Using SD-AVC

Using SD-AVC

Functionality	See...
Connect to the SD-AVC Dashboard	Connecting to the Dashboard, on page 1
View traffic analytics interactively, monitor devices operating with SD-AVC	Application Visibility Page, on page 2
Upload and deploy Protocol Packs	Protocol Packs Page, on page 6
View details of external sources of application classification	Cloud Connector Page, on page 8
View system information, application rules, and debugging tools	Serviceability Page, on page 11 Application Rules Page, on page 14

Connecting to the Dashboard

Using a browser (Chrome recommended) with access to the device hosting the SD-AVC Network Service, open the SD-AVC Dashboard. The Dashboard is accessible using the service IP configured when setting up the SD-AVC Network Service, and port 8443, in the format:

https://<service-ip>:8443

Example:

```
https://10.56.196.153:8443
```

Note   The SD-AVC Dashboard uses the same authentication as the platform hosting the SD-AVC Network Service. The host platform may use locally configured usernames and passwords, or it may use other methods, such as an Authentication, Authorization, and Accounting (AAA) server.

If prompted, enter the username and password used on the host platform.

Application Visibility Page

The **Application Visibility** page shows network activity handled by the devices in the network operating with SD-AVC, as well as displaying any warnings or errors for each device.

Table 1: Top of Window

Information/Control	Description
All Devices	Indicates that the application data displayed in this window includes traffic handled by all devices in the network that are operating with SD-AVC.
Time Range	Time range for application data displayed on this page.

Table 2: Summary Pane

Information/Control	Description
Classification Score	Last measured classification quality score for the device. This indicates the degree of classification quality (specificity), calculated according to traffic volume. Higher score indicates better quality.
Unclassified Traffic Discovery button ( )	Displays details of unclassified traffic. See Viewing Unclassified Traffic Details, on page 5. To return, use the menu in the **Timeline** pane.
First Packet Classification	Ratio of flows classified on the first packet, to total TCP/UDP flows.
Total Usage	Total traffic volume handled in the selected time range.
SD-AVC Coverage Ratio	Ratio of flows covered by the SD-AVC application rules pack, to the total number of TCP/UDP flows.
Asymmetric Index	Last measured degree of asymmetry seen by device. This is the ratio of asymmetric flows to total flows for TCP and DNS traffic. 0 is least asymmetry, and 10 is highest asymmetry.

Information/Control	Description
Timeline	Graph of one of the following (select in dropdown menu): • Bandwidth • Classification score • First packet classification score • SD-AVC coverage ratio • Unclassified Traffic

Table 3: Applications by Usage Pane

Information/Control	Description
Table of applications	Usage and business relevance for each network application. Select one or more applications to display data for the applications in the **Timeline** pane. Use the Search field to filter the display of traffic.

Table 4: SD-AVC Monitoring Pane

Information/Control	Description
Note: When filtering to display data for a single segment or device, this pane displays information for that segment or device.	
Segment	Network segments. Click to filter display by a network segment.
Devices	Number of devices in the network. Click the magnifying glass to list devices, and for filtering options. Device warnings and alerts. Click the warning/alert for details
Installed Protocol Packs	Protocol Packs installed on devices in the network.

Table 5: Business Relevance Pane

Information/Control	Description
Business Relevance Graph	**Note** Because business relevance depends on the network segment, this information is displayed when a single network segment or device is selected. Indicates portions of traffic classified as: • Business-relevant • Business-irrelevant • Default

Unclassified Traffic Analysis and Discovery

Background

The **SD-AVC Dashboard** > **Application Visibility** page shows a summary of network traffic, including a table of network applications, organized by network usage.

Traffic that has been identified and classified as belonging to a specific network application appears in the table by name.

Traffic that is not classified by Protocol Pack or external sources (example: MS-Office365) is called unclassified traffic. Unclassified traffic reduces the traffic classification score. Unclassified traffic appears as:

Label	Description
HTTP	Generic host, HTTP traffic
SSL	Generic host, SSL/HTTPS traffic
Unknown	Unknown socket

In the following example, WebEx Meeting traffic has been identified. Unclassified traffic is listed as **HTTP** and **Unknown**.

Application	Usage	Business Relevance
HTTP	0.00% (3.96 MB)	default
WebEx Meeting	6.84% (91.58 GB)	relevant
Unknown	6.35% (84.98 GB)	default

Partial Classification of Traffic

To improve traffic visibility and the classification score, SD-AVC analyzes top hosts and sockets that appear in unclassified traffic. For those using significant bandwidth, it provides a best-effort partial classification of the otherwise unclassified traffic. The process is dynamic, adapting to the network traffic of a given period.

Unclassified traffic that impacts the classification score by 1% or more meets the threshold for partial classification.

On the **SD-AVC Dashboard** > **Application Visibility** page, the partial classification appears as host or socket information in the traffic table.

Example:

- Unclassified HTTP traffic from the **am.cisco.com** domain

- Traffic on an unknown socket, with **source 128.107.107.107**, **port 50000**, using the **UDP** transport protocol

Application	Usage	Business Relevance
HTTP > am.cisco.com	7.44% (99.60 GB)	default
WebEx Meeting	6.84% (91.58 GB)	relevant
Unknown	6.35% (84.98 GB)	default
Unknown > 128.107.107.107:50000_UDP	1.94% (25.97 GB)	default

In the table, **HTTP**, **SSL**, or **Unknown** can refer to a single unclassified flow or an aggregate of numerous unclassified flows. In the example, numerous unclassified flows are represented by a single line: **Unknown**. The unclassified flows included in that line are each below the threshold for automatic partial classification, but together they total 6.35% of bandwidth.

Viewing Unclassified Traffic Details

On the **SD-AVC Dashboard** > **Application Visibility** page, in the **Summary** pane, click the **Unclassified traffic discovery** button ( ) to display detailed information for unclassified and partially classified traffic.

- The timeline changes mode to show unclassified traffic.

- The traffic table shows all unclassified and partially classified traffic.

As with the default view, you can select items in the traffic table to display their contribution to total traffic bandwidth in the timeline.

To return to the default view, select **Bandwidth** from the dropdown menu in the **Timeline** pane.

Improves Visibility, Does Not Affect Policy

Partial classification of traffic, as described here, improves application visibility, and improves the overall classification score.

Partial classification is dynamic, adapting to current traffic, so it not applied to security (firewall) or QoS policies.

Features affected by partial classification:

- Application visibility (FNF, performance-monitor, ezPM, MACE, ...)

Features not affected by partial classification:

- MQC/QoS

- WAAS

- Performance Routing (PfR)

- NAT

Enabling and Disabling

To enable or disable the feature, use the control in:

SD-AVC Dashboard > **Serviceability** > **System**

See Serviceability Page, on page 11.

Notes and Limitations

See SD-AVC Notes and Limitations.

Protocol Packs Page

The **SD-AVC Dashboard** > **Protocol Packs** page lists devices in the network, with Protocol Pack information for each.

Click **Manage & Deploy** to:

- Add Protocol Pack files to the repository, either from a local drive or by importing directly from Cisco. (Each Protocol Pack release may include one or more file versions, for compatibility with different devices in the network. Importing a Protocol Pack directly from Cisco automatically imports all file versions.) Protocol Packs in the repository are available to deploy to devices in the network.

- Deploy Protocol Packs to devices in the network.

Understanding Protocol Pack Files

Cisco releases Protocol Packs on an ongoing basis. Each Protocol Pack release provides updates that expand and improve AVC application recognition. When a new Protocol Pack is released, the SD-AVC Dashboard displays an alert on the **Application Visibility** page, in the **Devices** pane.

Typically, it is recommended to use the latest Protocol Pack compatible with the OS running on a device. The Protocol Library page indicates the latest Protocol Pack and provides compatibility information.

SD-AVC can import Protocol Packs directly from Cisco. Alternatively, Protocol Packs can be downloaded using the Cisco Software Download tool. When using the tool, specify a platform and then navigate to software downloads for the platform.

Protocol Pack filename format:

pp-adv-<platform-type>-<OS>-<engine-id>-<protocol-pack-version>.pack

Platform type may be, for example, asr1k, csr1000v, or isr4000. However, a Protocol Pack may be installed on any compatible device, even if that device is not indicated by the filename.

Importing the Latest Protocol Packs Directly from Cisco

When Cisco releases a new Protocol Pack, the SD-AVC Dashboard displays an alert on the Application Visibility page, in the Devices pane. Click the alert indicator to view details. SD-AVC can import the latest Protocol Pack release directly from Cisco, adding it to the repository. The Protocol Pack can then be deployed to devices in the network.

Step 1   **Protocol Packs** page > **Manage & Deploy** button > **Protocol Pack Repository** > **Import from cloud**

Step 2   If new Protocol Packs are available, they appear in a list. Select the Protocol Pack to import.

Uploading Protocol Packs from a Local Drive to the SD-AVC Repository

Use the SD-AVC network service to deploy Protocol Packs to participating devices in the network.

Step 1   Select a Protocol Pack to deploy (typically the latest Protocol Pack compatible with the OS running on a device). See the Protocol Library page for compatibility information.

Step 2   Download the Protocol Pack using the Cisco Software Download tool. In the filename of the downloaded Protocol Pack, note the engine ID.

Step 3   In the SD-AVC Dashboard, upload the Protocol Pack file into the Protocol Pack repository. The repository is stored on the device hosting the SD-AVC network service.

Protocol Packs page > **Manage & Deploy** button > **Protocol Pack Repository** > **Import from file system**

Deploying Protocol Packs to Devices

✎

Note   In SD-AVC high availability configurations, if a device switches over to its secondary SD-AVC network service, then switches back to its primary, the device has a temporary "switchback" status. During this brief period, you cannot deploy Protocol Packs to the device. See SD-AVC High Availability.

Step 1   Open the SD-AVC Dashboard Protocol Packs page.

Protocol Packs page > **Manage & Deploy** button > **Deploy to...**

Step 2   In the **Protocol Pack Repository** pane, select a Protocol Pack or the **Builtin** option.

The **Builtin** option re-installs the original built-in Protocol Pack that was included with the OS (for example, Protocol Pack 33.0.0 for Cisco IOS-XE Fuji 16.7.1).

Step 3   In the **Deploy to...** pane, select a segment and one or more devices, then click **Continue**.

Note   After selecting a Protocol Pack, only devices running an IOS version compatible with the Protocol Pack can be selected.

Step 4   Select the time to deploy the Protocol Pack(s), then click **Continue**.

Step 5   Review the deployment plan and click the **Deploy** button.

Note   To return to an earlier step, click the step number.

Cloud Connector Page

The **Cloud Connector** page displays additional sources of application information used for classifying network traffic.

The **Cloud Connector** option in the left pane indicates the status as Connected or Not Connected, and indicates whether any issues are affecting operation of the Cloud Connector.

Note   This page replaces the **External Sources** page that appeared in earlier SD-AVC releases.

Source	Description
Cloud Updates	Provides application data from multiple external sources.
MS Office 365 Web Service	Provides domain names used by Microsoft Office 365. Click the **View Details** button for details about each domain. **Note** Beginning with SD-AVC 3.0.0, MS Office 365 Web Service operates through Cloud Connector. When Cloud Connector is enabled, MS Office 365 Web Service is automatically enabled also. In earlier releases, this component was called MS Office 365 Connector.

Cloud Connector

Beginning with the Cisco SD-AVC 3.0.0 release, SD-AVC connects to a cloud service provided by Cisco that improves traffic classification. The server addresses used by public internet sites and services change continually. Cisco Cloud Connector uses the latest information available to improve SD-AVC classification of traffic previously classified only in generic terms. For example, without Cloud Connector enabled, traffic from a web application using an unknown server might be classified simply as SSL, without any additional details. When enabled, Cloud Connector might be able to provide additional up-to-date details about this traffic.

To benefit from this service, enable the Cloud Connector in SD-AVC.

By default, SD-AVC shares telemetry with the cloud service to improve classification throughout the network.

The Cloud Connector setup provides an option to select the location for storing your telemetry data, for compliance with EU General Data Protection Regulation (GDPR) regulations.

Enabling Cloud Connector in SD-AVC also enables the MS Office 365 Web Service, which was configured separately in earlier SD-AVC releases.

Telemetry Data Collection

The NBAR component of SD-AVC is configured to automatically connect and transmit telemetry data, in near real time, to Cisco. Telemetry information will be used by Cisco to improve SD-AVC functionality and facilitate development of new features that result in increased value. Telemetry information is transported securely to keep customer data private. Data collected includes general administrative information (such as SD-AVC IP address and telemetry status), cache rules (such as application name, IP addresses, and socket rating), unclassified and generic traffic (such as SSL and HTTP), analytics protocol discovery (such as number of active flows, number of TCP flows, and number of DNS flows), device information (such as deployed engine versions), and protocols information (such as application name and application attributes). Users may opt out of data collection for certain telemetry categories by turning this feature off in the "Settings" tab on the "Cloud Connector" page.

Enabling the Cloud Connector

Prerequisites

- **Cloud server domain access**

  The device hosting the SD-AVC network service requires access to the following Cisco SD-AVC cloud server domains:

  api.cisco.com
  cloudsso.cisco.com
  prod.sdavc-cloud-api.com

  Ensure that:

  - The host device's access to these domains is not blocked by a firewall.

  - If the host device operates in a network that connects to the internet by proxy, and if the proxy performs SSL inspection, configure the proxy to bypass these domains.

Procedure

1. In the SD-AVC Dashboard, open the **Cloud Connector** page.

2. On the **Cloud Connector** page, click **Settings**. A pop-up displays connection information.

3. In the pop-up, click the **Cisco API Console** link. The Cisco API Console page opens in a browser.

4. On the Cisco API Console page, sign in using your Cisco credentials.

5. On the Cisco API Console page, open the **My Applications** tab. A page opens for registering a new application.

Note (The steps on the Cisco API Console page are subject to change.)

6. Register SD-AVC.

   a. Name of your application:

      Use any descriptive name. Save this name for a later step.

      b. Select the **Client Credentials** checkbox.

      c. Select the **Hello API** checkbox.

      d. In the Terms of Service section, select the checkbox to agree with the terms.

      e. Click **Register**. The Cisco API Console page displays the Client ID and Client Secret details. Keep this page open to complete the procedure.

7. In the SD-AVC Dashboard, complete the activation process in the open pop-up.

      a. Enter the Client ID and Client Secret details from the Cisco API Console page.

Note These credentials expire after 90 days.

      b. For Organization Name, use the descriptive name that you entered on the Cisco API Console page in the "Name of your application" field.

      c. (Optional) Click Change Data Store Location, and select a region. This determines where your telemetry data is stored. For organizations located in Europe, it is recommended to change the location to Europe, in accordance with EU General Data Protection Regulation (GDPR) regulations.

      d. Wait for the Cisco Console API to propagate your credential information in the system. This may take a few minutes.

      e. Click **Authenticate**. The pop-up closes.

When this process is complete, the **Cloud Connector** page shows the external sources enabled: Cloud Updates and MS Office 365 Web Service. When enabled, the box for an external source shows a **View Details** button. For either of these sources, click View Details to show details of the network traffic classification affected.

Note After enabling Cloud Connector, there may be a delay of several minutes before any details are displayed by the **View Details** button.

On the **Application Visibility** page, the **Cloud Connector** pane shows a green indicator when Cloud Connector is enabled.

DNS Server Connectivity

Cloud Connector requires connectivity between the device hosting the SD-AVC network service, and one or more DNS servers. By default, SD-AVC has two Cisco OpenDNS DNS servers configured (208.67.222.222 and 208.67.220.220).

Optionally, you can add additional DNS servers or proxy DNS servers, as described below.

Adding DNS Servers

If you need to add additional DNS servers, configure them on the platform hosting the SD-AVC network service, using the **ip name-server** command, before installing the network service.

Example (adds two DNS servers):

```
(config)#ip name-server 198.51.100.1 198.51.100.2
```

Adding a Proxy DNS Server

If you need to configure a proxy DNS server, configure it on the platform hosting the SD-AVC network service before installing the network service, as follows:

1. Before configuring a proxy DNS server, remove any standard name servers.

    no ip name-server

2. Configure the host to act as a DNS server.

    ip dns server

3. Configure the external DNS server address.

    ip dns spoofing *address*

In the following example, 198.51.100.3 is the external DNS server.

```
(config)#no ip name-server
(config)#ip dns server
(config)#ip dns spoofing 198.51.100.3
```

Viewing DNS or Proxy Servers

To view the configured DNS or proxy servers:

In the **SD-AVC Dashboard** > **Application Visibility** page > **Cloud Connector** pane, click **Cloud Connector**.

A window opens, displaying a list of the default DNS servers, and any manually configured DNS and proxy servers.

Manually configured DNS servers have higher priority than the default servers. The priority of manually configured DNS servers is the order in which they were added—the first server added has the highest priority. If the highest-priority DNS server on the list is not available, SD-AVC uses the next in the list.

Serviceability Page

The Serviceability page provides system information, debugging tools, and detailed information about the application rules used to classify network traffic.

Tool	Description
System	System information, such as disk, memory, and CPU status, and system logs.
	System Logs **Serviceability** > **System** > **General Information** SD-AVC keeps a system log as a local file. The log is available for download here. Beginning with this release, SD-AVC can also send error messages to an external system log server in real time.
	Unclassified Traffic Visibility control **Serviceability** > **System** > **Settings** Enables/disables the unclassified traffic analysis feature (see Unclassified Traffic Analysis and Discovery, on page 4). When enabled, top hosts and sockets will be identified on the Application Visibility page, in the table and in the graph of traffic bandwidth. After enabling Unclassified Traffic Visibility, the effect is not immediate. SD-AVC gathers information about top hosts and sockets in network traffic (communicated from network devices to the SD-AVC network service by Netflow) and identifies them gradually. Similarly, after disabling the feature, the top hosts and sockets that have been identified may remain in the table and graph for a period of time (dependent on the time range displayed) while SD-AVC continues to analyze traffic and update the Application Visibility page. Default: Enabled

Tool	Description
	SSL Certificate **Serviceability** > **System** > **Settings** By default, the browser-based SD-AVC Dashboard provides a self-signed SSL certificate that appears in a browser as untrusted. Optionally, you can register your specific domain and acquire a signed SSL certificate **specifically for use with SD-AVC**, and import the certificate into SD-AVC. Connecting to the SD-AVC Dashboard is then secure and trusted. **Note** Ensure that the installed SSL certificate is valid. SD-AVC does not automatically remove an SSL certificate when it expires, so replace the certificate before it expires. An invalid certificate may prevent connection to the SD-AVC Dashboard. If you encounter difficulty connecting to the SD-AVC Dashboard because of an untrusted or expired certificate, connect using the IP address of the network service. You can ping the hostname to get the IP address of the network service. 1. Create a certificate for the SD-AVC domain (self-signed or signed by a certification authority), and save the certificate file to a local directory. 2. Click **Change** and upload the certificate file. • **Certificate**: Select **PKCS** or **JKS** for the certificate format. • **Keystore Passphrase**: Keystore passphrase for the certificate. • **Key Alias**: The key alias (called friendlyName when using OpenSSL) is set when creating the certificate. It may be a default value or a specified custom name. • **Key Password**: Enable this option if the alias is configured with a key passphrase, and enter the passphrase. 3. Click **Upload & Activate**. It may require a few minutes to activate the certificate before you can reconnect to the SD-AVC Dashboard. 4. Log into the SD-AVC Dashboard using the hostname associated with the SSL certificate. **Syslog Server** **Serviceability** > **System** > **Settings** SD-AVC can send error messages to an external system log server in real time. To configure a server, enter the server address and click **Update**.
Vertical Debug	Create rules to track specific traffic criteria, for debugging.
SD-AVC Message Capture	Collect and download SD-AVC messages (between the SD-AVC network service and one or more agents).

Tool	Description
Application Rules	Detailed information about the application rules used to classify network traffic. Application Rules Page, on page 14

Application Rules Page

The SD-AVC network service collects traffic classification data from network devices. The network service merges the data and sends it to devices as an application rules pack (see Operation). This page shows the merged application rules data.

Segment: Select the network segment using the dropdown menu at the top right.

Field	Description
IP	Server IP
Port	Port
VRF	VRF name, if applicable
Application Name	Application name, defined by: • Protocol Pack protocol • User-defined protocols
Entry Type	Network cache type: • **L3** • **socket-cache**
Source	Protocol/application: • **network**: Identification of flow by Protocol Pack • **dynamic**: Identification of flow by user-defined application • **ac_hosts** or **ac_sockets**: Tracking of flow by Unclassified Traffic Discovery feature
Rating	Number of significant flow (session) hits in the network layer
Transport	Transport protocol
TTL	Time to Live: Timespan (in cycles) for tracking the socket • If there is active traffic for the socket, the TTL remains at maximum value of 384. • If there is no active traffic for the socket, the TTL value is decremented over time.

SD-AVC System Time and Displayed Times

SD-AVC receives the UTC time from the host platform. UTC times appear in activity logs.

The SD-AVC Dashboard displays times according to the local time zone of the PC that is accessing the Dashboard. Times appear at the bottom left of the Dashboard, in timelines of network activity, and so on.

Note If the host platform clock is set incorrectly, the times shown in logs and in the Dashboard will be incorrect.

Setting the System Time on the Host Platform

To set the system time, use:

clock set *hh:mm:ss day month year*

Example:

```
#clock set 12:13:00 27 Mar 2018
```

Setting the Time Zone on the Host Platform

Note SD-AVC receives the time from the host platform as UTC.

To set the time zone (hour offset from UTC), use the following in config mode. The timezone-name is arbitrary.

clock timezone *timezone-name offset-from-UTC*

Example:

```
(config)#clock timezone NYC -5
```

Showing the time includes the configured offset (-5 hours for New York (NYC) in the example).

Example:

```
#show clock
15:47:59.481 NYC Thu Mar 22 2018
```

To remove the time zone setting and use UTC time:

```
(config)#no clock timezone
```