



Custom Applications



Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Table 1: Feature History

Feature Name	Release Information	Description
Support for Defining Custom Applications	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature adds support for defining custom applications.

- [Information About Custom Applications](#) , on page 1
- [Configure Custom Applications Using Cisco SD-WAN Manager](#), on page 4
- [Verify Custom Applications](#), on page 5

Information About Custom Applications

Cisco Network-Based Application Recognition (NBAR) is a Cisco technology that performs the SD-WAN Application Intelligence Engine (SAIE) flow on network traffic to identify network applications according to their traffic characteristics.



Note In Cisco vManage Release 20.7.1 and earlier releases, the SAIE flow is called the deep packet inspection (DPI) flow.

The specific traffic characteristics of a network application are called an application signatures. Cisco packages the signature for an application, together with other information, as a protocol. Cisco packages a large set of protocols, covering numerous commonly occurring network applications, as a Protocol Pack. Cisco updates and distributes Protocol Packs regularly. They provide a database of network application signatures for NBAR to use to identify network application traffic.

The term network applications is defined broadly, and may include all of the following, and more:

- Social media websites
- Voice over IP (VoIP) applications
- Streaming audio and video, such as Cisco Webex
- Cloud applications, such as for cloud storage
- SaaS applications
- Custom network applications specific to an organization

Identifying applications is useful for monitoring network traffic, configuring application-aware traffic policy, and more.

To summarize network application signatures, protocols, and Protocol Packs, and how NBAR uses them:

- The traffic of a network application has unique characteristics that can be used to identify the traffic as belonging to that specific application. These characteristics are called application signatures.
- Cisco packages the signature for a specific network application as a protocol.
- Cisco packages a large set of protocols, covering commonly occurring internet applications, as Protocol Packs.
- Cisco NBAR performs the SAIE flow on traffic to gather the information required to identify the sources of the traffic, and uses protocols, such as those provided in Protocol Packs, to match that information to specific network applications. The result is that NBAR identifies the network applications producing traffic in the network.

Cisco Software-Defined Application Visibility and Control (SD-AVC) uses Cisco NBAR application identification to provide information about application usage within a network.

Custom Applications

In addition to the standard protocols provided in a Protocol Pack, you can define protocols, called custom applications, to identify internet traffic, often for uncommon network applications that are of specific interest to their organization. Custom applications augment the protocols provided in a Protocol Pack.

You can use custom applications in the same way as any other protocol when configuring:

- Cisco Catalyst SD-WAN policies
- Application Quality of Experience (AppQoE) policies, such as application-aware routing, TCP acceleration, and Quality of Service (QoS)



Note The following terms are used in the documentation of related technologies, and are equivalent: custom applications, custom protocols, user-defined applications

Custom Applications in Cisco Catalyst SD-WAN

Cisco Software-Defined AVC (SD-AVC) is a component of Cisco Application Visibility and Control (AVC). It functions as a centralized network service, operating with specific participating devices in a network. One function of Cisco SD-AVC, which is included as a component of Cisco Catalyst SD-WAN, is to create and manage custom applications. Cisco Catalyst SD-WAN uses this Cisco SD-AVC functionality, through SD-AVC REST APIs, to enable you to define custom applications within Cisco Catalyst SD-WAN.

As a Cisco Catalyst SD-WAN user, you can use Cisco SD-WAN Manager to define custom applications. Cisco SD-AVC then pushes the custom applications to devices in the network. The devices in the network use the custom applications and other application protocols to analyze traffic traversing the devices.

The process of defining a custom protocol includes choosing criteria to identify network traffic as coming from a specific network application. The criteria can include characteristics of hosts originating the traffic, such as server names, IP addresses, and so on.

Priority of Protocols and Custom Applications

It is possible to define custom applications that match some of the same traffic as a protocol included in the Protocol Pack operating with Cisco NBAR. When matching traffic, custom applications have priority over Protocol Pack protocols. Deploying SD-AVC within an existing network does not require any changes to the network topology.

Restrictions for Custom Applications

- Maximum number of custom applications: 1100
- Maximum number of L3/L4 rules: 20000
- Maximum number of server names: 50000
- For server names, maximum instances of wildcard followed by a period (.): 50000
Example: *.cisco.com matches www.cisco.com, developer.cisco.com
- For server names, maximum instances of prefix wildcard as part of server name: 256
Example: *ample.com matches www.example.com
- Mapping the same domain to two different custom applications is not supported.
- DNS traffic and application traffic need to be in the same VRF for SD-AVC to perform first packet classification.
- Creating custom applications through CLI is not supported in Cisco Catalyst SD-WAN policy.
- Activation of custom applications:
 - When using Cisco vManage Release 20.5.1 releases and earlier: For devices using releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, the activation of custom applications is as follows:
 - A custom application created in Cisco SD-WAN Manager is not activated for visibility functionality (monitoring traffic) or control functionality (traffic policy) until a policy that makes use of the custom application is applied.

- When using Cisco vManage Release 20.5.1 or later: For devices using Cisco IOS XE Catalyst SD-WAN Release 17.5.1a or later, the activation of custom applications is as follows:
 - A custom application created in Cisco SD-WAN Manager is activated immediately for application visibility functionality only (monitoring traffic), such as for protocol-discovery counters and Flexible NetFlow (FNF). When activated for visibility functionality only, custom applications do not affect traffic policy.
 - When the custom application is used by a policy, it becomes activated for control functionality (traffic policy) also.

Configure Custom Applications Using Cisco SD-WAN Manager

Prerequisites

Install Cisco SD-AVC as a component of Cisco Catalyst SD-WAN. For information on how to enable SD-AVC on Cisco SD-WAN Manager, see [Information on how to enable SD-AVC for Cisco SD-WAN devices](#).

Perform the following steps to configure custom applications:

1. In Cisco SD-WAN Manager, select **Configuration > Policies**.
2. Select **Centralized Policy**.
3. Click **Custom Options** and select **Centralized Policy > Lists**.
4. Click **Custom Applications**, and then click **New Custom Application**.
5. To define the application, provide an application name and enter match criteria. The match criteria can include one or more of the attributes provided: server names, IP addresses, and so on. You do not need to enter match criteria for all fields.

The match logic follows these rules:

- Between all L3/L4 attributes, there is a logical AND. Traffic must match all conditions.
- Between L3/L4 and Server Names, there is a logical OR. Traffic must match either the server name or the L3/L4 attributes.

Field	Description
Application Name	(mandatory) Enter a name for the custom application. Maximum length: 32 characters
Server Names	One or more server names, separated by commas. You can include an asterisk wildcard match character (*) only at the beginning of the server name. Examples: *cisco.com, *.cisco.com (match www.cisco.com, developer.cisco.com, ...)

Field	Description
L3/L4 Attributes	
IP Address	Enter one or more IPv4 addresses, separated by commas. Example: 10.0.1.1, 10.0.1.2 Note The subnet prefix range is 24 to 32.
Ports	Enter one or more ports or port ranges, separated by commas. Example: 30, 45-47
L4 Protocol	Select one of the following: TCP, UDP, TCP-UDP

- Click **Add**. The new custom application appears in the table of custom applications.



Note To check the progress of creating the new custom application, click **Tasks** (clipboard icon). A panel opens, showing active and completed processes.

Example Custom Application Criteria

Criteria	How to configure fields
Domain name	Server Names: cisco.com
Set of IP addresses, set of ports, and L4 protocol	IP Address: 10.0.1.1, 10.0.1.2 Ports: 20, 25-37 L4 Protocol: TCP-UDP
Set of ports and L4 protocol	Ports: 30, 45-47 L4 Protocol: TCP

Verify Custom Applications

Verify Custom Applications in Cisco SD-WAN Manager

After you define a custom application, it appears in the **Custom Application List**, which shows all available protocols and custom applications. The **Custom Application List** is available here:

Configuration > Policies > Centralized Policy > Add Policy > Custom Applications.

Verify Protocols and Custom Applications on a Device

Use the **show ip nbar protocol-id** command to display all protocols and custom applications that are loaded on the router. It is helpful to filter the results. For example, to display all protocols and custom applications with "custom" in the name, use this:

```
vm5#show ip nbar protocol-id | include custom
custom_amazon          3899          PPDK LOCAL
custom_facebook        3284          PPDK LOCAL
```

See [show ip nbar protocol-id](#).