

Cisco SD-AVC Cloud Connector

- Cisco SD-AVC Cloud Connector feature history, on page 1
- Enable Cisco SD-AVC Cloud Connector, Cisco Catalyst SD-WAN Manager Release 20.14.1 and Later, on page 2
- Enable Cisco SD-AVC Cloud Connector, through Cisco Catalyst SD-WAN Manager Release 20.13.x, on page 3
- Enable Cloud Services, on page 8

Cisco SD-AVC Cloud Connector feature history

Table 1: Feature History

Feature Name	Release Information	Description
Cisco SD-AVC Cloud Connector	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	When enabling Cloud onRamp for SaaS to manage Office 365 traffic, you can limit best path selection to apply only to some Office 365 traffic, according to the Office 365 traffic categories defined by Microsoft, or to include all Office 365 traffic. The Cisco SD-AVC Cloud Connector provides support for this functionality.
Update to the SD-AVC Cloud Connector Enablement	Cisco vManage Release 20.10.1	Beginning with this release, enabling the Cloud Connector requires a cloud gateway URL and a one-time password (OTP) instead of a client ID and client secret.
New Procedure for Enabling Cisco SD-AVC Cloud Connector	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Control Components Release 20.14.1	This release introduces a new procedure for enabling Cisco SD-AVC Cloud Connector from the Cloud Services option in **Administration** > **Settings**. From this release, enabling Cloud Connector does not require an OTP or opening a TAC case.

Enable Cisco SD-AVC Cloud Connector, Cisco Catalyst SD-WAN Manager Release 20.14.1 and Later

Before Cisco Catalyst SD-WAN Manager Release 20.14.1, client ID, client secret credentials, and sometimes a cloud gateway URL and OTP were required to enable Cloud Connector. From Cisco Catalyst SD-WAN Manager Release 20.14.1, you can configure Cisco SD-AVC Cloud Connector using the Cloud Services page. With this feature, you need not retrieve an OTP or create a TAC case separately to enable SD-AVC Cloud Connector.

Prerequisites

Enable Cisco SD-AVC under **Administration** > **Cluster Management** to enable Cloud Connector.

Enable Cisco SD-AVC Cloud Connector Using Cloud Services

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **Cloud Services**.
3. Enable **Cloud Services** in the **Cloud Services** tab.

   From Cisco Catalyst SD-WAN Manager Release 20.18.2, after you enable Cloud Services, click **Register** in the **Cisco services onboarding popup** that appears and enter your Smart Account credentials.

   Alternatively, from Cisco Catalyst SD-WAN Manager Release 20.18.2, you can authenticate for Cloud Services from the **Cisco services registration** page.
4. Enter your Smart Account credentials.
5. (Optional) Enable **Analytics**.



Note Enable this option only if you have deployed Cisco Catalyst SD-WAN Analytics, and have confirmed that it is reachable by Cisco SD-WAN Manager.

6. Enable **SD-AVC Cloud Connector**.



Note If Cisco SD-WAN Manager is cloud-hosted by Cisco, this option does not appear and Cloud Connector is enabled automatically after you enable the Cloud Services option.

7. Click **Save**.

Enable Cisco SD-AVC Cloud Connector, through Cisco Catalyst SD-WAN Manager Release 20.13.x

Before You Begin

- Before Cisco vManage Release 20.10.1, enabling Cloud Connector required client ID and client secret credentials. From Cisco vManage Release 20.10.1, it requires a cloud gateway URL and OTP. An advantage to using an OTP is that, in contrast to a client secret, it does not expire. See the following table for details about the credentials required for different releases, upgrade scenarios, and hosting options.
- Cisco SD-AVC Cloud Connector is a necessary component for Cloud onRamp for SaaS to manage Office 365 traffic according to the Office 365 traffic category.

Table 2: Requirements to Enable SD-AVC Cloud Connector

Releases	Cisco SD-WAN Manager Hosting	Requirements to Enable Cloud Connector
Cisco vManage Release 20.3.1 to Cisco vManage Release 20.9.x	All hosting options	**Required credentials**: Client ID Client secret (As explained in the procedure, open the Cisco API Console page to create Cloud Connector credentials if you do not already have credentials.) **Note** When you receive a message in Cisco SD-WAN Manager indicating that SD-AVC credentials are expiring, return to the Cisco API Console and create new Cloud Connector credentials. **Other requirements**: Enable SD-AVC in cluster management, as described here.

Releases	Cisco SD-WAN Manager Hosting	Requirements to Enable Cloud Connector
Upgrade an existing instance to Cisco vManage Release 20.10.1 from an earlier release	All hosting options	**Notes**: In this scenario, the SD-AVC components operate differently than in earlier releases. Consequently, running the **request nms all status** command on the Cisco SD-WAN Manager instance shows that the "NMS SDAVC server" component is not enabled. This is expected behavior, and does not indicate any problem with SD-AVC. Note that the "NMS SDAVC gateway" component shows as enabled.
	Cisco-hosted	**Required credentials**: • Cloud gateway URL: Use: https://datamanagement-us01.sdwan.cisco.com/validate_sdavc/ • OTP: Use the Cisco Catalyst SD-WAN Portal to get the OTP. See the Cisco Catalyst SD-WAN Portal Configuration Guide for details. **Other requirements**: Enable SD-AVC in cluster management, as described here.
	Self-managed, hosted in a public cloud, a private cloud, or on-premises	

Releases	Cisco SD-WAN Manager Hosting	Requirements to Enable Cloud Connector
		Required credentials: • If Cloud Connector was already enabled at the time of the upgrade, the client ID and client secret credentials continue to work until the client secret expires. When the client secret expires, an alarm appears in Cisco SD-WAN Manager to indicate the expiration. At this point, enabling Cloud Connector requires the cloud gateway URL and OTP. Use datamanagement-us-01.sdwan.cisco.com for the URL, and open a TAC case to get the OTP. See the procedure in this section for information about opening a TAC case. • If Cloud Connector was not enabled at the time of the upgrade, enabling Cloud Connector requires the cloud gateway URL and OTP. Use datamanagement-us-01.sdwan.cisco.com for the URL, and open a TAC case to get the OTP. See the procedure in this section for information about opening a TAC case. **Other requirements**: Before enabling the Cloud Connector, enable SD-AVC in cluster management, as described here.

Releases	Cisco SD-WAN Manager Hosting	Requirements to Enable Cloud Connector
Fresh installation of Cisco vManage Release 20.10.1 and later	Cisco-hosted	**Required credentials**: Cloud Connector is enabled by default, without requiring manual entry of credentials. You can use the Cisco Catalyst SD-WAN Portal to view the OTP if needed. See the Cisco Catalyst SD-WAN Portal Configuration Guide for details. **Other requirements**: Enable SD-AVC in cluster management, as described here. **Notes**: In this scenario, the SD-AVC components operate differently than in earlier releases. Consequently, running the **request nms all status** command on the Cisco SD-WAN Manager instance shows that the "NMS SDAVC server" component is not enabled. This is expected behavior, and does not indicate any problem with SD-AVC. Note that the "NMS SDAVC gateway" component shows as enabled.
	Self-managed, hosted in a public cloud, a private cloud, or on-premises	**Required credentials**: • Cloud gateway URL: Use https://datamanagement-us-01.sdwan.cisco.com/validate_sdavc/ • OTP: Open a TAC case to get the OTP. See the procedure in this section for information about opening a TAC case. **Other requirements**: Enable SD-AVC in cluster management, as described here.

Enable Cisco SD-AVC Cloud Connector

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

2. Click **SD-AVC** and enable **Cloud Connector**.

   (If you are using Cisco vManage Release 20.10.x, Cisco vManage Release 20.11.x, or Cisco Catalyst SD-WAN Manager Release 20.12.x, click **Edit** and enable **Cloud Connector**.)

   (In Cisco vManage Release 20.9.x and earlier releases, the option is called **SD-AVC Cloud Connector**. In these releases, click **Edit** and enable **Cloud Connector**.)



Note If Cisco SD-WAN Manager is cloud-hosted by Cisco, this option does not appear and Cloud Connector is enabled automatically.

3. (This step applies to Cisco vManage Release 20.10.1 and later, and is handled automatically if Cisco SD-WAN Manager is Cisco-hosted.)

   See the **Before You Begin** section that precedes these steps for details about the requirements for enabling the SD-AVC Cloud Connector in different scenarios. As noted there, enable SD-AVC in cluster management before enabling the Cloud Connector.

   If you need to enter the cloud gateway URL, use: datamanagement-us-01.sdwan.cisco.com

   If you need to use the Cisco Catalyst SD-WAN Portal to get the OTP, see the Cisco Catalyst SD-WAN Portal Configuration Guide for details.

   If you need to open a TAC case to receive the OTP, open https://mycase.cloudapps.cisco.com/case. The workflow for receiving the OTP requires the following:

   - Entitlement information.
   - Smart Account.
   - Virtual Account.
   - The organization name configured in Cisco SD-WAN Manager.
   - Cisco SD-WAN Manager geographic location: Americas, European Union (EU), or Asia-Pacific (APAC).
   - Technology: Use Cisco Catalyst SD-WAN On-Prem for an on-prem installation or Cisco Catalyst SD-WAN - Cisco-Hosted for a Cisco-hosted installation.
   - SubTechnology: Use SDWAN Cloud Infra.

4. (For Cisco vManage Release 20.9.x and earlier releases) Enter the following credentials:

   - Client ID



Note Click (**i**) for **Client ID** and open the Cisco API Console page in a browser window to create Cloud Connector credentials if you do not already have credentials.

   - Client Secret
   - Organization Name: Use the descriptive name that you entered on the Cisco API Console page in the **Name of your application** field.

5. (Releases earlier than Cisco vManage Release 20.10.1) For **Affinity**, you can select a geographical location for storing the Cloud Connector data. For organizations located in Europe, it is recommended to change the location to Europe, in accordance with EU General Data Protection Regulation (GDPR) regulations.
6. For **Telemetry**, you can optionally disable the collection of telemetry data.

Note If Cisco SD-WAN Manager is cloud-hosted by Cisco, this option does not appear and telemetry is enabled automatically.

Create Credentials on the Cisco API Console

The following steps show how to create credentials in the Cisco API Console. These steps are provided here for convenience, and are subject to change.

1. On the Cisco API Console page, sign in using your Cisco credentials.
2. Click **My Apps and keys**. A page opens for registering a new application.
3. To register SD-AVC, follow the steps below:
   a. Name of your application: Use any descriptive name. Save this name for a later step.
   b. In the **Application Type** area, click Service.
   c. In the **Grant Type** area, check the **Client Credentials** check box.
   d. Check the **Hello API** check box.
   e. In the **Terms of Service** section, check the check box to agree with the terms.
   f. Click **Register**. The Cisco API Console page displays the Client ID and Client Secret details. Keep this page open to complete the procedure.

Note When you receive a message in Cisco SD-WAN Manager indicating that SD-AVC credentials are expiring, return to the Cisco API Console and create new Cloud Connector credentials.

Enable Cloud Services

While a Protocol Pack upgrade for devices in the network is in process, or is scheduled and pending, you cannot enable Cloud Services.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

Step 2 Click **Cloud Services**.

Step 3 Enable **Cloud Services** in the **Cloud Services** tab.

Step 4 Enter your Smart Account credentials in the fields.

Step 5 (Optional) Enable **Analytics**.

Note
Enable this option only if you have deployed Cisco SD-WAN Analytics, and have confirmed that it is reachable by Cisco SD-WAN Manager.

Step 6 Click **Save**.