Integrate Cisco IOS XE Catalyst SD-WAN Device with Cisco ACI

Table 1: Feature History

Feature Name	Release Information	Description
Integration with Cisco ACI	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	The Cisco IOS XE Catalyst SD-WAN and Cisco ACI integration functionality now supports predefined SLA cloud beds. It also supports dynamically generated mappings from a data prefix-list and includes a VPN list to an SLA class that is provided by Cisco ACI.

Cisco ACI release 4.1(1) adds support for WAN SLA policies. This feature enables tenant administrators to apply preconfigured policies to specify the levels of packet loss, jitter, and latency for tenant traffic over the WAN. When a WAN SLA policy is applied to tenant traffic, the Cisco APIC sends the configured policies to a Cisco Catalyst SD-WAN Controller. The Cisco Catalyst SD-WAN Controller, which is configured in Cisco ACI as an external device manager that provides Cisco IOS XE Catalyst SD-WAN capabilities, chooses the best possible WAN link that meets the loss, jitter, and latency parameters specified in the SLA policy.

The WAN SLA policies are applied to tenant traffic though contracts.

As an example of where this feature can be useful, consider a deployment in which branches connect to a data center over a WAN using multiple transport technologies, such as MPLS, internet, and 4G. In such deployments, there can be multiple paths between the branches and data centers. This feature provides optimized path selection in these situations based on application groups and SLA.

- Guidelines to Integrate with Cisco ACI, on page 2
- Verify Cisco ACI Registration, on page 2
- SLA Classes, on page 2
- Data Prefixes, on page 3
- VPNs, on page 3
- Map Data Prefix and VPN to SLA, on page 3
- Create an App-Route-Policy, on page 3
- Map ACI Sites, on page 4
- Unmap ACI Sites, on page 5
- Delete a Controller, on page 5

Guidelines to Integrate with Cisco ACI

The general steps that you perform in Cisco SD-WAN Manager to configure the integration are:

1. Verify that Cisco ACI has registered the desired controller as a partner with a Cisco Catalyst SD-WAN Controller, as described in the procedure, Verify Cisco ACI Registration, on page 2.
2. Attach devices to the Cisco Catalyst SD-WAN Controller, as described in the Map ACI Sites section.

The following guidelines apply when integrating Cisco SD-WAN Manager with Cisco ACI:

- Only new Cisco IOS XE Catalyst SD-WAN deployments support this integration.
- Make sure that any devices to which the Cisco APIC sends policies do not have any application-aware routing policies configured for them.
- Make sure each device to which the Cisco APIC sends policies has an attached template.
- Before you begin the integration, use the CLI policy builder to create a centralized policy and activate it by using the Cisco SD-WAN Manager policy builder.
- Before you apply WAN SLA policies, establish a connection between the Cisco Catalyst SD-WAN Controller and the Cisco APIC. For instructions, see Cisco ACI and Cisco IOS XE Catalyst SD-WAN Integration.
- Before you attach devices, configure Cisco ACI for this integration.

Verify Cisco ACI Registration

After you configure Cisco ACI for integration with Cisco SD-WAN Manager, perform the following steps in the Cisco SD-WAN Manager to verify that Cisco ACI has registered the desired controller as a Cisco SD-WAN Manager partner:

1. In Cisco SD-WAN Manager, select **Administration** > **Integration Management**.

   The Integration Management page displays.
2. On the Integration Management page, verify that ACI Partner Registration appears in the Description for the controller to which the Cisco APIC is to send policies.

SLA Classes

Cisco SD-WAN Manager provides preconfigured SLA classes for use with the ACI integration. These SLA classes are available automatically and cannot be modified or deleted.

To view these SLA classes, follow these steps:

1. In Cisco SD-WAN Manager, select **Configuration** > **Policies**.
2. From the Custom Options drop-down menu, select **Lists**.
3. Select **SLA Class** from the type list on the left.

The following SLA classes are available:

- Business Normal—Designed for normal business operations
- Voice—Designed for voice operations
- Business Critical—Designed for critical business operations that require low packet loss and latency
- Business High—Designed for highly important business operations

Data Prefixes

Cisco ACI creates data prefix lists that are required for integration and updates these lists dynamically as required. You do not need to configure the data prefixes in Cisco SD-WAN Manager.

To view these data prefixes, follow these steps:

1. In Cisco SD-WAN Manager, select **Configuration** > **Policies**.
2. From the Custom Options drop-down menu, select **Lists**.
3. Select **Data Prefix** from the type list on the left.

Because Cisco ACI provides these data prefixes automatically, the information in this list can vary. To make sure you are viewing current information, refresh the page occasionally.

VPNs

Cisco ACI creates VPNs that are required for integration and sends them to Cisco SD-WAN Manager. These VPNs become available in Cisco SD-WAN Manager automatically. You do not need to configure the VPNs in Cisco SD-WAN Manager.

To view these VPNs, follow these steps:

1. In Cisco SD-WAN Manager, select **Configuration** > **Policies**.
2. From the Custom Options drop-down menu, select **Lists**.
3. Select **VPN** from the type list on the left.

Map Data Prefix and VPN to SLA

After Cisco ACI establishes a mapping from a data prefix list and a VPN list to an SLA class, Cisco ACI sends the mapping to Cisco SD-WAN Manager. You can view these mappings in Cisco SD-WAN Manager on the page where you configure the app route policy.

Create an App-Route-Policy

After Cisco ACI maps a data prefix and a VPN to an SLA class list, you can create an app-rout-policy to define sequence rules for the Cisco ACI integration.

To create an app-route-policy, follow these steps:

1. In Cisco SD-WAN Manager, select **Configuration** > **Policies**.
2. Click the **More Actions** icon at the right of a row that contains a centralized policy, and then click **Edit**.
3. Select **Traffic Rules**.
4. Select **Add Policy** > **Create New**.
5. Click **ACI Sequence Rules**.
6. From the VPN drop-down, choose a VPN ID. Cisco SD-WAN Manager displays a list of data prefixes and SLA classes that are mapped to this VPN. (These mappings were sent by Cisco ACI.)
7. Check the box to the left of the data prefix and SLA class that you want to include with the policy, and then click **Import**.
8. Enter a name for the policy in the Name field and a description of the policy in the Description field, and then click **Save Application Aware Routing Policy**. Cisco SD-WAN Manager creates the policy.
9. To apply a site list and a VPN list to the policy, select **Policy Application**, then select **Application-Aware Routing**, and click **New Site Lists and VPN List**.
10. Select a site list and a VPN list for the policy.
11. Add sequence rules to the policy as needed.
12. Click **Save Policy Changes**.

Map ACI Sites

Mapping ACI sites designates the controller devices to which the policies from Cisco APIC apply.

Before you begin, review the guidelines in the Guidelines to Integrate with Cisco ACI section.

To attach devices to a controller, follow these steps:

1. In Cisco SD-WAN Manager, select **Administration** > **Integration Management**.
2. Click the **More Actions** icon to the right of the row for the applicable site and select **Attach Devices**.
3. In the Available Devices column on the left, select a group and search for one or more devices, select a device from the list, or click **Select All**.
4. Click the arrow pointing right to move the device to the Selected Devices column on the right.

Note To remove devices from the Selected Devices column, in that column select a group and search for one or more devices, select a device from the list, or click **Select All**, and then click the arrow pointing left.

5. Click **Attach**.

Unmap ACI Sites

Unmapping ACI sites stops Cisco APIC policies from being applied to the unmapped devices.

To detach devices from a controller, follow these steps:

1. In Cisco SD-WAN Manager, select **Administration** > **Integration Management**.

   The Integration Management page displays.

2. Click the **More Actions** icon to the right of the row for the applicable site and select **Detach Devices**.
3. In the Available Devices column on the left, select a group and search for one or more devices, select a device from the list, or click **Select All**.
4. Click the arrow pointing right to move the device to the Selected Devices column on the right.

Note To remove devices from the Selected Devices column, in that column select a group and search for one or more devices, select a device from the list, or click **Select All**, and then click the arrow pointing left.

5. Click **Detach**.

Delete a Controller

If you want to remove a controller as a partner with Cisco ACI, we recommend that you remove its registration by using Cisco ACI instead of deleting it in Cisco SD-WAN Manager. Deleting an ACI partner from Cisco SD-WAN Manager automatically deletes the data prefixes and VPNs that Cisco ACI created for the partner.

Before you begin, remove from policy definitions and data prefix lists and VPN lists that ACI created and make sure that these lists are not referenced from any policy.

1. In Cisco SD-WAN Manager, select **Administration** > **Integration Management**.
2. Detach all devices that are attached to the controller.

   For instructions, see the Detach Devices from a Controller section.

3. Click the **More Actions** icon to the right of the row for the applicable site and select **Delete Controller**.