Cisco Catalyst SD-WAN Application Management Guide, Releases 26.x and Later

Cisco SD-WAN
Updated June 8, 2026

© 2023-2025 Cisco Systems, Inc. All rights reserved.

Full Cisco Trademarks with Software License

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Topics included

Full Cisco Trademarks with Software License....ii

1 Application Catalog....6

Feature history for application catalog....7
Application catalog....7
Cloud-sourced applications....8
Applications in registry....9
Top applications observed in network....10
Benefits of Kubernetes clusters and Kubernetes services....10
Benefits of cloud SaaS feeds....10
Prerequisites for application catalog....10
Restrictions for application catalog....11
View applications....11
Configure custom applications....12
Export application list....14
Add cloud-sourced applications to the application catalog....14
Configure an application list....15
Enable Kubernetes clusters for cloud-based deployment....16
Enable manual discovery of Kubernetes clusters....16
Configure a Cloud SaaS feed in Cisco SD-WAN Manager....17
Monitor kubernetes clusters and services....18
Monitor cloud SaaS feeds....18

2 Application and Policy Compliance....20

Feature history for application and policy compliance....21
Policy compliance....21
Application compliance....22
Restrictions for the policy compliance check....23
View and resolve policy compliance issues....23
View and resolve application name conflicts....24
View application details....24

3 Protocol Pack management and compliance....26

Protocol Pack management and compliance....27
Protocol pack management and compliance....27
How protocol pack upgrades work when devices become compatible....27
Restrictions for protocol pack management and compliance....28
Upload a Protocol Pack to Cisco SD-WAN Manager....28

Upgrade a device protocol pack....29
Verify protocol pack compliance....30
View protocol pack status....30
Delete protocol packs....31

1 Application Catalog

Topics:

- Feature history for application catalog
- Application catalog
- Prerequisites for application catalog
- Restrictions for application catalog
- View applications
- Configure custom applications
- Export application list
- Add cloud-sourced applications to the application catalog
- Configure an application list
- Enable Kubernetes clusters for cloud-based deployment
- Enable manual discovery of Kubernetes clusters
- Configure a Cloud SaaS feed in Cisco SD-WAN Manager
- Monitor kubernetes clusters and services
- Monitor cloud SaaS feeds

Introduces the Application Catalog, outlining its purpose and key features for managing and accessing available applications.

Feature history for application catalog

Provides an overview of the Application Catalog feature and related capabilities, including Kubernetes cluster discovery and monitoring, cloud SaaS feeds, and cloud-sourced applications, with release information and descriptions for each capability.

Table 1: Feature history

Feature Name	Release Information	Description
Application Catalog	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	The **Application Catalog** feature provides control and visibility for applications running in your network environment. The application catalog is continuously updated as new applications are developed to ensure that your Cisco SD-WAN Manager environment adapts to changes in application use.
Discover and Monitor Kubernetes Clusters	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	The Cisco SD-WAN Manager integrates Kubernetes cluster discovery and monitoring to monitor your network infrastructure and your containerized applications from a single interface. The Kubernetes cluster management streamlines the network and applications while providing a visibility and control on the applications.
Cloud SaaS Feeds	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	Cloud SaaS (Software as a Service) feeds are information or data feed from SaaS applications that are hosted on the cloud. These applications can range from customer relationship management (CRM) tools to financial software, and Cisco SD-WAN Manager provides real-time data and updates as feeds from the SaaS applications.
Cloud-Sourced Applications	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	Cloud-sourced applications, derived from the Cisco SD-AVC component, complement applications from other sources, such as Protocol Packs and custom applications. You can use cloud-sourced applications in security and centralized policies, and in Cloud OnRamp for SaaS.

Application catalog

Describes the application catalog in Cisco SD-WAN Manager that provides visibility and control of applications in a Cisco Catalyst SD-WAN environment and uses Cisco SD-AVC for cloud-sourced updates and application coverage.

The application catalog is a feature that

- provides visibility and control of applications in a Cisco Catalyst SD-WAN environment, powered by the Cisco SD-AVC component
- centralizes operational tasks such as updating applications and cloud SaaS feeds, creating custom applications, grouping applications, and creating application lists
- optimizes network connectivity based on the specific requirements of different Kubernetes services.

Application catalog features

The application catalog includes applications ranging from business productivity apps like Office 365 or Google Workspace to social media platforms, cloud platforms, and customer-created applications.

Cisco Catalyst SD-WAN support more than 4000 applications, 2500 Cloud Sourced applications through SD-AVC in addition to the existing 1500 applications supported by NBAR2.

> **Note**
>
> You can use custom applications in the same way as any other protocol when configuring policies using policy groups or using centralized policies. For more information on configuring policies using Policy Groups refer to the Objects and Profiles section in the *Cisco Catalyst SD-WAN Policy Groups Configuration Guide*.

The **Application Catalog** tab includes these features:

- Overview
- Applications
- Application Source Settings
- Discovered Application
- Application List
- Configure SD-AVC
- Configure Cloud Connection
- Cloud Sourced Applications

Cloud-sourced applications

Cloud-sourced applications help you use applications from the dynamically updated Cisco SD-AVC database in Cisco SD-WAN Manager policies and Cloud OnRamp for SaaS.

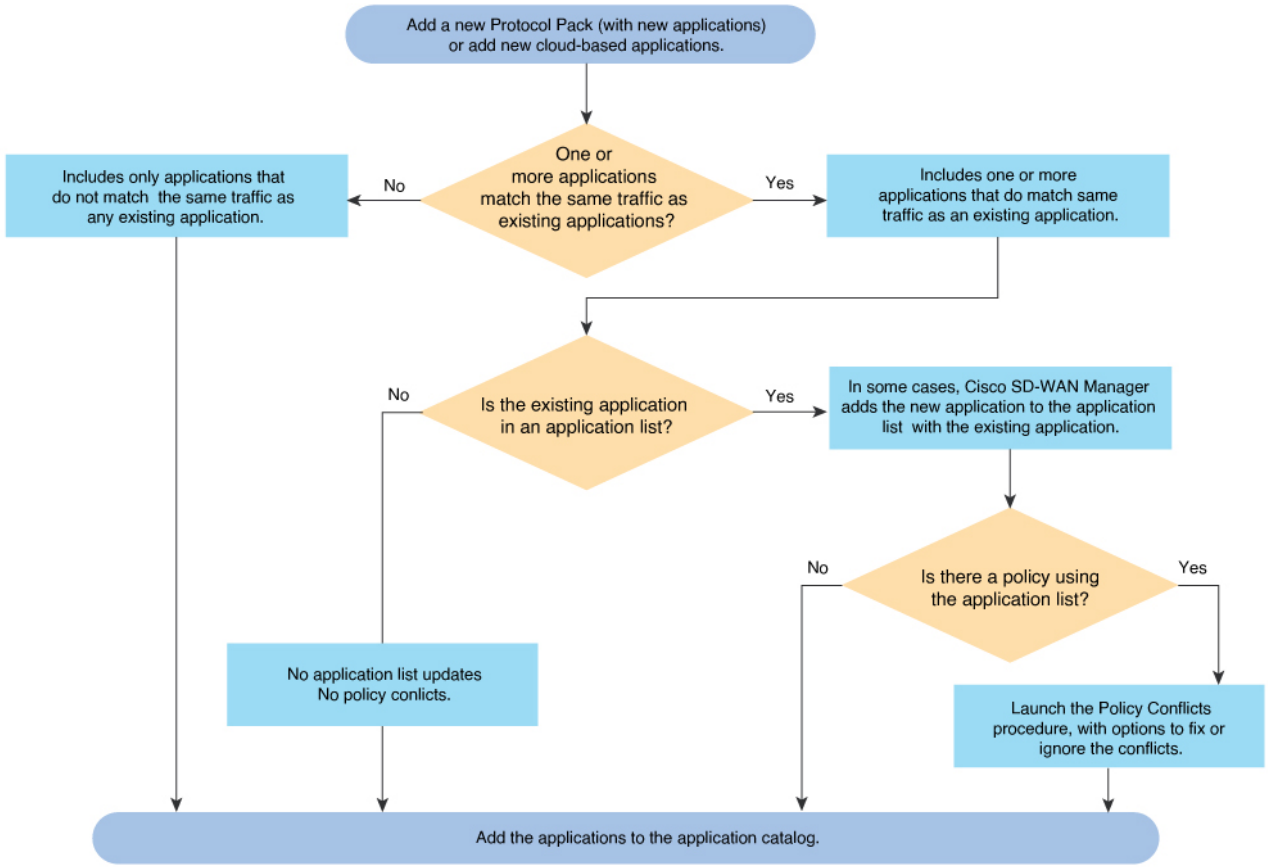
Cloud-sourced applications are applications that

- Cisco Catalyst SD-WAN sources from the Cisco SD-AVC component, and
- can be used in Cisco SD-WAN Manager security policies, centralized policies, and Cloud OnRamp for SaaS.

Cisco SD-AVC uses cloud-based sources to continuously update its network applications database. The dynamic database regularly adds new applications and updates information about existing applications.

A cloud-sourced application may match some of the same traffic as an existing application. In some cases, Cisco SD-WAN Manager prompts you to take action to resolve any conflicts.

Figure 1: Logic to add an application to the catalog



Applications in registry

The applications in registry chart shows the distribution of applications in the Cisco SD-WAN Manager application registry.

The chart includes these application categories:

Category	Description
Built in	Applications that are built-in or pre-installed in the system.
Discovered	Applications that are discovered or detected by the system.
Custom	Custom-built applications specifically developed for the system.

Each chart segment represents an application category. The segment size indicates the relative proportion of applications in that category.

Use this chart to gain insights into the application landscape and understand the composition of applications in the system. This chart illustrates the applications in the Cisco SD-WAN Manager application registry. The device application registry is updated after pushing a configuration to the devices. For example, when a new custom application is created, it is not updated in the device application registry until a policy with that custom application is pushed to the device, however, it will be counted in the custom application on this chart since Cisco SD-WAN Manager already has the definition in its registry. All the custom applications created are seen in the **Applications** tab and in the chart as custom apps.

Top applications observed in network

The **Top applications observed in network** doughnut chart shows the top application categories observed in network traffic.

Each chart segment represents an application category. The segment size indicates the relative presence or frequency of that category in the observed network traffic.

Use this chart to understand which application categories are prominent in the network and how application traffic is distributed.

You can view application details by timestamp, such as **Last 1 Hour** or **Last 3 Hours**. The maximum selectable time period is 24 hours.

Benefits of Kubernetes clusters and Kubernetes services

Provides a concise list of benefits from integrating Kubernetes clusters and services with centralized network operations, including unified management, enhanced visibility, improved application performance, operational efficiency, and stronger security across network and application layers.

- Unified network management: Cisco SD-WAN Manager gives the ability to add Kubernetes clusters and it discovers any applications running on them.
- Enhanced visibility: The Cisco SD-WAN Manager and Kubernetes clusters integration provides complete visibility over both network infrastructure and application definitions, making it easier to identify and resolve issues.
- Improved performance: Cisco Catalyst SD-WAN's ability to optimize network traffic, combined with direct visibility over Kubernetes resources, results in improved application performance.
- Greater efficiency: The network management based on application requirements and Kubernetes services leads to greater operational efficiency.
- Advanced security: The Cisco SD-WAN Manager and Kubernetes clusters integration provides more robust security for both network and application layers.

Benefits of cloud SaaS feeds

Provides an overview of how cloud SaaS feeds enhance application classification and performance by supplying real-time updates that support intelligent routing and optimization decisions across cloud applications.

- Cloud SaaS feeds provide real-time data on cloud application classification. Cisco SD-WAN Manager uses this information to make intelligent decisions about routing and optimizing traffic to ensure the best possible performance for these applications.
- The Application classification is enhanced and up-to-date with latest Cloud SaaS feeds.

Prerequisites for application catalog

Outlines the prerequisites to use the application catalog, including enabling SD-AVC and optionally the SD-AVC Cloud Connector. Consider release differences where services are enabled by default on cloud-hosted fabrics.

- Enable SD-AVC from **Administration**>**Settings** for application catalog functionality.
- Enable SD-AVC Cloud Connector **Administration**>**Settings** to use SaaS feeds for enhanced application classification (Optional, but recommended).

Restrictions for application catalog

Outlines restrictions that affect the Application Catalog, including NBAR inspection and applicability, constraints for cloud-sourced applications with Cloud Connector, and Kubernetes integration limits such as supported providers and capacity for custom applications, rules, and server names.

Restrictions for NBAR application classification

NBAR classification in the Application Catalog is limited to early packets and applies only to routed traffic.

Restrictions for cloud-sourced applications

When you add a cloud-sourced application to the application catalog with Cloud Connector enabled, Cisco SD-WAN Manager restricts you from disabling Cloud Connector.

Restrictions for kubernetes clusters and kubernetes services

Kubernetes integration for the Application Catalog supports a limited set of cloud providers and enforces capacity limits.

- Only Google Cloud and Amazon Web Services are supported as cloud providers.

  Note

  AWS GovCloud is not supported.

  Other cloud providers can utilize Kubernetes Clusters and Kubernetes Services feature using the manual upload option.

- Maximum number of custom applications: 1100
- Maximum number of L3/L4 rules: 20000
- Maximum number of server names: 50000

View applications

Provides instructions for viewing all applications associated with your cloud account in vManage, including navigating the Application Catalog and filtering the list using application attributes.

View the applications associated with your cloud account including the applications you create and the default applications on Cisco SD-WAN Manager.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** > **Applications**.

   A list of applications associated with your Cisco SD-WAN Manager appears.

2. Choose an application attribute from the **Select Application Attributes** drop-down box. For example, **Application Source**.

   From the **Choose Filter** drop-down choose a filter to view only the relevant applications.

What to do next

.

Configure custom applications

Configure custom applications in Cisco Catalyst SD-WAN by using the Application Catalog to enter names, server identifiers, families, groups, traffic classes, business relevance, IPs, ports, protocols, and SaaS probe endpoints, then save. Verify you can export the application list to Applications.csv for reuse.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** > **Applications** > **Custom Application**
2. Enter **Application name**, and configure these fields.

Field	Description
Application Name	Enter a name for the application list.
Server Names	Enter the server names. The names specify the fully qualified domain names or regex starting with '*' but not ending with '*', or both separated by commas. For example, *.customapp.com, customapptest.com, *appcustom.
Application Family	Choose the application family. The options include instant messaging, game, mail, routing, and so on.
Application Group	Choose the application group. The options include flash-group, ipsec-group, concur-group, and so on.

Field	Description
Traffic Class	Choose the traffic class. The options include multimedia-conferencing, network-control, real-time-interactive, and so on. **Note** This attribute is used to categorize network traffic into different classes based on specific criteria like source and destination IP addresses, port numbers, etc. Traffic classes are crucial in the traffic matching process because they enable the Cisco Catalyst SD-WAN to identify and sort traffic, which helps in efficiently managing bandwidth and resources. When setting up the policy group workflow, different traffic classes can be allocated different priorities.
Business Relevance	Choose the business relevance from the drop-down list. The options are: · **Bronze** · **Gold** · **Silver** **Note** This attribute is used to specify the priority of network traffic based on its relevance to business operations. For example, traffic related to critical business applications can be assigned a higher relevance, and therefore, a higher priority. This ensures that important traffic gets the resources it needs for optimal performance.
IPv4 Address	Enter the IPv4 addresses separated by commas. Subnet prefix length is 24 to 32.
Ports	Enter the port number or range or both separated by a space. For example, 1 2 10-20.
L4 Protocol	Enter L4 protocol. The options are: · TCP · UDP · TCP-UDP

Field	Description
SaaS probe endpoint type	• Choose **IP Address** and enter IP address. Cloud OnRamp for SaaS probes the server using port 80. • Choose **FQDN** enter a fully qualified domain name of the application server. • Choose **URL** to enter a URL using HTTP or HTTPS. Cloud OnRamp for SaaS probes the server using port 80 or port 443, depending on the URL provided.
SaaS probe endpoint value	Enter an endpoint value, based on the endpoint type that you choose. For example, 192.168.0.1, https://www.example.com, www.google.com

3. Click **Save**.

Export application list

Provides instructions for exporting the application list as a CSV file and explains how to use custom applications with policy groups and centralized policies in Cisco Catalyst SD-WAN.

Procedure

Click **Export** to export the application list.

The **Applications.csv** file is downloaded to the local desktop.

You can use custom applications in the same way as any other protocol when configuring Cisco Catalyst SD-WAN policies using policy groups or using centralized policies. For more information on configuring policies using policy groups, refer to Objects and Profiles section of the *Cisco Catalyst SD-WAN Policy Groups Configuration Guide*.

Add cloud-sourced applications to the application catalog

Configure the application catalog in SD-WAN Manager by selecting cloud-sourced applications and applying them. Address any policy conflicts when prompted, either fixing them or deferring, to ensure the catalog includes the intended cloud-sourced entries.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog**.
2. Click **Cloud-sourced Application**.
3. Choose one or more cloud-sourced applications by selecting the check box next to each application.
4. Click **Apply Application(s)** and choose **Apply Selected Application(s)**.

   A cloud-sourced application may match some of the same traffic as an existing application. If this creates a conflict, Cisco SD-WAN Manager prompts you to take action to resolve any conflicts. For information about the logic, see Information About Cloud-Sourced Applications.

5. If the policy conflict pop-up window opens, choose an option.
   - **Fix Conflicts**: Opens the **Conflicts** tab to enable you to update the policy.
   - **Manage Cloud-Sourced Application Conflicts**: Adds cloud-sourced applications after fixing the policy conflicts.
   - **Ignore and Apply**: Defer resolving conflicts that affect policies and add cloud-sourced applications to the application catalog.

   > **Note**
   >
   > To remove cloud-sourced applications from the application catalog, contact Cisco technical support.

Configure an application list

Configure an application list in the Application Catalog to create or update a list of applications or families. Configure filters to find default or custom lists and prepare entries for use in Policy Group-based policies.

Procedure

1. Create Application List.
   a) From the **Configuration** > **Application Catalog** > **Application List**, click **Create Application List**.
   b) Choose **Create New** to create a new application list, or choose **Existing** to update an existing application list.
   c) Enter the **Application List** or choose an **Application List** from the drop-down list to update an existing application list.
   d) Choose an application or application family from the **Application** or **Application Family** drop-down list.
   e) Click **Save**.

      The application list is created.

2. Find the application or application set.
   a) On the **Application Lists** page, find the existing application or application family by using the **Find Application/ Application Set** field.
   b) Choose the **Default Application List** or **Custom Application List** from the **Show** drop-down list.

      You can filter the application or application family lists.

      The **Summary** pane displays the total, custom, and default application lists.

      The selected application list appears.

   c) Click **Create Application List** to create or edit an existing application list.

> **Note**
>
> Application lists configured in the Application Catalog can only be used in the configuration of policies using Policy Groups.

Enable Kubernetes clusters for cloud-based deployment

Configure Kubernetes cluster discovery in vManage by enabling a cloud account or manually uploading a kubeconfig in Application Catalog. This allows services and applications on your clusters to be discovered and viewed for further application management.

Procedure

1. From the Cisco SD-WAN Manager menu, click **Configuration** > **Application Catalog**.
2. Click the **Application Source Setttings** tab.
3. In the **Kubernetes Cluster** section, click **Cloud Account**.
4. Click **Add Account**.
5. Select a cloud account and click **Enable**.

   The **Kubernetes Cluster** table displays the cloud accounts with the Kubernetes discovery status in the **Status** column.

   > **Note**
   >
   > You'll see a list of cloud accounts appearing already in the **Kubernetes Cluster** cluster table if you've configured the cloud accounts using the Cloud OnRamp for Multicloud feature.

Enable manual discovery of Kubernetes clusters

Details the process for manually enabling Kubernetes cluster discovery by uploading a kubeconfig file, viewing cluster status, accessing discovered services and applications, and creating custom applications as needed.

Procedure

1. In the Cisco SD-WAN Manager menu, click **Configuration** > **Application Catalog**
2. Navigate to the **Application Source Setttings** tab.
3. In the **Kubernetes Cluster** section, click **Manually Upload**.
4. Choose or drag and drop a kubeconfig file and click **Add**.

> **Note**
>
> Maximum file size: 10 MB

The **Kubernetes Cluster** table displays the cloud accounts, with the Kubernetes discovery status in the **Status** column.

What to do next

After you have configured the Kubernetes cluster, navigate to the **Discovered Application** tab to view the services and applications discovered on those Kubernetes clusters and create custom applications if needed.

Configure a Cloud SaaS feed in Cisco SD-WAN Manager

Configure a Cloud SaaS feed in SD-WAN Manager to control how applications are classified using cloud-provided feeds. This procedure navigates to Application Source Settings and enables or disables a feed for the application you select.

Procedure

---

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** > **Application Source Settings**.
2. In the **Cloud SaaS Feeds** table, you see a list of cloud application feeds.

   > **Note**
   >
   > Only if you've enabled SD-AVC and Cloud connections, you'll see the list of cloud SaaS feeds.

3. In the **Actions** column, click the **...** icon adjacent to the respective cloud SaaS feed row.
4. Click **Enable** to view cloud SaaS feeds for the application of your choice.

   > **Note**
   >
   > Choose **Disable** so that the application classification doesn't use the Cloud SaaS feeds and instead uses NBAR classification logic.

Monitor kubernetes clusters and services

Verify Kubernetes cluster and service status in Application Catalog by navigating from vManage to the relevant tabs and reviewing tables. Verify discovery information for clusters and monitoring details for applications to confirm visibility of operational data.

Procedure

1. Monitor Kubernetes clusters.
   a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog**.
   b) Navigate to the **Application Source Settings** tab in the **Application Catalog** page.
   c) The **Kubernetes Cluster** table displays the cluster details along with the Kubernetes cluster discovery status.
2. Monitor applications.
   a) Navigate to the **Discovered application** tab in the **Application Catalog** page.
   b) The **Kubernetes Services** table displays the discovered applications and the details to monitor the application status.

Monitor cloud SaaS feeds

Verify cloud SaaS feed details in Cisco SD-WAN Manager by navigating to Application Source Settings and opening the View Feeds page. This helps you review feed information captured from configured application sources.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** > **Application Source Settings**.
2. In the **Action** column, click **...** icon and choose **View Feeds**.
3. In the **View Feeds** page, you see detailed information regarding the particular cloud SaaS feeds.

2 Application and Policy Compliance

Topics:

- Feature history for application and policy compliance
- Policy compliance
- Application compliance
- Restrictions for the policy compliance check
- View and resolve policy compliance issues
- View and resolve application name conflicts
- View application details

Provides a concise overview of application and policy compliance concepts, describing purpose and scope for administrators who assess conformance and ensure consistent policy enforcement across environments.

Feature history for application and policy compliance

Outlines the introduction and release details of Policy Compliance and Application Compliance features, highlighting how they detect policy changes and protocol conflicts to ensure consistent application and policy operations.

Table 2: Feature History

Feature Name	Release Information	Description
Policy Compliance	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Control Components Release 20.14.1	This feature analyzes application-aware policies to determine whether the updates to applications in a later Protocol Pack release change the operation of a policy. Any such change is considered a policy compliance issue. To ensure that the operation of each policy remains aligned to the policy intent, the feature flags any compliance issues to enable you to address them.
Application Compliance	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Control Components Release 20.16.1	When you update the reference Protocol Pack, Cisco SD-WAN Manager checks whether any protocols in the Protocol Pack introduce name conflicts with currently defined custom applications. If so, Cisco SD-WAN Manager does not complete the update of the reference Protocol Pack.

Policy compliance

Describes how policy compliance checks compare policy application lists with the currently loaded Protocol Pack to identify reclassified or renamed applications and overly broad matches, helping preserve policy intent as Protocol Packs evolve.

A policy compliance check is a verification process that

- determines whether policies match applications that have become classified in a more granular fashion in a later Protocol Pack release
- checks for renamed applications, and
- checks for policies that match traffic broadly by transport protocol, such as http.

Check policy compliance

Various types of policies specify application traffic to match by using application lists, which contain one or more applications. The applications in application lists may be from a Protocol Pack or may be user-defined custom applications. As new Protocol Packs are released, changes occur to the protocol set. These changes may include adding applications that provide more granular classification of existing applications, renaming applications, and so on.

For example, an earlier Protocol Pack may include an application that captures all traffic for a set of services. A later Protocol Pack may include separate applications for different components of the services to provide more granular classification of the traffic. To illustrate with a fictional example, an application x-media might be broken into x-audio and x-video for more granular classification.

When checking the applications in a policy, Cisco SD-WAN Manager compares them with the applications in the Protocol Pack currently loaded in Cisco SD-WAN Manager. This check keeps the policy intent intact after new applications are added.

If Cisco SD-WAN Manager detects a compliance issue with a policy, it displays the affected policies and relevant new applications.

Application compliance

Describes application compliance, a name check that Cisco SD-WAN Manager runs when actions add new applications to the application catalog. It detects conflicts with existing custom application names and may block updates until you address conflicts.

A application compliance check is a feature in Cisco SD-WAN Manager that

- checks new applications when you add them to the application catalog, and
- detects name conflicts with currently defined custom applications.

Check application compliance

The application compliance check occurs during these actions:

Table 3: Application compliance checks

Event	Description
Updating the reference Protocol Pack	If uploading the new Protocol Pack would cause a name conflict, Cisco SD-WAN Manager aborts the upload. For about 24 hours, the task list shows the names of the custom applications that are potentially causing a name conflict. In the task list, click **Completed** and click the failed task to view the details. You can also view the names of these custom applications on the **Monitor** > **Logs** > **Audit Logs** page.
Adding cloud-sourced applications	If adding cloud-sourced applications would cause a name conflict, Cisco SD-WAN Manager aborts adding the cloud-sourced applications. For about 24 hours, the task list shows the names of the custom applications that are potentially causing a name conflict. In the task list, click **Completed** and click the failed task to view the details. You can also view the names of these custom applications on the **Monitor** > **Logs** > **Audit Logs** page.
Upgrading to Cisco Catalyst SD-WAN Manager Release 20.16.1 from a previous release	The upgrade includes Protocol Pack 71.0.0. This may potentially bring a Protocol Pack update from what you had loaded in a previous release of Cisco SD-WAN Manager. After this upgrade, Cisco SD-WAN Manager performs an application compliance check to detect any name conflicts. If there is a name conflict, Cisco SD-WAN Manager shows a message indicating the conflict, on the - **Maintenance** > **WAN Edge** page, and - **Configuration** > **Application Catalog** page. You can view details in the **Compliance** tab on the **Configuration** > **Application Catalog** page, or on the **Monitor** > **Compliance** page.

To prevent name conflicts with custom applications, from Cisco Catalyst SD-WAN Manager Release 20.16.1, Cisco SD-WAN Manager appends "-Custom" to the name of new custom applications.

Restrictions for the policy compliance check

Outlines restrictions for policy compliance check when using applications in Protocol Packs on Cisco IOS XE devices, and directs you to the NBAR2 Protocol Pack Library for release-specific updates and compatibility details.

- See the NBAR2 Protocol Pack Library for information about which Protocol Pack updates are available for each Cisco IOS XE release.
- Devices using a Cisco IOS XE release earlier than Cisco IOS XE Catalyst SD-WAN Release 17.14.1a support only policies that use applications that were available in the original built-in Protocol Pack release of the Cisco IOS XE release. They do not support policies that use applications added in subsequent Protocol Pack releases.

  For example, if the original built-in Protocol Pack release of the Cisco IOS XE release did not include application x, and a policy uses application x, then a router using a release earlier than Cisco IOS XE Catalyst SD-WAN Release 17.14.1a cannot support that policy. This is true even if you later upgrade the router to use a Protocol Pack that includes application x.

View and resolve policy compliance issues

Verify policy compliance issues and update or edit affected policies using the Policy Compliance area in Cisco SD-WAN Manager. Verify noncompliant policies against the current Protocol Pack and choose to update application lists or change the policy.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** > **Compliance**.

   In releases before Cisco Catalyst SD-WAN Manager Release 20.16.1, the option is **Policy Compliance**.

   In the **Policy Compliance** area, the table shows the policies that do not comply with the application lists in the current Protocol Pack.

2. In the **Policy Compliance** area, click **...** in the **Actions** column adjacent to the policy you want to update and choose one of these:
   - **Update Application**: Automatically updates the relevant application lists used by affected policies to incorporate the new application or applications.

     Note

     - Ensure that all devices in the network are using Cisco IOS XE Catalyst SD-WAN Release 17.14.1a or later. If there are devices in the network using earlier releases, updating applications may cause a failure in employing a policy.
     - For policies created using policy groups, this action does not deploy the policy to the devices. In this case, to update devices to use the adjusted policy, deploy the policy manually to the devices.

   - **Change Policy**: Opens the policy to enable you to manually edit the policy and address the use of the affected application.

View and resolve application name conflicts

Verify application name conflicts and compliance status in vManage to identify affected applications and policies. Use the Application Catalog Compliance tab or Monitor Compliance page to review conflicts introduced by upgrades and plan remediation.

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, Cisco Catalyst SD-WAN Control Components Release 20.16.1

Most methods of adding new applications automatically abort if there is a potential application name conflict. But upgrading to Cisco Catalyst SD-WAN Manager Release 20.16.1 or later from an earlier release can introduce name conflicts.

If there is a name conflict, Cisco SD-WAN Manager shows a message indicating the conflict, on the

- **Maintenance** > **WAN Edge** page, and
- **Configuration** > **Application Catalog** page.

You can view details

in the **Compliance** tab on the **Configuration** > **Application Catalog** page, or

on the **Monitor** > **Compliance** page.

Follow these steps to view and resolve application name conflicts:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog**.

   The page shows a message if there are any application name conflicts.

2. Click the **Compliance** tab.

   The **Application Compliance** area shows the affected applications and policies. It provides instructions for removing the custom applications to resolve the name conflict.

   If you intend to recreate a custom application, giving it a new name, note down the information in the custom application before removing it.

View application details

Verify application details in the application catalog to review configuration and metadata for custom applications. This procedure uses the menu to open the Applications tab and view details for a selected entry.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog**.
2. Click the **Applications** tab.
3. In the **Action** column, click **...** adjacent to a custom application and choose **View**.

3 Protocol Pack management and compliance

Topics:

- Protocol Pack management and compliance
- Protocol pack management and compliance
- How protocol pack upgrades work when devices become compatible
- Restrictions for protocol pack management and compliance
- Upload a Protocol Pack to Cisco SD-WAN Manager
- Upgrade a device protocol pack
- Verify protocol pack compliance
- View protocol pack status
- Delete protocol packs

Provides an overview of protocol pack management and compliance, outlining the purpose and scope of protocol packs and how they are maintained to align with organizational and regulatory requirements.

Protocol Pack management and compliance

Provides an overview of protocol pack management and compliance, outlining the purpose and scope of protocol packs and how they are maintained to align with organizational and regulatory requirements.

Protocol pack management and compliance

Describes how Cisco SD-WAN Manager includes a pre-installed Protocol Pack for classifying network traffic by application and explains that you can upload newer Protocol Pack releases when available to keep application policies and visibility current.

A Protocol Pack is a standard set of protocols that

- classifies network traffic according to the application producing the traffic
- supports application-aware policy, security policy, and QoS policy to match traffic based on the application producing the traffic, and
- provides application visibility by tracking which applications produce traffic within the network.

Protocol pack releases

Cisco SD-WAN Manager includes a pre-installed Protocol Pack, which is a standard set of protocols for classifying network traffic according to the application producing the traffic. The protocols, also called applications, can be used for application-aware policy, security policy, and QoS policy, to match traffic based on the application producing the traffic. And they are used for tracking which applications are producing traffic within the network—called application visibility.

Periodic Protocol Pack releases include updates to the application set, such as these:

- Expanding individual applications to a set of related applications to enable more granular classification of traffic
- New applications
- Renamed applications

For example, a Protocol Pack release may enable classifying the traffic produced by a multimedia application, and a subsequent release could distinguish with better granularity between the audio traffic and the video traffic that the multimedia application produces.

How protocol pack upgrades work when devices become compatible

Describes how upgrade requests for Protocol Packs are handled when some devices run incompatible Cisco IOS XE versions, including saving the request until a compatible software upgrade occurs and dropping the request if a subsequent upgrade still does not support the Protocol Pack.

If you attempt to execute a Protocol Pack upgrade for a set of devices, it is possible that one or more of the devices are using a Cisco IOS XE software version that does not support the new Protocol Pack. In this case, the upgrade does not proceed for those devices.

You can choose an option for SD-WAN Manager to save the upgrade request. SD-WAN Manager then checks the device when it receives a software upgrade, and if the new software version supports the Protocol Pack, SD-WAN Manager completes the upgrade.

Summary

Workflow

In unusual cases, SD-WAN Manager may drop the request to upgrade a device's Protocol Pack. This occurs when the next software upgrade on the device also does not support the Protocol Pack that you tried to push to the device.

1. You try to push a Protocol Pack x to a device using a software version that does not support the Protocol Pack x.

   Result: SD-WAN Manager does not push the Protocol Pack. It saves the request and checks back later to determine when the device will be able to support Protocol Pack x.

2. You upgrade the device's software to another version that still does not support Protocol Pack x.

   Result: In this case, SD-WAN Manager still cannot push the Protocol Pack to the device, and it drops the pending request.

Restrictions for protocol pack management and compliance

Outlines restrictions and recommendations for managing Protocol Pack upgrades using Cisco SD-WAN Manager, including minimum release requirements, upgrading the reference Protocol Pack first, and performing centralized upgrades with Cisco SD-WAN Manager rather than device-level CLI.

- We recommend upgrading the reference Protocol Pack on Cisco SD-WAN Manager to the latest version before upgrading the Protocol Pack on any devices in the network to that version.
- Minimum Cisco SD-WAN Manager release for upgrading Protocol Packs: Cisco Catalyst SD-WAN Manager Release 20.15.1
- We recommend using Cisco SD-WAN Manager to upgrade the Protocol Pack release on devices in the network, and not to do this individually on devices by CLI.

Upload a Protocol Pack to Cisco SD-WAN Manager

Configure protocol pack management by uploading a new Protocol Pack to Cisco SD-WAN Manager. Configure this action to make the pack available for device upgrades and, when newer, to update the reference release used for application and policy compliance.

Before you begin

For information about Protocol Pack releases, see the Cisco Protocol Pack documentation. A list of Protocol Packs appears on the NBAR2 Protocol Pack Library page.

Uploading a Protocol Pack that is a later release than previously uploaded Protocol Packs has two effects:

- As with any upload, the Protocol Pack is available for upgrading compatible devices in the network.
- If the uploaded Protocol Pack is a later release than previously uploaded Protocol Packs, it becomes the new reference release for Cisco SD-WAN Manager.

  Cisco SD-WAN Manager shows the current reference release on the **Configuration** > **Application Catalog** > **Application Source Settings** page, in the **Version** field.

  Cisco SD-WAN Manager uses the reference release as the basis for determining application compliance, policy compliance, and device Protocol Pack version compliance.

Procedure

1. Download a Protocol Pack from the Cisco Software Download site.
2. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** and click **Application Source Settings**.

3. Locate the **SD-WAN Manager Protocol Pack** section of the page.
4. Click **Upload SDWAN Manager Protocol Packs** to save the Protocol Pack to Cisco SD-WAN Manager.

   The uploaded Protocol Pack is available to upgrade any compatible devices in the network.

   As noted in **Before You Begin**, if the uploaded Protocol Pack is a later release than previously uploaded Protocol Packs then it becomes the new reference release. A pop-up window shows whether changing the reference Protocol Pack release would affect policy or device compliance.

   If any protocols in the Protocol Pack introduce name conflicts with existing custom applications, the upload does not proceed. See Information About Application Compliance section in the *Cisco Catalyst SD-WAN Policy Groups Configuration Guide*.

5. Click **Update** or **Ignore and Proceed** to complete the upload.

   Note

   If you do not want to complete the upload, such as if you do not want to change the reference Protocol Pack release, click **Cancel Update**.

Upgrade a device protocol pack

Configure Protocol Pack upgrades for devices in SD-WAN Manager by selecting target devices, choosing a release, and optionally scheduling or deferring installation until compatible software is available.

Before you begin

Install and enable Cisco SD-AVC on Cisco SD-WAN Manager before you upgrade device Protocol Packs. Cisco SD-AVC is required to use the Upgrade Device Protocol Pack feature. For more information, see Enabling SD-AVC on Cisco SD-WAN Manager in the *Cisco Catalyst SD-WAN Getting Started Guide*.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** and click **Application Source Settings**.
2. Locate the **SD-WAN Manager Protocol Pack** section of the page.
3. Select one or more devices in the table by checking the check boxes for the devices.
4. Click **Upgrade Device Protocol Pack**.
5. In the pop-up window, choose a Protocol Pack release to install. Optionally, choose a scheduled upgrade.

   Note

   If you schedule an upgrade for a later time, you cannot perform additional upgrades until that upgrade is complete. Only one upgrade task can be active at a given time. In a multitenant scenario, it is one upgrade task per tenant.

6. In case one or more selected devices have a software version that does not support the Protocol Pack, you can optionally select to upgrade the Protocol Pack later. Choose the Auto upgrade when device is compatible.

SD-WAN Manager saves the request to upgrade the Protocol Pack on those devices. SD-WAN Manager monitors the devices when they receive a software upgrade, and if the new software version supports the Protocol Pack, SD-WAN Manager completes the intended upgrade, installing the Protocol Pack.

Cisco SD-WAN Manager upgrades the Protocol Pack on the device if the device software version allows the upgrade.

Verify protocol pack compliance

Verify protocol pack compliance by manually initiating a check so devices and policies are assessed against the latest available protocol pack. Use this when protocol packs have been uploaded or upgraded and you want an immediate, up-to-date compliance status.

Before you begin

When you upload a new Protocol Pack, Cisco SD-WAN Manager automatically checks whether each device in the network is using the latest available Protocol Pack–called compliance. In addition, it checks policy and device Protocol Pack compliance at regular intervals.

You can trigger the compliance check manually using this procedure. This may be helpful, for example, to check compliance after upgrading the Protocol Pack on one or more devices.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** and click **Application Source Settings**.
2. Locate the **SD-WAN Manager Protocol Pack** section of the page.
3. Click **Sync Compliance**.

View protocol pack status

Verify protocol pack status in Cisco SD-WAN Manager by navigating to Application Source Settings and reviewing version, compatibility, reachability, and upgrade indicators for each router to confirm devices align with the latest release and are managed successfully.

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** and click **Application Source Settings**.
2. Locate the **SD-WAN Manager Protocol Pack** section of the page.

   At the top of the section, the **Version** field shows the latest Protocol Pack release uploaded to Cisco SD-WAN Manager.

   The table shows each router, the loaded Protocol Pack release, and related information, as described in this table:

Field	Description
Hostname	Device hostname.
Site ID	Device site ID.

Field	Description
Device Model	Device model name.
Software Version	Software release operating on the device.
Protocol Pack Version	Protocol Pack release loaded on the device.
Reachability	Reachability of the device by Cisco SD-WAN Manager.
Compatibility Status	• Green: The Protocol Pack loaded on the device matches the Protocol Pack loaded in Cisco SD-WAN Manager. • Red: The Protocol Pack loaded on the device does not match the Protocol Pack loaded in Cisco SD-WAN Manager.
Upgrade Status	Indicates whether a Protocol Pack upgrade has been performed on the device, and the status of the update: • **No job history**: No attempt to upgrade the Protocol Pack. • **In-progress**: Cisco SD-WAN Manager is currently upgrading the Protocol Pack on a device. • **Success**: Cisco SD-WAN Manager has upgraded the Protocol Pack. • **Skipped**: Cisco SD-WAN Manager did not find a compatible Protocol Pack. • **Failure**: Cisco SD-WAN Manager has tried unsuccessfully to upgrade a Protocol Pack. • **Scheduled**: Cisco SD-WAN Manager is scheduled to upgrade the Protocol Pack. • **Canceled**: Cisco SD-WAN Manager has canceled a scheduled upgrade.

Delete protocol packs

Verify and delete unused Protocol Packs in the Application Catalog from Application Source Settings. Configure removals only for packs not deployed, scheduled, or used as the reference Protocol Pack.

Before you begin

Follow these steps to delete protocol packs:

Procedure

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog**.
2. Open **Application Source Settings**.
3. Click **Delete Protocol Pack**.

   SD-WAN Manager shows a list of the loaded Protocol Packs. The list provides an option to delete Protocol Packs that are not in use in the network, and that don't meet other conditions that require them to remain available. The conditions include, but are not limited to:

- Protocol Packs that are currently deployed or scheduled for deployment
- The Protocol Pack that SD-WAN Manager is using as its reference Protocol Pack

4. From the list of loaded Protocol Packs, delete any desired Protocol Pack that has the delete option available.