Cisco SD-AVC

Cisco SD-AVC feature history

Table 1: Feature History

Feature Name	Release Information	Feature Description
Default Enablement of SD-AVC	Cisco Catalyst SD-WAN Control Components Release 20.18.1	The Cisco SD-AVC component is enabled by default in new Cisco Catalyst SD-WAN environments. The control for enabling or disabling is in **Administration** > **Settings** > **SD-AVC**.
Cloud-hosted SD-AVC Service for On-premises Environments	Cisco Catalyst SD-WAN Control Components Release 20.18.1	This release extends the use of a cloud-hosted SD-AVC service to on-premises installations of Cisco Catalyst SD-WAN where internet access is available.

Cisco SD-AVC

Default enablement

From SD-WAN Control Components 20.18.1, the SD-AVC component is enabled by default in new Cisco Catalyst SD-WAN installations. The enablement applies to all Cisco SD-WAN Manager nodes.

Upgrade from releases earlier than SD-WAN Control Components 20.18.1

For Cisco Catalyst SD-WAN environments that have been upgraded from releases earlier than SD-WAN Control Components 20.18.1, SD-AVC is not necessarily enabled. The status of SD-AVC enablement before upgrade is preserved after upgrade. The control for enabling or disabling is in **Administration** > **Settings** > **SD-AVC**.

Cloud-hosted SD-AVC service

From Cisco Catalyst SD-WAN Control Components Release 20.10.1, some Cisco Catalyst SD-WAN environments have used a cloud-hosted SD-AVC service instead of a local service. Specifically, these installation types have used cloud-hosted SD-AVC:

- Cisco Cloud-delivered Catalyst SD-WAN
- Cisco Hosted Catalyst SD-WAN

Cisco Catalyst SD-WAN Control Components Release 20.18.1 extends the use of the cloud-hosted SD-AVC service to on-premises installations of Cisco Catalyst SD-WAN where internet access is available, and where Cloud Services are enabled. In air-gapped environments without internet access, or if the Cloud Services feature is not enabled, Cisco Catalyst SD-WAN uses a local SD-AVC service.

Benefits of the cloud-hosted SD-AVC service

- Resources

  Using the cloud-hosted SD-AVC service reduces the load on SD-WAN Manager host resources.

- Service maintenance

  Cisco can provide patches to the cloud-hosted SD-AVC service at any time, optimizing SD-AVC operation.

Supported solutions for the cloud-hosted SD-AVC service

SD-WAN

Restrictions for the cloud-hosted SD-AVC service

- Compliance for government installations

  For compliance reasons, some government installations of Cisco Catalyst SD-WAN do not use all available cloud services, including cloud-hosted SD-AVC.

- Upgrade information

  This information is relevant only if you have upgraded your Cisco Catalyst SD-WAN environment from a release earlier than Cisco Catalyst SD-WAN Control Components Release 20.18.1.

Upgraded from	Conditions	Result
Release earlier than Cisco Catalyst SD-WAN Control Components Release 20.18.1	Cloud services and SD-AVC enabled	The upgraded environment uses the cloud-hosted SD-AVC service.
	Either Cloud Services disabled, or SD-AVC disabled	The upgraded environment uses the local SD-AVC service. After upgrading, if you enable Cloud Services (**Administration** > **Settings** > **Cloud Services**), the environment switches to using the cloud-hosted SD-AVC service.

Install Cisco SD-AVC, Cisco vManage Release 20.3.1 and Later

Installing or upgrading to Cisco vManage Release 20.3.1 automatically includes installation of Cisco SD-AVC as a component.

For information about Cisco SD-AVC, see Cisco SD-AVC.

Enable Cisco SD-AVC, Cisco vManage Release 20.3.1 through SD-WAN Manager 20.16.x

Enabled by default

From SD-WAN Manager 20.18.1, SD-AVC is enabled by default.

Prerequisites

Ensure that routers in the network that are included in the Cisco Catalyst SD-WAN topology have a DNS server configured.

Note Cisco SD-AVC must operate on only one Cisco SD-WAN Manager instance. In a Cisco SD-WAN Manager cluster, enable Cisco SD-AVC on only one instance of Cisco SD-WAN Manager.

To enable Cisco SD-AVC, perform the following steps.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.
2. For the desired host (the portal on which you are enabling SD-AVC), click **...** and select **Edit**.
3. In the **Edit Manager** pop-up window, select the checkbox for **Enable SD-AVC**.

Note The **Edit Manager** pop-up window provides an option for disabling the application server. After disabling the application server, you cannot later enable other services using this method. If you need to disable the application server, do not do this at the same time that you enable other features.

4. Enter the username and password, using Cisco SD-WAN Manager credentials. Reboot the device to apply the changes.
5. After the reboot, Cisco SD-WAN Manager comes up automatically and displays progress on the SD-AVC activation. Wait for the activation to complete.
6. (optional) After installation is complete, you can verify that Cisco SD-WAN Manager has the SD-AVC virtual service installed and operating correctly.
    a. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.
    b. Click **Service Configuration**, in the Cisco SD-WAN Manager row of the table. Verify that SD-AVC indicates that it is reachable.

Enable SD-AVC on Cisco IOS XE Catalyst SD-WAN Devices

To enable SD-AVC on the Cisco IOS XE Catalyst SD-WAN device, create a localized policy that enables **app visibility** and apply the policy to the template for the Cisco IOS XE Catalyst SD-WAN device.

Prerequisites

- A template exists for the Cisco IOS XE Catalyst SD-WAN device (example: Cisco ASR 1001-X, Cisco ISR 4321).
- TCP port 10501 destination traffic must be permitted.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. To add a policy and enable Application, follow the steps below:
    a. Click **Add Policy**.
    b. Click **Next** on the several screens (Create Groups of Interest, Configure Forwarding Classes/QOS, Configure Access Control Lists, Configure Route Policy) until the **Policy Overview** screen.
    c. In the **Policy Overview** screen, enter a policy name and policy description.
    d. Select **Application**.
    e. Save the policy.
4. To add the localized Policy to the device template, follow the steps below:
    a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
    b. For the device on which you have to enable SD-AVC, click **…** and select **Edit** from the menu.
    c. Click **Additional Templates**.
    d. Add the localized policy created in an earlier step of this procedure.
    e. Click **Update** and proceed through the next screens to push the updated template to the device.

5. (Optional) After pushing the update to the device, you can check the status of SD-AVC on the device with one of the following commands.

   ```
   show avc sd-service info summary
   ```

   or

   ```
   show avc sd-service info connectivity
   ```

Installing Cisco SD-AVC, Cisco vManage 20.1.1 and Earlier

Note Beginning with Cisco vManage Release 20.3.1/Cisco IOS XE Catalyst SD-WAN Release 17.3.1a, the Cisco SD-AVC installation has changed. See Install Cisco SD-AVC, Cisco vManage Release 20.3.1 and Later, on page 3.

Overview

Beginning with the 18.4 release, Cisco Catalyst SD-WAN can optionally incorporate Cisco Software-Defined Application Visibility and Control (SD-AVC) on Cisco IOS XE Catalyst SD-WAN devices. The SD-AVC network service operates as a container within Cisco SD-WAN Manager.

What are the benefits of this feature?

Cisco SD-AVC uses Cisco NBAR2 and other components that operate on devices in the network to provide:

- Recognition of network application traffic for visibility, analytics, application-aware routing, and application-based policies, such as QoS and application-based firewall policy.
- Analytics at the network level.

Cisco SD-AVC Installation Requirements for Cisco SD-WAN Manager

The following table describes the SD-AVC installation requirements.

Cisco SD-WAN Manager Installation Scenario	Requirements
Cisco vManage 18.4 on a cloud-based server, provided fully configured by the Cisco cloud operations team	The SD-AVC package is pre-installed by the Cisco cloud operations team.
Cisco vManage 18.4 on a self-managed cloud or local server	Install the SD-AVC package as described below.
Upgrading from an earlier version of Cisco SD-WAN Manager to Cisco vManage 18.4	Install the SD-AVC package as described below.

Enabling SD-AVC on Cisco SD-WAN Manager

Prerequisites

- Download the latest container image for the SD-AVC network service. Save the file to an accessible location on the server hosting Cisco SD-WAN Manager. This container is required for the procedure. To download the container, open the Cisco Software Download page and enter "SD-WAN". Select "Software-Defined WAN (SD-WAN)" from the results, then "SD-WAN" in the results. In the software packages available for download, select SD-AVC.
- Ensure that routers in the network that are included in the SD-WAN topology have a DNS server configured.
- The virtual machine in which Cisco SD-WAN Manager operates must have the following resources available to dedicate to the SD-AVC network service:
  - vCPU: 4
  - RAM: 5 GB
  - Storage: 40 GB

Procedure

1. Ensure that the downloaded SD-WAN image is compatible with your version of Cisco SD-WAN Manager.
   a. Display the checksum for the compatible image, using the following API:

      https://*[vManage-IP-address]*/dataservice/sdavc/checksum

      Example: https://10.0.0.1/dataservice/sdavc/checksum

   b. Verify that the checksum of the downloaded image matches this.
2. To upload the SD-AVC virtual service package to Cisco SD-WAN Manager:
   a. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Software Repository**.

   b. Click **Virtual Images** and select **Upload Virtual Image** to upload the SD-AVC package.
3. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management** page.
4. For the desired host (the Cisco SD-WAN Manager portal on which you are enabling SD-AVC), click **…** and choose **Edit**.
5. In the Edit Cisco SD-WAN Manager dialog box, enter the username and password, using Cisco SD-WAN Manager credentials.
6. Select the checkbox for **Enable SD-AVC**. Click **Update**.
7. Cisco SD-WAN Manager prompts you to confirm before rebooting the device to apply the changes to the device. Click **OK** to confirm.
8. After the reboot, Cisco SD-WAN Manager comes up automatically and displays progress on the SD-AVC activation. Wait for the activation to complete.

9. (Optional) After installation is complete, you can verify that Cisco SD-WAN Manager has the SD-AVC virtual service installed and operating correctly.
   a. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.
   b. In Service Configuration, in Cisco SD-WAN Manager row of the table, verify that the SD-AVC shows a green checkmark.

For information about Cisco SD-WAN Manager commands, see *Cisco SD-WAN Manager Command Reference* documentation.

Enable SD-AVC on Cisco IOS XE Catalyst SD-WAN Devices

To enable SD-AVC on the Cisco IOS XE Catalyst SD-WAN device, create a localized policy that enables **app visibility** and apply the policy to the template for the Cisco IOS XE Catalyst SD-WAN device.

Prerequisites

- A template exists for the Cisco IOS XE Catalyst SD-WAN device (example: Cisco ASR 1001-X, Cisco ISR 4321).
- TCP port 10501 destination traffic must be permitted.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policies**.
2. Click **Localized Policy**.
3. To add a policy and enable Application, follow the steps below:
   a. Click **Add Policy**.
   b. Click **Next** on the several screens (Create Groups of Interest, Configure Forwarding Classes/QOS, Configure Access Control Lists, Configure Route Policy) until the **Policy Overview** screen.
   c. In the **Policy Overview** screen, enter a policy name and policy description.
   d. Select **Application**.
   e. Save the policy.
4. To add the localized Policy to the device template, follow the steps below:
   a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
   b. For the device on which you have to enable SD-AVC, click **…** and select **Edit** from the menu.
   c. Click **Additional Templates**.
   d. Add the localized policy created in an earlier step of this procedure.
   e. Click **Update** and proceed through the next screens to push the updated template to the device.
5. (Optional) After pushing the update to the device, you can check the status of SD-AVC on the device with one of the following commands.

```
show avc sd-service info summary
```

or

```
show avc sd-service info connectivity
```