for security inspection.
- Traffic is forwarded to the internet from SIG.

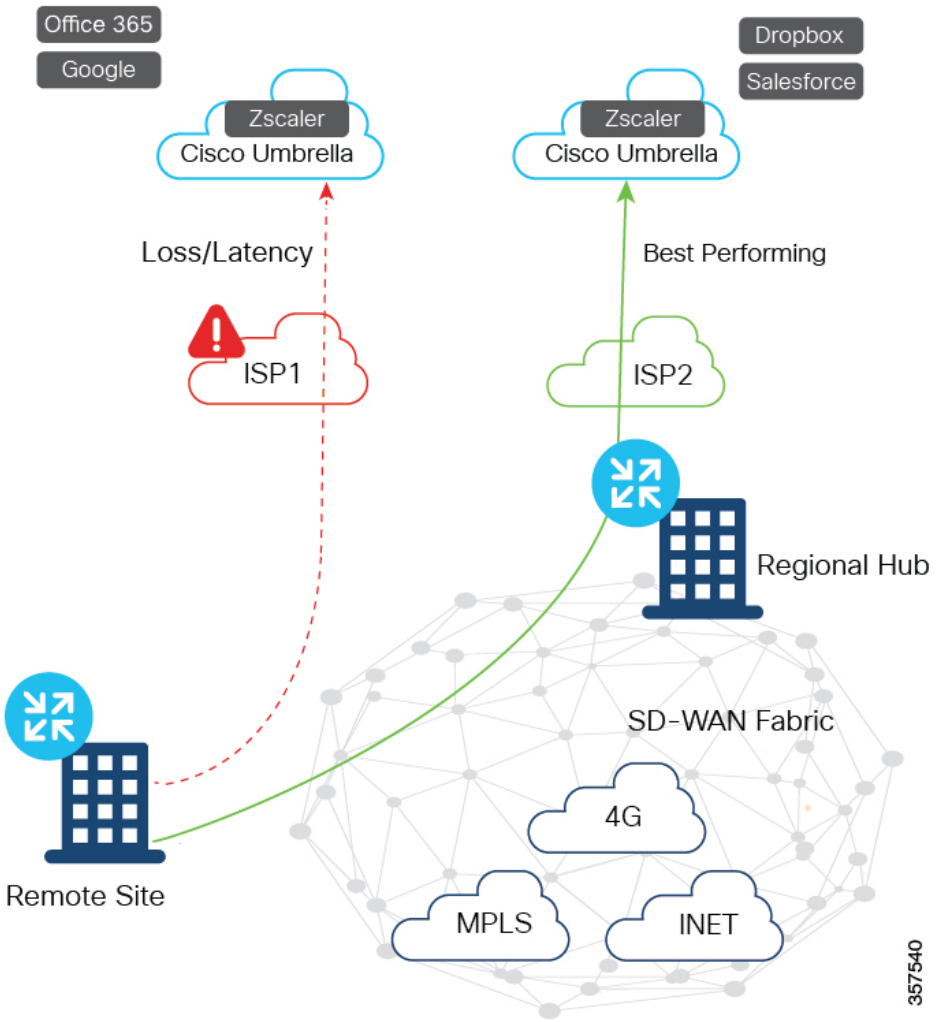
Access to SaaS Applications with Multiple SIG Tunnels from Branch Using a Gateway



In this scenario:

- Multiple VPN0 tunnels over GRE or IPSec are set up from one or more regional hubs to Zscaler and Cisco Umbrella.
- Traffic from branch is forwarded to the best-performing regional hub for a given SaaS application, and is terminated at Zscaler and Cisco Umbrella for security inspection.
- Traffic is forwarded to the internet from SIG.

Access to SaaS Applications with Multiple SIG Tunnels from Branch Using DIA and Gateway



In this scenario:

- Multiple VPN0 tunnels over GRE or IPsec are set up from a branch, regional hub, or both to Zscaler and Cisco Umbrella.
- Traffic from branch, regional hub, or both is forwarded through the best-performing tunnel for a given SaaS application, and is terminated at Zscaler and Cisco Umbrella for security inspection.
- Traffic is forwarded to the internet from SIG.

Configure Cloud OnRamp for SaaS Over SIG Tunnels

Configure Cloud OnRamp for SaaS over SIG Tunnels Using DIA

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS**.
2. From **Manage Cloud OnRamp for SaaS** drop-down list, choose **Direct Internet Access (DIA) Sites**.

3. Click **Attach DIA Sites**.

   The **Attach DIA Sites** dialog box displays all the sites in your overlay network, with the available sites highlighted.

4. In **Device Class**, select:

   Cisco OS (cEdge)

5. In the **Available Sites** pane, select a site that you want to attach, and click the right arrow. To remove a site, in the **Selected Sites** pane, click a site, and then click the left arrow.

6. Click **Add TLOC to selected sites**.

7. Click **Secure Internet Gateway (SIG) Interfaces**.

8. Click **All Auto SIG Interfaces** or **SIG Interface List** from **Attach DIA Sites** window, and then choose from the list of tunnels that are configured from the Cisco Secure Internet Gateway template.

Note The Tunnel1000X entry in the **SIG Interface List** field refers to the interface name, the equivalent of the IPSec interface name entered when configuring a SIG template.

9. Click **Save Changes**.

10. Click **Attach**.

    Cisco SD-WAN Manager pushes the feature template configuration to the devices, and the **Task View** window displays a **`Validation Success`** message.

Configure Cloud OnRamp for SaaS over SIG Tunnels Using a Gateway

To configure Cloud OnRamp for SaaS over SIG tunnels a Gateway, perform the following steps:

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

2. From **Manage Cloud OnRamp for SaaS** drop-down list, choose **Gateways**.

3. Click **Attach Gateways**.

   The **Attach Gateways** pop-up window displays all the sites in your overlay network, with available sites highlighted.

4. In **Device Class**, select:

   Cisco OS (cEdge)

5. In the **Available Sites** pane, select a site that you want to attach, and click the right arrow. To remove a site, in the **Selected Sites** pane, click a site, and then click the left arrow

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

7. Click **VPN 0**.

8. Click **Secure Internet Gateway (SIG) Interfaces**.

9. Click **All Auto SIG Interfaces**, or **SIG Interface List** from **Attach Gateways** window, and then choose from the list of tunnels that are configured from the Cisco Secure Internet Gateway template.

Note The Tunnel1000X entry in the **SIG Interface List** field refers to the interface name, the equivalent of the IPSec interface name entered when configuring a SIG template.

10. Click **Save Changes**.
11. Click **Attach**. Cisco SD-WAN Manager pushes the feature template configuration to the devices, and the **Task View** window displays a **`Validation Success`** message.

Configure Cloud OnRamp for SaaS Over SIG Tunnels Using the CLI

This section provides sample CLI configurations for Cloud OnRamp for SaaS over SIG tunnels.

Configure Cloud OnRamp for SaaS over SIG Tunnels for DIA and Gateway Sites

```
Device# config-transaction
Device(config)# probe-path {branch|gateway}
{all-auto-sig-tunnels|sig-tunnel-list} list of SIG tunnels
Device(config)# ip sdwan route vrf vrf ip address service sig
```

Enable NBAR Protocol Discovery for Cloud OnRamp for SaaS Over SIG Tunnels for Gateway Sites

```
Device# config-transaction
Device(config)# probe-path gateway {all-auto-sig-tunnels|sig-tunnel-list} list
 of SIG tunnels
Device(config)# ip sdwan route vrf vrf ip address service sig
Device(config)# interface tunnel-id
Device(config-if)# ip nbar protocol-discovery
```

Example

The following example configures Cloud OnRamp for SaaS over SIG tunnels for a gateway site and enables NBAR protocol discovery on tunnel interfaces Tunnel100001 and Tunnel100002.

```
Device# config-transaction
Device(config)# probe-path gateway all-auto-sig-tunnels
Device(config)# ip sdwan route vrf 1 192.168.0.1 service sig
Device(config)# interface Tunnel101
Device(config-if)# ip nbar protocol-discovery
Device(config-if)# interface Tunnel102
Device(config-if)# ip nbar protocol-discovery
```

Configure VPN with Loopback Interfaces

```
Device# config-transaction
Device(config)# vrf definition vrf
Device(config-vrf)# address-family ipv4
Device(config-vrf)# exit-address-family

Device(config)# interface  Loopback interface_number
Device(config-if)# no shutdown
Device(config-vrf)# vrf forwarding vrf_number
```

```
Device(config-vrf)# ip address ip address mask
Device(config-vrf)# exit
```

Monitor Cloud OnRamp for SaaS Over SIG Tunnels

To monitor Cloud OnRamp for SaaS over SIG tunnels, perform the following steps:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. From the list of devices that is displayed, select a device.
3. Click **Real Time** in the left pane.
4. Click **Device Options** drop-drop list, and choose one of the following commands:

Device Option	Description
CloudExpress Applications	Displays the best path for applications that are configured with Cloud OnRamp for SaaS. The best path could be a local interface with DIA, or the path to a remote gateway.
CloudExpress Gateway Exits	Displays the loss and latency on each gateway exit for applications that are configured with Cloud OnRamp for SaaS.
CloudExpress Local Exits	Displays the application loss and latency on each DIA interface that is enabled for Cloud OnRamp for SaaS.

5. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Cloud OnRamp for SaaS** to access the dashboard where you can view the applications available on Cloud OnRamp for SaaS.

Monitor Cloud OnRamp for SaaS Over SIG Tunnels Using the CLI

Example 1

The following is a sample output from the **show sdwan cloudexpress local-exits** command on Cisco IOS XE Catalyst SD-WAN devices . This example displays the application loss and latency on each DIA interface that is enabled for Cloud OnRamp for SaaS.

```
Device# show sdwan cloudexpress local-exits

VPN APPLICATION INTERFACE LATENCY LOSS
------------------------------------------------------------------------
1 office365 Tunnel100015 10 0
1 office365 Tunnel100016 3 0
1 amazon_aws Tunnel100015 10 0
1 amazon_aws Tunnel100016 3 0
```

Example 2

The following is a sample output from the **show sdwan cloudexpress gateway-exits** command on Cisco IOS XE Catalyst SD-WAN devices. This example displays the loss and latency on each gateway exit for applications that are configured with Cloud OnRamp for SaaS.

```
Device# show sdwan cloudexpress gateway-exits

                                                                                LOCAL  REMOTE
VPN  APPLICATION              GATEWAY IP               LATENCY  LOSS  COLOR  COLOR
-------------------------------------------------------------------------------------------
1    salesforce               172.16.255.14            72       2     lte    lte
1    google_apps              172.16.255.14            16       0     lte    lte
```

Example 3

The following is a sample output from the **show sdwan cloudexpress applications** command on Cisco IOS XE Catalyst SD-WAN devices. This example displays the best path for applications that are configured with Cloud OnRamp for SaaS. The best path could be a local interface with DIA, or the path to a remote gateway.

```
Device# show sdwan cloudexpress applications

                                EXIT     GATEWAY
LOCAL  REMOTE
VPN  APPLICATION                TYPE     SYSTEM IP      INTERFACE  LATENCY  LOSS
COLOR  COLOR
-----------------------------------------------------------------------------------------------
1    salesforce                 gateway  172.16.255.14  -          103      1
lte    lte
1    google_apps                gateway  172.16.255.14  -          47       0
lte    lte
```

Example 4

The following is a sample output from the **show ip route vrf** command on Cisco IOS XE Catalyst SD-WAN devices. This example displays the IP routing table that is associated with a specific VPN routing and forwarding (VRF) instance.

```
Device# show ip route vrf vrf1

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route

Gateway of last resort is not set

B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C    10.0.0.0/8 is directly connected, Ethernet1/3
B    10.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20
```

Example 5

The following is a sample output from the **show sdwan run probe-path** command on Cisco IOS XE Catalyst SD-WAN devices. This example displays the probe path for SIG tunnels.

```
Device# show sdwan run probe-path
probe-path branch sig-tunnel-list Tunnel100015 Tunnel100016
```

Configuration Example for Cloud OnRamp for SaaS Over SIG Tunnels

The following example shows the configuration of Cloud on Ramp for SaaS over SIG tunnels:

Example

```
Device(config)# probe-path branch sig-tunnel-list Tunnel100015 Tunnel100016
Device(config)# probe-path branch all-auto-sig-tunnels
```

Troubleshooting Cloud OnRamp for SaaS

The following sections describe problem scenarios and troubleshooting information.

Cannot Enable Telemetry for the Webex Application

Problem

You cannot enable telemetry for the Webex application in Cloud OnRamp for SaaS.

Solutions

For context for each of the following steps, see Enable Webex Server-Side Metrics, on page 38.

1. Ensure that you have created the application integration, using the Webex developer site.
2. Ensure that you have entered the correct redirect URL, in the format below:

   https://*vManage-ip-address*:*port*/dataservice/webex/redirect
3. Ensure that when you enable Webex in Cloud OnRamp for SaaS, you enter the correct client ID and client secret.

Failing to Identify the Best Path for Each Webex Region

Problem

Cloud OnRamp for SaaS fails to identify the best path for each Webex region.

Solutions

1. If a device fails to identify the best path, run the **show avc sd-service info connectivity** command on the device to ensure that Cisco SD-AVC is enabled.
2. From the Cisco SD-WAN Manager menu, choose **Monitor** > **SD-AVC Cloud Connector**. Choose the **Webex** application and verify that the region field is populated.

3. Verify that DNS and NAT are operating correctly, outside of the context of Cloud OnRamp for SaaS configuration. Cloud OnRamp for SaaS functionality depends on these to be configured correctly.
4. Verify that the region's responder server is operational and reachable by the device. To do this, ping the server from the device and verify that the server responds to the ping.

   The regional responder server names are in the following format:

   pinger.*region-name*.infnet.webex.com

   The following example is for the us-west region:

   ```
   Device#ping pinger.us-west-1.infnet.webex.com
   ```

Debug and Show Commands

Note The following debug and show commands are applicable for Cisco IOS XE Catalyst SD-WAN devices running Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and later.

Table 5:

Description	Command
To debug the CXP and Cisco SD-WAN Analytics interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-analytics* **debug**
To analyze the verbose level debug traces of the CXP and Cisco SD-WAN Analytics interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-analytics* **verbose**
To set platform software trace cxpd RP active cxpd-analytics notice to set the debug level to the notice level debug traces of CXP and Cisco SD-WAN Analytics interaction scenarios (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-analytics* **notice**
To enable debug traces to analyze the CXP App best path selection logic handling	Use the command **set platform software trace** *cxpd RP active cxpd-app* **debug**
To enable verbose level debug traces to analyze the CXP App best path selection logic handling	Use the command **set platform software trace** *cxpd RP active cxpd-app* **verbose**
To set the debug level to the notice level and to disable the CXP App best path selection logic handling debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-app* **notice**
To enable debug traces to analyze the CXP config parsing handling	Use the command **set platform software trace** *cxpd RP active cxpd-config* **debug**
To enable debug traces to analyze the verbose level CXP config parsing handling	Use the command **set platform software trace** *cxpd RP active cxpd-config* **verbose**

Description	Command
To set the debug level to the notice level and to disable the CXP config parsing handling debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-config* **notice**
To enable debug traces to analyze the CXP and DPI module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-dpi* **debug**
To enable verbose level debug traces to analyze the CXP and DPI module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-dpi* **verbose**
To set the debug level to the notice level and to disable the CXP and DPI module interaction scenarios debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-dpi* **notice**
To debug traces to analyze the CXP and FTM module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-ftm* **debug** This trace can be enabled to analyze the data plane programming issues from CXP. From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the *cxpd-ftm* keyword in this command is deprecated
To debug traces to analyze the CXP and FMANRP module interaction scenarios	From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, use the command **set platform software trace** *cxpd RP active cxpd-fmanrp* **debug** This trace can be enabled to analyze the data plane programming issues from CXP.
To enable verbose level debug traces to analyze the CXP and FTM module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-ftm* **verbose** From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, *cxpd-ftm* keyword in this command is deprecated.
To enable verbose level debug traces to analyze the CXP and FMANRP module interaction scenarios	From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, use the command **set platform software trace** *cxpd RP active cxpd-fmanrp* **verbose**
To set the debug level to the notice level and to disable the CXP and FTM module interaction scenarios debugs enabled (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-ftm* **notice** From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the *cxpd-ftm* keyword in this command is deprecated.
To set the debug level to the notice level and to disable the CXP and FMANRP module interaction scenarios debugs enabled (this disables all the trace levels higher than notice)	From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, use the command **set platform software trace** *cxpd RP active cxpd-fmanrp* **notice**

Description	Command
To enable debug traces to analyze the CXP and OMP module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-omp* **debug** This trace can be enabled to analyze the CXP Gateway metrics handling issues
To enable verbose level debug traces to analyze the CXP and OMP module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-omp* **verbose**
To set the debug level to the notice level and to disable the CXP and OMP module interaction scenario debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-omp* **notice**
To enable debug traces to analyze the CXP operational commands handling	Use the command **set platform software trace** *cxpd RP active cxpd-oper* **debug**
To enable verbose level debug traces to analyze the CXP operational commands handling	Use the command **set platform software trace** *cxpd RP active cxpd-oper* **verbose**
To set the debug level to the notice level and to disable the CXP operational parsing handling debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-oper* **notice**
To enable debug traces to analyze the CXP and IOS interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-rtm* **debug**
To enable verbose level debug traces to analyze the CXP and IOS module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-rtm* **verbose**
To set the debug level to the notice level and to disable the CXP probe metrics debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-rtm* **notice**
To enable debug traces to analyze the CXP probe metrics handling issues	Use the command **set platform software trace** *cxpd RP active cxpd-telemetry* **debug**
To enable verbose level debug traces to analyze the CXP probe metrics handling issues	Use the command **set platform software trace** *cxpd RP active cxpd-telemetry* **verbose**
To set the debug level to the notice level and to disable the CXP probe metrics debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-telemetry* **notice** level
To enable debug traces to analyze the CXP and TTM module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-ttm* **debug**
To enable verbose level debug traces to analyze the CXP and TTM module interaction scenarios	Use the command **set platform software trace** *cxpd RP active cxpd-ttm* **verbose**
To set the debug level to the notice level and to disable the CXP and TTM module interaction scenarios debugs (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-ttm* **notice**

Description	Command
To enable debug traces to analyze the CXP module level issues (mostly during the bootup scenarios)	Use the command **set platform software trace** *cxpd RP active cxpd-misc* **debug**
To enable debug traces to analyze the verbose CXP module level issues (mostly during the bootup scenarios)	Use the command **set platform software trace** *cxpd RP active cxpd-misc* **verbose**
To set the debug level to the notice level and to disable the CXP module level debugs and (this disables all the trace levels higher than notice)	Use the command **set platform software trace** *cxpd RP active cxpd-misc* **notice**
To check the trace levels of different CXPD btraces enabled	Use the command **show platform software trace** *level cxpd* **RP active**
To view syslogs and console logs	Use the command **show** *sdwan notification stream viptela*