Application and Policy Compliance

Application and Policy Compliance

Table 1: 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.

Information About 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.

If a policy matches traffic using an application list that includes the x-media application, the policy does not make use of the later, more granular classification as x-audio and x-video.

Check Policy Compliance

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. Cisco SD-WAN Manager checks policies for the following compliance issues:

- Checks existing policies to determine whether the policies match applications that have become classified in a more granular fashion in a later Protocol Pack release.
- Checks for renamed applications. For example, renaming application Skydrive to Onedrive.
- Checks for policies that match traffic broadly by transport protocol, such as http. When a policy matches traffic so broadly, it is difficult to anticipate which new applications, in later Protocol Packs, may be included in the match.

This check keeps the policy intent intact after new applications are added.

View Compliance Issues

If Cisco SD-WAN Manager detects a compliance issue with a policy, it displays the affected policies and relevant new applications. For information about viewing compliance issues, see View and Resolve Policy Compliance Issues , on page 4.

Information About Application Compliance

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

Application compliance is a feature in Cisco SD-WAN Manager that checks new applications when you do something that adds applications to the application catalog. When you add applications, it checks whether any of the new applications have the same name as a currently defined custom application, which would cause a name conflict.

The application compliance check occurs during these actions:

Table 2: Application Compliance Check

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.

Resolving Compliance Issues

To resolve name conflict issues, remove the custom applications that have name conflicts. See View and Resolve Application Name Conflicts, on page 4.

Preventing Name Conflicts

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

- 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

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

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

Information About Application Compliance, on page 2 describes the details of when Cisco SD-WAN Manager performs an application compliance check. 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.

Procedure

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

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

Step 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. See View Application Details, on page 5.

View Application Details

Procedure

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

Step 2 Click the **Applications** tab.

Step 3 In the **Action** column, click **...** adjacent to a custom application and choose **View**.