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 7
View details of external sources of application classification	Connectors Page, on page 9
Configure custom applications	Custom Applications in SD-AVC, on page 16
View system information, application rules, and debugging tools	Serviceability Page, on page 17 Application Rules Page, on page 20

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 or selected segment	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.
More Actions (…) button	After selecting a specific network segment, you can use **More Actions** > **Clear State** to clear the traffic classification data collected by the SD-AVC network service for that segment. This resets the application rules pack that the SD-AVC network service sends to devices in that network segment, and resets the application rules data stored on devices in the segment. The clear state process may take several minutes on the SD-AVC network service and on devices in the network segment. During this time, if a device sends packets to the SD-AVC network service, the packets are rejected. **Note** This feature requires that the devices in the network use Cisco IOS XE Amsterdam 17.3.x or later.

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.

Information/Control	Description
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.
Timeline	Graph of one of the following (select in dropdown menu): • Bandwidth • Classification score • First packet classification score • SD-AVC coverage ratio • Unclassified Traffic • Domain Hits See Domain Information, on page 6.

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.

Information/Control	Description
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	Usag
HTTP	0.00
WebEx Meeting	6.84
Unknown	6.35

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**

Notes and Limitations

See SD-AVC Notes and Limitations.

Domain Information

Minimum releases: Cisco IOS XE Release 17.9.1 for devices, SD-AVC 4.4.0

Devices operating with SD-AVC collect a list of the domains associated with each flow that the device handles, and a count of the number of flows associated with each domain. SD-AVC aggregates this information from all devices in the network and displays it in the SD-AVC Dashboard.

This information is useful for visibility into the top domains used in the network.

Display Domain Information

1. In the SD-AVC Dashboard, click **Application Visibility**.

2. In the timeline, click the drop-down list and choose **Domain Hits** to view the top five domains.

3. Click **Application Insights** to display a timeline and other options.

4. Click the drop-down list in the timeline and choose **Domain Hits**.

   A table shows the following information:

Field	Description
Domain	Domains and subdomains used for flows in the network. The domain information is collected by devices in the network and aggregated by SD-AVC.
Hits	Number of flows handled by devices in the network, for each domain or subdomain, within the time interval configured in the SD-AVC Dashboard. SD-AVC displays the top 100 domains, as determined by the number of flows (hits).
Last Application Name	If NBAR is able to classify the domain, this field displays an application name that corresponds to the domain.

5. You can click one or more domains in the list to display a graph of their contributions to the total number flows, over time.

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.

Connectors Page

This page displays details of the **Cloud Connector**, which manages multiple sources of application information used for classifying network traffic. The page displays any errors or warnings for the Cloud Connector, if applicable.

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

Cloud Connector

From the SD-AVC menu, choose **Cloud Connector**.

SD-AVC connects to a cloud service provided by Cisco that provides information that improves traffic classification, often enabling classification of traffic from the first packet of a flow. 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.

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

Source	Description
Cloud Updates	Provides application data from multiple external sources.

Source	Description
MS Office 365 Web Service	Provides domain names and related information used by Microsoft Office 365. • **View Details**: Use this to display details about each domain, including the service instance of the domain. For information about how Microsoft Office 365 defines service instances, see the Office 365 documentation. See Office 365 Traffic Categories, on page 10. • **Select Service Instance**: Use this to limit the Microsoft Office 365 server domains that the SD-AVC network service sends to devices in the network, to include only specific geographical regions. See Limit the Microsoft Office 365 Server Domains Sent to Devices in the Network, on page 13. **Note** To configure whether this service is enabled by default, use the **Serviceability** > **System** > **Settings** > **MS Office365 Service** option.

Telemetry Data Collection

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

The Cloud Connector setup enables you to specify the location for storing telemetry data for each network segment. This provides the flexibility to store telemetry data for different segments in different locations, and assists in compliance with EU General Data Protection Regulation (GDPR) regulations.

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.

Office 365 Traffic Categories

Cloud Connector receives information from Microsoft about domains and L3/L4 combinations (IP ranges, port, and L4 protocol) used for Office 365 traffic. Microsoft indicates the traffic category (Optimize, Allow, or Default) for each domain and L3/L4 combination. (See Microsoft 365 Network Connectivity Principles.) Cisco SD-AVC identifies traffic from each of the domains and L3/L4 combinations as Office 365 traffic, and assigns it the traffic category provided by Microsoft

You can use the Office 365 traffic category when creating traffic policy, enabling you to apply policy decisions based on Office 365 traffic categorization. Recognizing Office 365 traffic by the L3/L4 combination offers the special advantage of first-packet classification, allowing traffic policy to be applied from the first packet of a flow.

Device requirement: To use Office 365 categories, devices must be using Cisco IOS XE Amsterdam 17.3.1 or later.

Policy example using Office 365 traffic categories: The following policy, configured on a device in the network, uses Office 365 traffic categories **optimize** and **allow**.

```
class-map match-any optimize
match traffic-category optimize
class-map match-all allow
match traffic-category allow
!
policy-map type epbr epbr-policy-return
parameter default flow-stickness
class optimize
   set ipv4 vrf traffic next-hop 10.0.0.254
class allow
   set ipv4 vrf traffic next-hop 10.0.0.254


interface GigabitEthernet0/0/1
service-policy type epbr input epbr-policy
```

Enable 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 a proxy server is required, configure the server from the SD-AVC Dashboard, using **Serviceability** > **Proxy Settings**.

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.

Note Procedure details in the Cisco API Console are subject to change.

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

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

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

6. Register SD-AVC.

   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.

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.

Enable or Disable Sending Microsoft 365 Server Information to Devices in the Network

1. In the SD-AVC dashboard, click **Serviceability**.

2. Click **System**.

3. Click **Settings**.

4. Enable or disable the **MS Office365 Service** option.

Limit the Microsoft Office 365 Server Domains Sent to Devices in the Network

The NBAR component of Cisco IOS XE routing software uses Protocol Pack information to identify Microsoft Office 365 traffic. This enables you to create application-aware traffic policies that match Microsoft Office 365 traffic and route the traffic as needed. For further information about this, see Configure Enhanced PBR to Allow and Optimize Office365 Traffic, in Enhanced Policy-Based Routing and Site Manager.

When you are using SD-AVC, and you enable the Microsoft Office 365 Web Service, the SD-AVC network service adds a layer of information about Microsoft Office 365 traffic, enabling NBAR to provide a more detailed classification of the traffic, as follows:

Table 6: NBAR Classification of Microsoft Office 365 Traffic

NBAR, using information from the Protocol Pack	NBAR, using information from SD-AVC
Classifies all Microsoft Office 365 traffic	• Using SD-AVC, NBAR classifies and categorizes Microsoft Office 365 traffic according to Microsoft-defined categories: Optimize, Allow, and Default. NBAR provides this categorization on the first packet of a flow. According to the Microsoft model, Optimize refers to traffic requiring the highest network performance. This categorization is useful for creating traffic policies for specific types of Microsoft Office 365 traffic (Optimize, Allow, or Default). • Provides detailed server information (domain names and IP addresses) for Microsoft Office 365 servers worldwide, together with the service instance information for each server. Examples of service instances are China, Germany, USGovGCCHigh, and USGovDoD. The additional categorization of the traffic into Optimize, Allow, or Default, typically applies to all Microsoft Office 365 traffic. But you can configure SD-AVC to limit the Microsoft Office 365 server information that it provisions to devices in the network, to include only a subset of service instances. This can be helpful when configuring the network to meet certain compliance requirements.

Use this procedure to limit the Microsoft Office 365 server information sent to devices in the network, to include only servers within specific service instances. For information about how Microsoft Office 365 defines service instances, see the Office 365 documentation.

Use Case

A use case for limiting the Microsoft Office 365 servers sent to devices is to enable you to create a traffic policy that affects only Microsoft Office 365 traffic meeting both of the following conditions:

- The traffic is categorized by Microsoft as Optimize.

- The traffic connects to a Microsoft server within a specific subset of service instances.

For example, an organization might need to configure a traffic policy that applies only to Microsoft Office 365 traffic that is categorized as Optimize, and that uses USGovGCCHigh and USGovDoD-compliant service instances. The organization might configure this traffic policy to bypass a firewall used for other traffic, in order to provide better performance for this select Optimize-type traffic. For their network that employs SD-AVC, the organization can do the following:

- Use the procedure described below to limit the Microsoft Office 365 servers to USGovGCCHigh and USGovDoD service instances.

- Define a traffic policy for the network that matches the Optimize category for Microsoft Office 365 traffic. The action for this policy might be to direct only this traffic to a specific proxy server that bypasses a firewall, to provide better performance. The traffic policy does not match any other network traffic, including Microsoft Office 365 traffic categorized as Allow or Default. It also does not match any Microsoft Office 365 traffic that connects to Microsoft servers outside of the USGovGCCHigh and USGovDoD service instances.

Prerequisites

Use this procedure before enabling the cloud connector. See Enable the Cloud Connector, on page 11.

Procedure

1. Verify that the cloud connector has not yet been enabled.

   See Enable the Cloud Connector, on page 11.

   Note If you enable the cloud connector before configuring the specific geographic regions you want to include, the SD-AVC network service may already have sent the full domain list to devices in the network.

2. Disable the Microsoft Office365 Service option.

   See Enable or Disable Sending Microsoft 365 Server Information to Devices in the Network, on page 13.

3. In the SD-AVC dashboard, click **Cloud Connector**.

   The **MS Office 365 Web Service** is disabled, indicating that the SD-AVC network service is not connected to the MS Office 365 Web Service.

4. In the **MS Office 365 Web Service** pane, click **Select Service Instance**.

5. Select service instance regions to include Microsoft Office 365 server domains in those regions, and click **Apply**.

6. To enable the service, click the toggle in the **MS Office 365 Web Service** pane.

The SD-AVC network service sends a list of Microsoft Office 365 server domains, filtered according to your selections, to the devices in the network.

✎

Note Within several minutes, the updated list of server domains replaces any list previously sent to the devices.

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, 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
```

Viewing DNS Servers

To view the configured DNS servers, open the **SD-AVC Dashboard** > **Serviceability** page > **System** pane.

Configuring a Proxy Server

Some organizations require use of a proxy server. Use the **Proxy Settings** page to view or configure a proxy server.

1. On the **SD-AVC Dashboard** > **Serviceability** page, click **Proxy Settings**. The current proxy server configuration is shown.

2. To configure or update proxy server settings, enter the following:

    • Protocol: HTTP or HTTPS

    • Server IP: IP address or domain name

    • Server Port: Port number

3. If credentials are required, click **Advanced Options** and enter the credentials.

4. Click **Save**.

Customization Page

Custom Applications in SD-AVC

Network devices operating with SD-AVC use Cisco NBAR2 and other tools to identify network traffic. The composite of information that NBAR2 uses to identify a network applications is called an "application" (or a "protocol" in the Protocol Packs released periodically by Cisco). Custom applications, also called user-defined applications, may be specified network-wide using SD-AVC.

Each application includes a signature of details that identify the network application, such as:

- Server names

- IP addresses

- Ports

- L3 or L4 protocol

You can configure custom applications using the SD-AVC Dashboard or using the SD-AVC REST API. See User-defined Applications.

Creating a Custom Application

The following procedure describes the typical workflow for creating a custom application in SD-AVC. It is also possible to create a custom application by these methods:

- In the SD-AVC Dashboard, on the **Application Visibility** page, select **Unclassified Traffic**, select one or more rows, and click the **Customize** button. This opens the **Custom Applications** page, with the IP address of the selected unclassificed traffic entered automatically.

- Configure custom applications using the SD-AVC REST API. See User-defined Applications.

Note If you create custom applications using the SD-AVC Dashboard, do not create a new set of custom applications through the REST API using POST. Doing so overwrites the custom applications created through the SD-AVC Dashboard. You can add custom applications through the REST API using PUT.

1. In the SD-AVC Dashboard, on the **Customization** page, click **Applications**.

2. In the **Custom Application Rules** page, click **New Rule**.

3. In the drop-down list of network segments, select a segment.

4. In the **Application Name** field, enter the name of the source.

5. Click **New Application** and enter information as follows.

Field	Description
Server Names	Enter one or more server names.

Field	Description
L3/L4	Select this and enter: • One or more IP addresses. • Ports or port range. • L3 or L4 protocol: TCP, UDP, or TCP-UDP
Attributes	(optional) Specify attributes for the application: • Category • Subcategory • Application Group • Business Relevance • Traffic Class • Application Set

6. Click **Save & Deploy**. The new application appears in the list of applications.

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	**Serviceability** > **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: Enable/Disable **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
	Behavioral Based Classification: Enable/Disable **Serviceability** > **System** > **Settings** Cisco NBAR uses a method called behavioral classification to assist in classifying traffic. This method relies on heuristic techniques to determine the purpose of servers or clients. This method might produce undesired results in some cases – for example, when the SD-AVC network service communicates with networks through a proxy device. For these situations, disable behavioral based classification in SD-AVC. **Note** — Using the Disable option requires that the devices in the network use Cisco IOS XE Amsterdam 17.3.x or later.

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	**Serviceability** > **Vertical Debug** Create rules to track specific traffic criteria, for debugging.

Tool	Description
SD-AVC Message Capture	**Serviceability** > **SD-AVC Message Capture** Collect and download SD-AVC messages (between the SD-AVC network service and one or more agents).
Application Rules	**Serviceability** > **Application Rules** Detailed information about the application rules used to classify network traffic. Application Rules Page, on page 20
Proxy Settings	View or configure proxy server settings. Configuring a Proxy Server, on page 15

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

Field	Description
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
```