Configure Policies

Policy Overview

Cisco DNA Center enables you to create policies that reflect your organization's business intent for a particular aspect of the network, such as network access. Cisco DNA Center takes the information collected in a policy and translates it into network-specific and device-specific configurations required by the different types, makes, models, operating systems, roles, and resource constraints of your network devices.

Using Cisco DNA Center, you can create virtual networks, access control policies, traffic copy policies, and application policies.

Group-Based Access Control

Cisco DNA Center implements Software-Defined Access in two ways:

- Virtual networks (VNs) provide macro-level segmentation, such as to separate IoT devices from the corporate network.
- Group-based policies provide micro-level segmentation, such as to control what types of network traffic to permit or deny between engineering and HR groups.

Group-Based Access Control policies provide the following benefits:

- Rich identity-based access control functionality with network automation and assurance benefits.
- Granular access control.
- Scalable groups apply to all virtual networks, which simplifies policy management.
- Policy views help you to understand the overall policy structure, and create or update required access control policies.

- Eliminates the need to switch between different applications to manage scalable groups and define protected assets.
- Provides enhanced features for deploying enterprise-wide access control policies.
- Restricts lateral movement of threats like ransom ware before you have identity or Network Admission Control (NAC) applications in place.
- Provides an easy migration path to Cisco Identity Services Engine (Cisco ISE) for users who are using third-party identity applications, but want to move to Cisco ISE.

For information about creating IP pools, sites, and virtual networks in Cisco DNA Center, see the Cisco DNA Center User Guide.

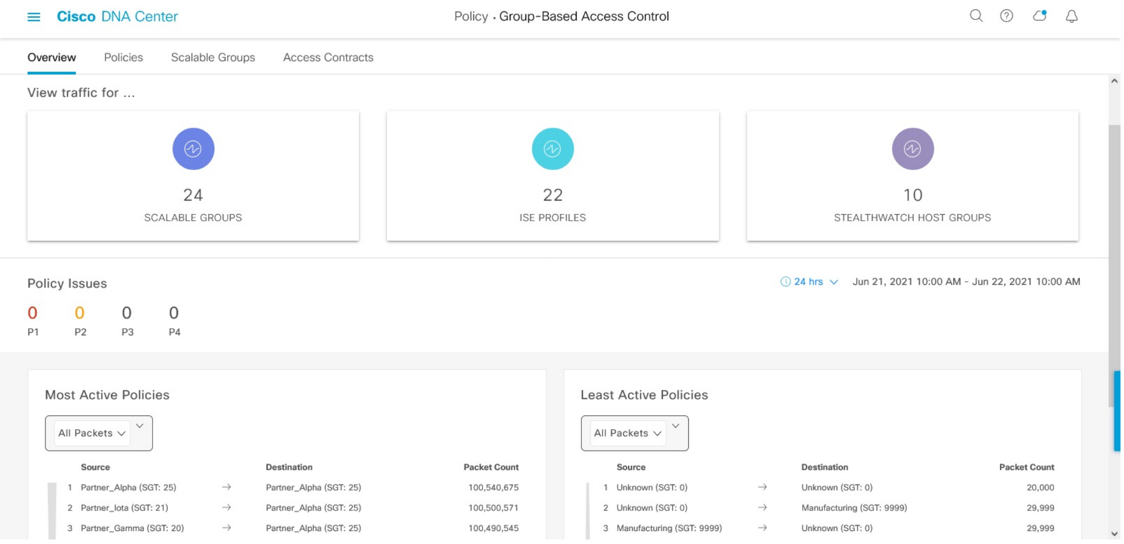
For information about configuring Cisco DNA Center for Cisco ISE, see the Cisco DNA Center Installation Guide.

For information about configuring Cisco ISE for Cisco DNA Center, see the Cisco Identity Services Engine Administrator Guide.

Group-Based Access Control Policy Dashboard

The Group-Based Access Control Policy dashboard provides you with a summary of network activity, policy-related issues, and traffic trends. In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Group-Based Access Control** > **Overview** to view this dashboard.

Figure 1: Group-Based Access Control Policy Dashboard



Most Active Policies

	Source		Destination	Packet Count
1	Partner_Alpha (SGT: 25)	→	Partner_Alpha (SGT: 25)	100,540,675
2	Partner_Iota (SGT: 21)	→	Partner_Alpha (SGT: 25)	100,500,571
3	Partner_Gamma (SGT: 20)	→	Partner_Alpha (SGT: 25)	100,490,545

Least Active Policies

	Source		Destination	Packet Count
1	Unknown (SGT: 0)	→	Unknown (SGT: 0)	20,000
2	Unknown (SGT: 0)	→	Manufacturing (SGT: 9999)	29,999
3	Manufacturing (SGT: 9999)	→	Unknown (SGT: 0)	29,999

You can view the following details in this dashboard:

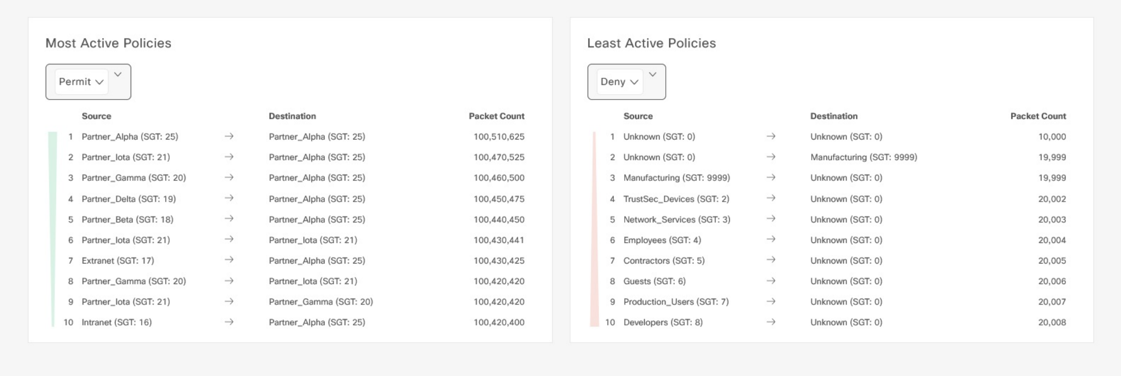
- **View Traffic**: You can view the traffic for scalable groups, Cisco ISE profiles, and stealthwatch host groups. You must install the Group-Based Policy Analytics package to view this data. Group-Based Policy Analytics provides you with insights to create group-based policies by visualizing communications between assets in order to assess the impact of introducing new access controls, and understand exactly which protocols you need to allow in the policies. Cisco Group-Based Policy Analytics aggregates information on groups of assets on your network, and their communication. For more information, see Cisco Group-Based Policy Analytics, on page 12.

- **View Policy-Related Issues**: It displays a count of policy-related issues. Click a counter to view the details. It opens the **Assurance Issues** dashboard in a new browser tab, where you can view the details.

  Note that this view of policy-related issues is for the currently selected time period. Use the time selector to adjust the time window, as needed.

- **View Most Active and Least Active Policies**: It provides the details about the most active and least active policies. By default, this view is based on the count of total number of packets seen in the network for each policy (for each source-to-destination group pairing). You can use the drop-down list to select only the permitted packets or dropped packets. You can use the dropped packets option to see which policies are enforcing policy-based drops most actively.

  Figure 2: Most and Least Active Policy Dashlets



Most Active Policies

	Source		Destination	Packet Count
1	Partner_Alpha (SGT: 25)	→	Partner_Alpha (SGT: 25)	100,510,625
2	Partner_Iota (SGT: 21)	→	Partner_Alpha (SGT: 25)	100,470,525
3	Partner_Gamma (SGT: 20)	→	Partner_Alpha (SGT: 25)	100,460,500
4	Partner_Delta (SGT: 19)	→	Partner_Alpha (SGT: 25)	100,450,475
5	Partner_Beta (SGT: 18)	→	Partner_Alpha (SGT: 25)	100,440,450
6	Partner_Iota (SGT: 21)	→	Partner_Iota (SGT: 21)	100,430,441
7	Extranet (SGT: 17)	→	Partner_Alpha (SGT: 25)	100,430,425
8	Partner_Gamma (SGT: 20)	→	Partner_Iota (SGT: 21)	100,420,420
9	Partner_Iota (SGT: 21)	→	Partner_Gamma (SGT: 20)	100,420,420
10	Intranet (SGT: 16)	→	Partner_Alpha (SGT: 25)	100,420,400

Least Active Policies

	Source		Destination	Packet Count
1	Unknown (SGT: 0)	→	Unknown (SGT: 0)	10,000
2	Unknown (SGT: 0)	→	Manufacturing (SGT: 9999)	19,999
3	Manufacturing (SGT: 9999)	→	Unknown (SGT: 0)	19,999
4	TrustSec_Devices (SGT: 2)	→	Unknown (SGT: 0)	20,002
5	Network_Services (SGT: 3)	→	Unknown (SGT: 0)	20,003
6	Employees (SGT: 4)	→	Unknown (SGT: 0)	20,004
7	Contractors (SGT: 5)	→	Unknown (SGT: 0)	20,005
8	Guests (SGT: 6)	→	Unknown (SGT: 0)	20,006
9	Production_Users (SGT: 7)	→	Unknown (SGT: 0)	20,007
10	Developers (SGT: 8)	→	Unknown (SGT: 0)	20,008

  Note that this view of policy activity is for the currently selected time period. Use the time selector to adjust the time window, as needed.

Group-Based Access Control Policies

The access control policies define which network traffic can pass from a source scalable group to a destination scalable group.

- **Scalable Group**: A classification category, to which you can assign users, network devices, or resources. Scalable groups are used in access control policies. You can associate scalable groups with virtual networks based on your organization's network configuration, access requirements, and restrictions.

- **Contract**: An access contract is a set of rules that controls the type of network traffic that is allowed to pass between the source and destination scalable groups. In other words, a contract is a traffic filter definition. Access contracts define the actions (permit or deny) performed when the traffic matches a network application, protocol, and port. The default action is to use the Catch All rule when no other rules match.

- **Group-Based Access Control Policies**: A group-based access control policy identifies a specific source and destination group pair and associates an access contract. The access contract specifies what types of traffic are permitted or denied between the source group and the destination group. These policies are unidirectional.

Scalable groups and access contracts are the basic building blocks of access control policy. While creating the access control policy, you can use the scalable groups and contracts that you have created before or create new scalable groups and contracts while creating the policy. If you want to specify the network resources that can be accessed from a specific source group, you can create an access control policy with a single source and multiple destination groups. On the other hand, if you want to specify the source groups that are permitted to access a particular network resource, you can create an access control policy with a single destination and multiple source groups. For example, if you want to specify the network resources that can be accessed by the users associated with the "contractors" source scalable group, you can create an access control policy with a single source and multiple destination groups. If you want to specify the source groups that are permitted to access the "Finance Servers" destination scalable group, you can create an access control policy with single destination and multiple source groups.

You can specify the default policy to use when no contract is specified for a source and destination scalable group combination. The default policy is **Permit**. You can change this policy to **Deny**, **Permit_IP_Log**, or **Deny_IP_Log**, if necessary. You can set the default policy based on your network type, an open or closed network.

Note We recommend that you change the default policy from "Permit" to "Deny" only if you have created explicit policies to permit necessary network traffic for all your network infrastructure devices. Failure to do so can result in loss of network connectivity.

List View

Click the **List** icon at the top right of the **Group-Based Access Control** window to launch the **List** view.

- **Source View**: Displays a list of existing policies organized based on the source groups. You can expand each row to view the specific source-destination policy details.
- **Destination View**: Displays a list of existing policies organized based on the destination groups. You can expand each row to view the specific source-destination policy details.

To see which destination groups are available from a specific source group, use the **Source** view. To see which source groups are permitted to access a particular destination group, use the **Destination** view. For example, to see which destination groups are available to users who are part of the "Contractors" source scalable group, use the **Source** view. To see which source groups can access the "Finance servers" destination scalable group, use the **Destination** view.

You can also view the policy enforcement statistics data in the policies listing table. The total number of policy permits and denies are displayed for the selected time period.

The policy enforcement statistics are collected from the network devices that are provisioned for group-based policy and telemetry data language (TDL) subscription. These configurations are normally provisioned automatically for network devices that are part of a fabric. Manual configuration can be done for nonfabric network devices.

Note the following points while using the policy enforcement statistics data:

- Policy enforcement statistics data is available only when Group-Based Policy Analytics package is deployed.

- Telemetry subscription is added as part of base provisioning for both fabric and nonfabric network devices. TrustSec enforcement command is pushed when a new network device is added to DNAC and assigned to a site.

- Software-Defined Access (SDA) adds TrustSec enforcement for the network devices that are added to a fabric. TrustSec telemetry data is collected only when this enforcement is enabled on a network device. If it is not enabled, the telemetry subscriptions used for policy monitoring are used to collect the TDL data for TrustSec.

- Cisco IOS XE 16.12 and later support TDL streaming data.

- NETCONF must be enabled on the network devices.

- The following configuration must be added manually for the nonfabric network devices:

  ```
  cts role-based enforcement vlan-list <VLAN of the endpoints>
  ```

- After upgrading to Cisco DNA Center 2.2.2, you might see the following message in the **Provision > Network Devices > Inventory** window:

  ```
  We detected IOS-XE devices in your network where new telemetry subscription for assurance
  data needs to be enabled and some of the existing subscription needs to be optimized
  for performance. Please note that you will have to enable netconf and configure the
  netconf port in the Inventory credentials for these devices. Also note that these devices
  will receive a new subscription for group based policy monitoring telemetry. Do you
  want to take an action to provision these subscriptions?
  ```

  Click **Apply Fix** to push the configuration to all network devices with site assigned.

Click **Deploy** to deploy the updated policies to the network devices. When you click **Deploy**, Cisco DNA Center requests the Cisco Identity Services Engine (Cisco ISE) to send notifications about the policy changes to the network devices.

Matrix View

Click the **Grid** icon at the top right of the **Group-Based Access Control** window to launch the Matrix view. The Matrix view is a core policy view, which provides an overview of all policies for all scalable groups (whether explicit or default). You can use the Matrix view to view all source and destination policies and understand the overall policy structure. You can view, create, and update access control policies from the Matrix view.

The Matrix view contains two axes:

- Source Axis: The vertical axis lists all the source scalable groups.

- Destination Axis: The horizontal axis lists all the destination scalable groups.

Place the cursor on a cell to view the policy for a given source scalable group and a destination scalable group. The color of a cell is based on the policy that applies to that cell. The following colors indicate which policies are applied to each cell:

- **Permit**: Green

- **Deny**: Red

- **Custom**: Gold

- **Default**: Gray

Place the cursor on the **Permit**, **Deny**, **Custom**, or **Default** icon that is displayed at the top of the matrix to view the cells to which that policy is applied.

Click a cell to open the **Create Policy** or **Edit Policy** slide-in pane that allows you to create or edit the policies for the selected cell. The **Create Policy** slide-in pane shows the source and destination scalable groups as read-only fields. You can update the policy status and access contract.

You can create custom views of the policy matrix to focus only on the policies that you are interested. To do this, click the **View** drop-down list and choose **Create View**. While creating the custom view, you can specify the subset of scalable groups that you want to include in the custom view. You can save the custom views and edit them later, if required. Click the **View** drop-down list and choose **Manage Views** to create, edit, duplicate, or delete the custom views. The **Default View** shows all the source and destination scalable groups.

You can navigate through the matrix by dragging the matrix content area with the cursor or by using horizontal and vertical scroll bars. You can also use the mini-map to navigate through the matrix. The mini-map helps you to easily navigate through the matrix when the matrix size is large and it extends beyond the screen size. You can move and place the mini-map anywhere on your screen. The mini-map provides the whole matrix view. The light gray portion in the mini-map represents the portion of the matrix that is currently displayed on your screen. You can drag that area to scroll through the matrix.

Note The mini-map is closed by default. Click the **Expand** icon to expand and view the mini-map.

The Matrix view highlights the cell and the corresponding row (source scalable group) and column (destination scalable group) when a cell is selected. The coordinates (source and destination scalable groups) of the selected cell are displayed near the matrix content area.

Click **Deploy** to deploy the updated policies on the network devices. When you click **Deploy**, Cisco DNA Center requests Cisco ISE to send notifications about the policy changes to the network devices.

You can use the **Filter** option to view a subset of the policy matrix, for a selected set of source and destination groups. You can create a filter to focus only on the policies that you are interested. To create the filter, select the source and destination groups that you want to include.

Cisco DNA Center integrates with Cisco ISE. Cisco ISE provides the runtime policy platform for providing policy download to the network devices on behalf of Cisco DNA Center. The TrustSec Workcenter user interface screens for Security Groups, Security Group Access Control Lists (SGACLs), and Egress Policy are displayed in Read-Only mode in Cisco ISE to prevent policy synchronization issues.

Policy Creation Overview

1. Define categorizations for your organization, or the portion of your organization that you plan to start with.

2. Create scalable groups for the categorizations that you identified.

3. Create access contracts for the types of network traffic you wish to control. There are predefined sample access contracts to Permit or Deny all traffic, and also some example contracts showing more specific traffic filtering. You can create additional, more granular access contracts based on specific application definitions.

4. Decide which categories of network users require access to particular network resources, such as application servers and connections to other networks.

5. Create access policies, associate a source group, a destination group, and an access contract, to define how traffic is allowed to flow from the source to the destination.

Create Scalable Groups

Before you begin

To perform the following task, you must be a Super Admin or Network Admin.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Group-Based Access Control** > **Scalable Groups**.

Step 2 Click **Create Scalable Group**.
The **Create Scalable Group** slide-in pane appears.

Step 3 In the **Create Scalable Group** slide-in pane, enter a name and description (optional) for the scalable group.

Note The following characters are supported for the **Name** field:

- alphanumeric characters
- underscore (_)

The scalable group name must start with an alphabetic character.

Cisco DNA Center generates the tag value. You can update this value, if necessary. An error message is displayed if the value that you specify is already used by an existing scalable group. The valid range is from 2 to 65519.

Step 4 Choose the **Virtual Networks** to be associated with this scalable group from the drop-down list. By default, the default virtual network (`DEFAULT_VN`) is selected.

Step 5 Check the **Propagate to ACI** check box if you want the scalable group to be propagated to Cisco Application Centric Infrastructure (ACI).

Step 6 Click **Save**.

The **Scalable Groups** window displays the scalable group name, tag value, assigned virtual networks, and associated policies. You can also view the sample scalable groups in this window. You can use or delete those scalable groups.

You can edit or delete the scalable groups from the **Scalable Groups** window. Click the **Scalable Group Name** link to view the details of a scalable group. Click **Edit** in the **View Scalable Group** window to update the scalable group details. When you click **Deploy**, Cisco DNA Center requests Cisco ISE to send notifications about the changes to the network devices.

Click the link in the **Policies** column of a scalable group to view the access control rules that use that scalable group and the policy to which it belongs. You cannot delete a scalable group if it is used in any access policy.

An orange triangle icon is displayed next to a scalable group if synchronization with Cisco ISE is not completed.

Cisco ISE supports packets coming from ACI to the TrustSec domain by synchronizing the Internal Endpoint Groups (IEPGs) and creating correlating read-only scalable groups in Cisco ISE. These scalable groups are displayed in the **Scalable Groups** window with the value `ACI` in the **Created In** column. You cannot edit or delete the scalable groups that are learned from ACI, but you can use them in the policies.

The **Associated Contracts** column shows the associated ACI-learned contracts for the scalable groups that are learned from ACI. Click the link displayed in the **Associated Contracts** column to view the details about the associated contracts.

When an IEPG is updated in ACI, the corresponding scalable group configuration is updated in Cisco ISE. A new EEPG is created in ACI, when a scalable group is created in Cisco ISE.

Note You cannot create a scalable group with the name "ANY" or tag value 0xFFFF/65535. Scalable Group ANY/65535 is a reserved internal scalable group that is used for the Cisco DNA Center default policy.

While synchronizing the scalable groups in Cisco DNA Center with Cisco ISE:

- If a scalable group is present in Cisco DNA Center and is not present in Cisco ISE, it is created in Cisco ISE.
- If a scalable group is present in Cisco ISE and is not present in Cisco DNA Center, it is created in Cisco DNA Center.
- If the scalable group name is same in both Cisco DNA Center and Cisco ISE, but the description and ACI data are different, Cisco DNA Center is updated with the data specified in Cisco ISE.
- If the scalable group name is same in Cisco DNA Center and Cisco ISE, but the tag values are different, a new scalable group with the tag value specified in Cisco ISE is created in Cisco DNA Center. The name of the existing scalable group in Cisco DNA Center is updated with the suffix `_DNAC`.
- If the tag value is same but the scalable group name is different, the scalable group name in Cisco DNA Center is updated with the name specified in Cisco ISE.

Create Access Contracts

An access contract is a set of rules that controls the type of network traffic that is allowed to pass between the source and destination scalable groups. Access contracts define the actions (permit or deny) performed when the traffic matches a network application, protocol, and port.

Note Security Group Access Control List (SGACL) in Cisco ISE is called `Access Contract` in Cisco DNA Center.

Before you begin

To perform the following task, you must be a Super Admin or Network Admin.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Group-Based Access Control** > **Access Contracts**.

Step 2 Click **Create Access Contract**.

Step 3 In the **Create Access Contract** slide-in pane, enter a name and description for the contract.

Step 4 Create the traffic filter rules:

- From the **Action** drop-down list, choose **Deny** or **Permit**.

- From the **Application** drop-down list, choose the application for which you want to apply that action. The port and protocol are automatically selected based on the application that you select.

  If you want to specify the transport protocol, source port, and destination port, choose the **Advanced** option from the **Application** drop-down list.

You can create multiple rules. To create multiple rules for a contract, click the + symbol and choose the settings for the **Action** and **Application** columns. The rules are checked in the order in which they are listed in the contract. Use the handle icon at the left end of a rule to drag and change the order of the rule.

You can enable or disable logging for any traffic filter rule (including the default action) by using the **Logging** toggle. Logging is disabled by default. When logging is enabled, the network device sends a syslog message when the traffic filter rule is hit. This might be helpful in troubleshooting and initial testing of a policy. However, we recommend that you use this option sparingly, because it might have a resource and performance impact on the network devices.

Step 5 From the **Default Action** drop-down list, choose **Deny** or **Permit**.

You can enable logging for the default action, if required.

Step 6 Click **Save**.

You can view, create, duplicate, update, and delete contracts from the **Access Contracts** listing window.

You can also view the sample contracts in the **Access Contracts** window. You can use or delete those sample contracts. However, you cannot delete the default contracts (Permit IP, Deny IP, Permit_IP_Log, and Deny_IP_Log).

Click the **Contract Name** link in the **Access Contracts** window to view the details of a contract. Click **Edit** in the **View Contract** window to edit the contract details.

An orange triangle icon is displayed next to a contract if synchronization with Cisco ISE is incomplete.

The contracts that are learned from ACI are displayed in the **Access Contracts** window with the value `ACI` in the **Created In** column. You cannot edit or delete the contracts that are learned from ACI, but you can use them in the policies while using the ACI-learned scalable groups. While creating or updating a policy from the Matrix view, if you select an ACI-learned scalable group as the destination group, the associated contracts are displayed in the **Preferred Contracts** tab. You can view all the contracts in the **All Contracts** tab.

You can view the number of rules used in each contract in the **Rules Count** column.

Click the link in the **Policies** column of a contract to view the policies that use that contract.

You cannot delete a contract if it is used in a policy. You must delete the contract from that policy before you delete the contract.

When you update the scalable groups, contracts, or policies, you must deploy the changes on the network devices. If you update the policies and do not deploy the updated policies, notifications about the policy changes are not sent to the network devices and the policies that are currently active in the network may not be consistent with the policy information displayed in Cisco DNA Center. To resolve this situation, you must deploy the updated policies on the network devices.

You can duplicate an existing contract and create a new contract by editing the required details. When you duplicate a contract, all information in the existing contract is copied and the copied contract has the existing contract name with the string `Copy` appended at the end.

You can use the **Filter** option to search for the contracts that you look for.

While synchronizing the access contracts in Cisco DNA Center with Cisco ISE:

- If a contract is present in Cisco DNA Center and is not present in Cisco ISE, it is created in Cisco ISE.
- If a contract is present in Cisco ISE and is not present in Cisco DNA Center, it is created in Cisco DNA Center.
- If the contract name is the same in Cisco DNA Center and Cisco ISE, but the description and traffic rule content are different, Cisco DNA Center is updated with the data specified in Cisco ISE.
- If the contract name and rule are the same, but the description is different, Cisco DNA Center is updated with the description specified in Cisco ISE.
- Text SGACL command lines in Cisco ISE are migrated as content that cannot be parsed. You can edit these contracts, but Cisco DNA Center does not parse them or check syntax. The changes that you make in Cisco DNA Center are reflected in Cisco ISE.
- If a policy has multiple SGACLs in Cisco ISE, those contracts are migrated as default policies in Cisco DNA Center.

Create Group-Based Access Control Policy

Scalable groups and access contracts are the basic building blocks of an access control policy. While creating an access control policy, you can use the scalable groups and contracts that you have created before, or create new scalable groups and contracts while creating the policy.

If you want to specify the network resources that can be accessed from a specific source group, you can create an access control policy with a single source and multiple destination groups. On the other hand, if you want to specify the source groups that are permitted to access a particular network resource, you can create an access control policy with a single destination and multiple source groups.

For example, if you want to specify the network resources that can be accessed by the users associated with the *Contractors* source scalable group, you can create an access control policy with a single source and multiple destination groups. If you want to specify the source groups that are permitted to access the *Finance Servers* destination scalable group, you can create an access control policy with a single destination and multiple source groups.

Group-based access control policies can also be created or updated based on the traffic flows for a given source and destination group pair.

To create a group-based access control policy, use the following procedure.

Step 1 From the **Policy List** or **Matrix** view, click **Create Policies**.

Step 2 To create an access control policy with a single source and multiple destination groups, click **Source to Destination(s)** and complete these steps:

a) Click the radio button next to the source scalable group that you want to select. If the scalable group that you need does not exist, click **Create Scalable Group** to create a new scalable group. For more information, see Create Scalable Groups, on page 7.

b) Click **Next**.

c) Choose the destination scalable groups to map to the selected source scalable group.

You can view the scalable group details and edit the scalable groups, if necessary.

If a policy already exists between the source and destination, an orange triangle icon is displayed near a scalable group.

d) Click **Next**.

e) Click the radio button next to the contract that you want to select. If the contract that you need does not exist, click **Create Contract** to create a new contract. For more information, see Create Access Contracts, on page 8.

You can view and edit the contract details, if necessary.

Note You can choose only one contract for a policy.

f) Click **Next**.

The **Summary** window lists the policies that are created based on the selected scalable groups and contract.

g) Click **Save**.

Step 3 To create an access control policy with a single destination and multiple source groups, click **Destination to Source(s)** and complete the following steps:

a) Click the radio button next to the destination scalable group that you want to select. If the scalable group that you need does not exist, click **Create Scalable Group**.

b) Click **Next**.

c) Choose the source scalable groups to map to the selected destination scalable group.

You can view the scalable group details and edit the scalable groups, if necessary.

If a policy already exists between the source and destination, an orange triangle icon is displayed near a scalable group.

d) Click **Next**.

e) Click the radio button next to the contract that you want to select. If the contract that you need does not exist, click **Create Contract**.

You can view and edit the contract details, if necessary.

Note You can choose only one contract for a policy.

f) Click **Next**.

The **Summary** window lists the policies that are created based on the selected scalable groups and contract.

g) Click **Save**.

Note You can toggle between the **List** view and the **Drag and Drop** view using the **Toggle** button in the top-right corner of the Scalable Group listing area. The **Drag and Drop** view allows you to drag and drop the scalable groups to the **Source** and **Destination** fields while creating the access control policy. However, only the first 50 scalable groups are listed in the **Drag and Drop** view. You can use the **Drag and Drop** view if you have a smaller number of scalable groups (up to 50). If you have more than 50 scalable groups, use the **List** view to view them all.

To create or modify a group-based access control policy based on the traffic flows:

1. From the policy matrix view, click the cell for which you want to create or modify the group-based access control policy.

2. In the **Policy Details** slide-in pane, click **View Traffic Flows**.

   In the **View Traffic Flows** slide-in pane, you can see the rules for the selected contract or the default policy in the left pane. You can view the traffic flows that match any selected rule in the right pane.

3. Click **View Traffic** in the Default Action rule to see the list of flows that match that rule. While modifying an existing policy using access contracts with additional rules, you can use the **View Traffic** option for any rule to see the list of flows matching that rule.

4. For policies that are using the Default Action rule (with no explicitly selected access contract), you can select an access contract or create a new access contract to be used by that policy.

   For policies with access contract PERMIT or DENY, you can select an access contract or create a new access contract to be used by that policy.

   For policies with custom access contract, you can edit the selected access contract.

   While saving a newly created or edited contract, you have the following options:

   - Save the changes to the existing contract. Changes affect all policies that reference the contract.
   - Save the changes as a new contract. Changes are applied only to the current policy.
   - Save the changes as a new contract. Changes are not applied to any policy.

While synchronizing the policies in Cisco DNA Center with Cisco ISE:

- If a policy is present in Cisco DNA Center and is not present in Cisco ISE, it is created in Cisco ISE.
- If a policy is present in Cisco ISE and is not present in Cisco DNA Center, it is created in Cisco DNA Center.
- If a policy contract is different in Cisco ISE, Cisco DNA Center is updated with the contract specified in Cisco ISE.
- Policy mode information (Enabled, Disabled, or Monitor) is also imported from Cisco ISE.

Cisco ISE has an option to allow multiple SGACLs for a single policy (this option is not enabled by default in Cisco ISE). Cisco DNA Center does not support the use of multiple access contracts for a single policy. During policy synchronization, if a policy in Cisco ISE has multiple SGACLs, the Cisco DNA Center administrator is given the option to change that policy to have no contract selected (to use the default policy). The administrator can select a new or existing access contract for that policy after the policy synchronization is complete.

Cisco Group-Based Policy Analytics

Group-Based Policy Analytics enables you with insights, to create group-based policies by visualizing communications between assets, to assess the impact of introducing new access controls, and understand exactly which protocols you need to allow in the policies.

Cisco Group-Based Policy Analytics aggregates information on groups of assets on your network, and their communication to answer the following questions:

- Which groups are communicating with each other?
- What kind of communication is this?
- Which group does a given asset belong to?

Installation

You can purchase one of following types of licenses for Cisco DNA Center:

- Cisco DNA Essentials
- Cisco DNA Advantage
- Cisco DNA Premier

Cisco DNA Advantage and Cisco DNA Premier contain the Group-Based Policy Analytics package. This package consists of the following archives (.tar.gz files):

- Backend
- User Interface
- Summarizer Pipeline
- Aggregation definitions

Cisco Group-Based Policy Analytics is a part of Cisco DNA Center but, is not installed by default. In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System** > **Software Updates** > **Installed Apps**. Scroll down to **Group-Based Policy Analytics** under **Policy Applications**. Click **Install** to install the application.

Hardware and Software Compatibility

Platform Support

Cisco Group-Based Policy Analytics is supported on the following hardware platforms:

- 44 cores, single node or three-node cluster
- 56 cores, single node or three-node cluster
- 112 cores, single node or three-node cluster

These platforms must meet the performance and scalability requirements mentioned here.

For details about the supported hardware, see Cisco UCS M4 appliances or Cisco UCS M5 appliances.

The following table lists the performance metrics that Cisco DNA Center and Cisco Group-Based Policy Analytics support on each of the core platforms. The NetFlow metrics were introduced by Cisco Group-Based Policy Analytics.

Table 1: Performance Metrics

Metric	44 cores, three nodes	56 cores	112 cores
Devices (NADs)	5000 1000 switches or 1000 routers or a combination of both; 4000 APs	8000 2000 switches or 2000 routers or a combination of both; 6000 APs	18,000 5000 switches or 5000 routers or a combination of both; 12,000 APs

Metric	44 cores, three nodes	56 cores	112 cores
Clients (endpoints)	25,000 20,000 wireless; 5,000 wired	40,000 30,000 wireless; 10,000 wired	100,000 60,000 wireless; 40,000 wired
NetFlows per sec	30,000	48,000	120,000

Device Support

You must enable NetFlow to use Cisco Group-Based Policy Analytics. The following table shows the various ways in which NetFlow can be enabled on different network devices.

Table 2: Device Support

Network Devices	Series	NetFlow Configurable in telemetry section of Network Settings in Cisco DNA Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow Configurable using the template editor tool in the Cisco DNA Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow Collection in Fabric Deployment	NetFlow Collection in Nonfabric Deployment
Routers	Cisco 1000 Series Integrated Services Routers (ISR1K)	Yes	Yes	Yes	Yes
	Cisco 4000 Series Integrated Services Routers (ISR4K)	Yes	Yes	Yes	Yes
	Cisco Cloud Services Router 1000v Series (CSR 1000v)	Yes	Yes	Yes	Yes
	Cisco 1000 Series Aggregation Services Routers (ASR1K)	Yes	Yes	Yes	Yes

Network Devices	Series	NetFlow Configurable in telemetry section of Network Settings in Cisco DNA Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow Configurable using the template editor tool in the Cisco DNA Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow Collection in Fabric Deployment	NetFlow Collection in Nonfabric Deployment
Switches	Cisco Catalyst 9200 series	Yes	Yes	Yes	Yes
	Cisco Catalyst 9300 Series	Yes	Yes	Yes	Yes
	Cisco Catalyst 9400 Series	Yes	Yes	Yes	Yes
	Cisco Catalyst 9500 Series	No	Yes	Yes	Yes
	Cisco Catalyst 9600 Series	No	Yes	Yes	Yes
	Cisco Catalyst 2k series	No	Yes	NA	Yes
	Cisco Catalyst 3560 series	No	Yes	NA	Yes
	Cisco Catalyst 3650 series	No	Yes	Yes	Yes
	Cisco Catalyst 3850 series	No	Yes	Yes	Yes
	Cisco Catalyst 4k series	No	Yes	Yes	Yes
	Cisco Catalyst 6500 Series Switches	No	Yes	Yes	Yes
	Cisco Catalyst 6800 Series Switches	No	Yes	Yes	Yes
Wireless Controllers	Cisco 3504 Wireless Controller (AireOS-Based)	Yes	Yes	No	Yes, only central switching SSID
	Cisco 5520 Wireless Controller (AireOS-Based)	Yes	Yes	No	Yes, only central switching SSID
	Cisco 8540 Wireless Controller (AireOS-Based)	Yes	Yes	No	Yes, only central switching SSID
	Cisco Catalyst 9800 based controller	Yes	Yes	Yes	Yes

Cisco ISE

Cisco ISE 2.4 Patch 7 and later, Cisco ISE 2.6 Patch 1 and later, and Cisco ISE 2.7 and later are supported.

Cisco Stealthwatch

Cisco Stealthwatch 7.x or later is supported.

Browser Support

Cisco Group-Based Policy Analytics is compatible with 64-bit Windows, Macintosh, and Linux systems with the following web browsers:

- Google Chrome: Version 73.0 or later
- Mozilla Firefox: Version 65.0 or later

Understand Connectors

Cisco Group-Based Policy Analytics gathers telemetry from the following sources, which are also known as connectors. You can configure the connectors either by following the Initial Configuration of Cisco Group-Based Policy Analytics, on page 17 workflow, or by choosing **Policy** > **Group-Based Access Control** > **Analytics** > **Configurations** > **Analytics Settings**.

Group Data Connectors

The group data connectors collect information about groups that assets are classified into. Cisco ISE and Cisco Stealthwatch are group data connectors.

- **Cisco ISE**

  Cisco ISE is a next-generation identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. Cisco ISE is installed on a virtual machine, a physical machine or a combination of both. Cisco ISE uses the Cisco Platform Exchange Grid (pxGrid) service as the publisher-subscriber module for sharing SessionDirectory, Scalable Groups, and other information. PxGrid uses a query interface and supports bulk download. Users on the network are authenticated, authorized, and accounted for, and a session directory is maintained. User events are published to the connectors that are subscribed to the SessionDirectory service. Other services like scalable group notifications can also be subscribed to.

  User identity and device information obtained during authentication is used to classify the packets, as they enter the network. This packet classification is maintained by tagging packets when they enter the network so that they can be properly identified for applying security and other policy criteria along the data path. The tag, also called the Scalable Group Tag (SGT), allows Cisco ISE to enforce access control policies by enabling the network device to act upon the SGT to filter traffic.

  In addition, Cisco ISE collects information about endpoints connected to your network, such as the type of device, OS, OS version, IP address and other attributes. These are called ISE profiles.

  The Cisco ISE connector provides Cisco Group-Based Policy Analytics with SGT definitions and profiles from Cisco ISE.

- **Cisco Stealthwatch**

  Cisco Stealthwatch is a network-based anomaly detection system which provides advanced threat detection, accelerated threat response and network traffic security analysis. The Cisco Stealthwatch connector obtains the host groups that are configured on Cisco Stealthwatch. A host group is essentially a virtual container containing multiple host IP addresses or IP address ranges that have similar attributes, such as location, function, or topology.

Communication Connector

The communication connector helps gather information on traffic seen between groups, that could be leveraged in Group-Based Policy decisions. This is done using NetFlow from network devices managed by Cisco DNA Center. NetFlow is collected and aggregated natively by Cisco DNA Center.

Initial Configuration of Cisco Group-Based Policy Analytics

This workflow helps you configure the data connectors that are required to collect telemetry data related to network activity, and endpoints from specific sources such as Cisco ISE, Cisco Stealthwatch, and NetFlow. This task is useful when you are configuring the data connectors for the first time.

Before you begin

Cisco DNA Center must have Cisco Group-Based Policy Analytics installed.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Group-Based Access Control** > **Overview**.
The **Create policies with more confidence** window appears.

Step 2 Click **Get Started**.
The **Configure your data connectors** window appears.

Step 3 Click **Let’s Do It**.

The **Configure Group Data Connectors** window appears.

If the Cisco ISE version installed on Cisco DNA Center is earlier than the version required for running Cisco Group-Based Policy Analytics, an error message is displayed.

Step 4 Click **Configure** at the bottom of the connector that you want to configure.
A new window opens, redirecting you to the Cisco DNA Center **Settings** window, where you can configure the required connectors. You must configure the Cisco ISE connector. Configuring the Cisco Stealthwatch connector is optional.

Step 5 Close the **Settings** window. You will see a green dot next to the **Configure** option for the successfully configured connectors in the **Configure Group Data connectors** window.

Step 6 Click **Next**.

The **Configure Communication Connectors** window appears.

Step 7 Configure the communication connector (NetFlow) by using one of the following options:

- Provision NetFlow on the Cisco DNA Center device interface manually.
- Click **Template Editor** to configure NetFlow using the **Template Editor Tool** in Cisco DNA Center.
- Click **Telemetry in Network Settings** to configure NetFlow in the telemetry section of network settings.

Step 8 Click **Next**.
The **Summary** window displays the configuration details of the connectors.

Step 9 Click **Done** to start discovering your groups and endpoints.

Explore Groups and Endpoints

The following section provides information about the different ways to visualize traffic between different groups.

Multiple Groups to Multiple Groups

When you click the number that is displayed in the **Scalable Groups** box in the **Overview** window, the **Explore Scalable Groups** window is displayed. In this window, you can see a summary of all the group-to-group communication among Scalable Groups. By default, the time range for this view is the last available 24 hours of data. Note that this is different from the time range mentioned in the **Overview** window, where it is set to the last 14 days. The chart shows the top 25 source Scalable Groups and their corresponding interactions, starting with the source Scalable Group with the highest number of unique flows within the given time period and so on.

Click the icon to display the chart view, or ☰ to display the table view.

In the table view, if you click the **See destinations** link on a particular row, it opens a window showing all the destination Scalable Groups for the selected source Scalable Group, and the unique flow count for each destination Scalable Group.

Click a source group to view the **Single Group to Multiple Groups** window.

When you hover your cursor over a link, the link is highlighted and a tooltip shows the number of unique traffic flows. Clicking the link takes you to the **Single Group to Single Group** window.

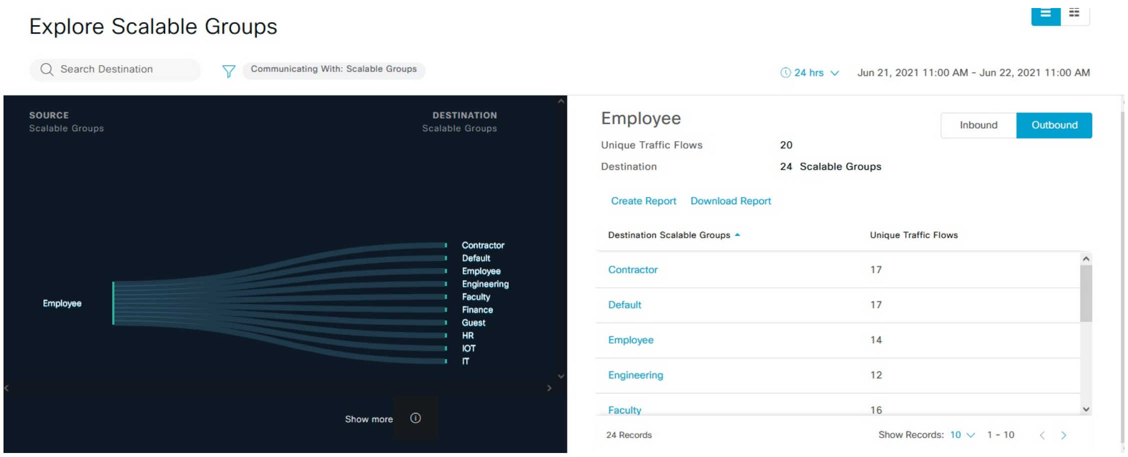
When you click the number displayed in the **ISE Profiles** box in the **Overview** window, the **Explore ISE Profiles** window is displayed. In this window, you can see a summary of all the communication from ISE Profiles as the source and Scalable Groups as the destination. In order to focus on group-based policy decisions, either the source or destination category must be Scalable Groups in this view.

When you click the number displayed in the **Stealthwatch Host Groups** box in the **Overview** window, the **Explore Stealthwatch Host Groups** window is displayed. In this window, you can see a summary of all the communication, with Stealthwatch Host Groups as the source and the Scalable Groups as the destination. In order to focus on group-based policy decisions, either the source or destination category must be Scalable Groups in this view.

Single Group to Multiple Groups

Single Group to Multiple Groups: Outbound

This window displays the activity between a single source group and multiple destination groups. The source or the destination or both must be a Scalable Group. By default, the time range for this view is the last available 24 hrs of data and the default number of links or records shown is 10.



Explore Scalable Groups

Search Destination

Communicating With: Scalable Groups

24 hrs Jun 21, 2021 11:00 AM - Jun 22, 2021 11:00 AM

Employee

Unique Traffic Flows 20

Destination 24 Scalable Groups

Create Report Download Report

Destination Scalable Groups	Unique Traffic Flows
Contractor	17
Default	17
Employee	14
Engineering	12
Faculty	16

24 Records Show Records: 10 1 - 10

Click the icon to display the chart view or to view the table view.

Outbound displays the connections initiated by the selected scalable group. **Inbound** displays the connections initiated by another group to this scalable group.

Click any column to sort in ascending or descending order.

Click a group to view the **Single Group to Single Group** window with the corresponding destination as the selected group. The source group does not change.

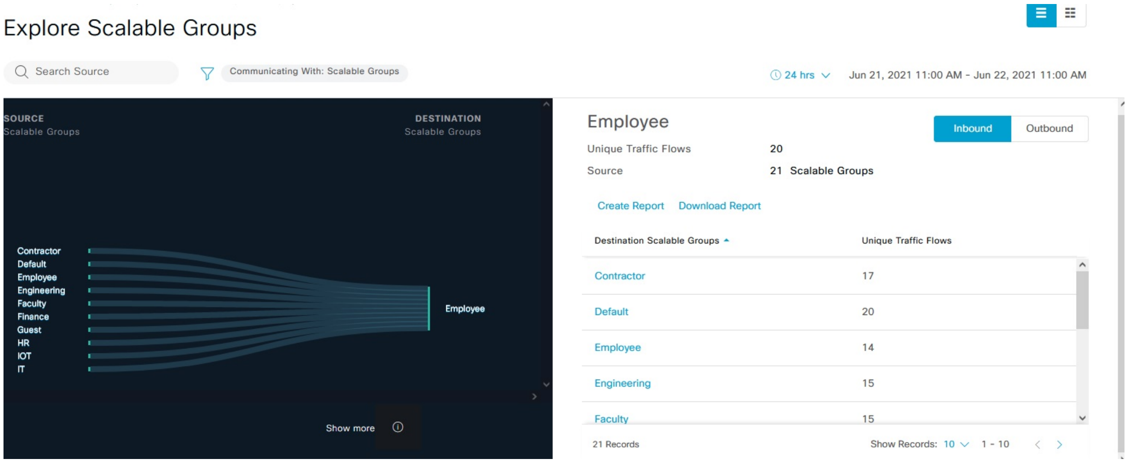
When you hover your cursor over a link, it is highlighted, and a tooltip shows the number of unique traffic flows. If you click this link, it takes you to the **Single Group to Single Group** window.

Click **Create Report** to generate a new report in CSV format with the information in this view. The **Reports** window opens, where you can see the generated report. This window also provides you access to previously generated reports and allows you to download the reports.

Click **Download Report** to view the generated reports. The **Reports** window opens, where you can click the *download* icon under the **Last Run** column to download a report.

Single Group to Multiple Groups: Inbound

If you click **Inbound**, it shows all the connections initiated by any group as the source and the selected Scalable Group as destination.


Explore Scalable Groups

Search Source | Communicating With: Scalable Groups | 24 hrs | Jun 21, 2021 11:00 AM - Jun 22, 2021 11:00 AM

Employee

Inbound | Outbound

Unique Traffic Flows 20

Source 21 Scalable Groups

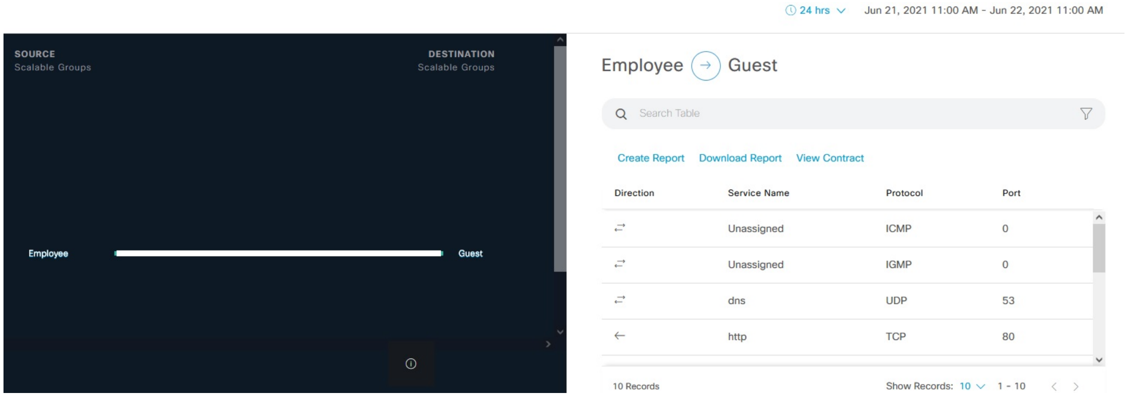
Create Report Download Report

Destination Scalable Groups	Unique Traffic Flows
Contractor	17
Default	20
Employee	14
Engineering	15
Faculty	15

21 Records Show Records: 10 1 - 10

Single Group to Single Group

This window shows the activity between a single source group and a single destination group. The source group or the destination group or both must be a scalable group. By default, the time range for this visual is the last available 24 hours of data and the default number of links or records shown is 10.


24 hrs Jun 21, 2021 11:00 AM - Jun 22, 2021 11:00 AM

Employee → Guest

Search Table

Create Report Download Report View Contract

Direction	Service Name	Protocol	Port
⇄	Unassigned	ICMP	0
⇄	Unassigned	IGMP	0
⇄	dns	UDP	53
←	http	TCP	80

10 Records Show Records: 10 1 - 10

When you hover your cursor over a link, it is highlighted and a tooltip shows the number of unique traffic flows.

When you click the directional arrow displayed between the source and destination groups, the source and destination groups are interchanged in this view.

Click **Create Report** to generate a new report in CSV format with the information in this view. The **Reports** window opens, where you can see the generated report. This window also provides you access to previously generated reports and allows you to download the reports.

Click **Download Report** to view the generated reports. The **Reports** window opens, where you can click the *download* icon under the **Last Run** column to download a report.

The left pane in the **View Contract** window displays the rules for permitted and denied traffic between the source and destination groups. You can view the traffic flows that match any selected rule in the right pane. You can also view the ports and protocols used for the traffic flows. For more information about contracts, see Access Contracts.

Click the icon to display the chart view or ☰ to display the table view.

You can set the date and time using the Date and Time Selector.

Access Contracts

Access Contracts can now be created and modified directly in the Analytics workflow.

View Contract

To launch the **View Contract** window, from the **Explore Scalable Groups** window, click **View Contract**. The left pane in the **View Contract** window displays the rules for permitted and denied traffic between the source and destination groups. You can view the traffic flows that match any selected rule in the right pane.

This table can also be accessed from the **Policies** window. In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Group-Based Access Control** > **Policies**.

From the policy matrix view, click the cell for which you want to create or modify contracts. In the **Policy Details** slide-in pane, click **View Traffic Flows**.

If there is currently no contract assigned between the source and destination groups, no data is displayed. You can use the **Change Contract** or **Create Access Contract** option to create or modify the contract.

Click **View traffic** in the **Action** column to see the list of flows that match that rule.

Create Access Contract

To launch the **Contract Content** window, from the **Policy Details** pane, click **Create Access Contract**. To create the traffic filter rules:

1. From the **Action** drop-down list, choose **Deny** or **Permit**.
2. From the **Application** drop-down list, choose the application for which you want to apply that action. The port and protocol are automatically selected based on the application that you select.

   If you want to specify the transport protocol, source port, and destination port, choose the **Advanced** option in the **Application** drop-down list.

You can create multiple rules. To create multiple rules for a contract, click the Plus icon and choose the settings for the **Action** and **Application** columns. The rules are checked in the order in which they are listed in the contract. Use the Handle icon at the left end of a rule to drag and change the order of the rule.

You can use the **Add to Contract** option within the **All Unique Traffic Flows** pane to add an entry to the contract.

While saving a newly created or edited contract, you have the following options:

- **Update current policy only**: A duplicate of the contract is created and applied to the current policy. Other policies that reference this contract are not affected.
- **Update contract for all referenced policies**: The contract is updated and applied to the current policy and other policies that reference this contract.
- **Create a new contract with no policies affected**: A duplicate of the contract is created but not applied to any policy.

Change Contract

To launch the **Change Contract** window, from the **Policy Details** pane, click **Change Contract**. All available contracts are displayed. You can select the required contract and click **Change** to add that contract to the policy.

Edit Contract

The **Edit** option is displayed only when a contract has already been added to the policy. If you want to edit the contract details, click **Edit** displayed after the name of the contract.

After updating the contract, click **Save**. The following options are available:

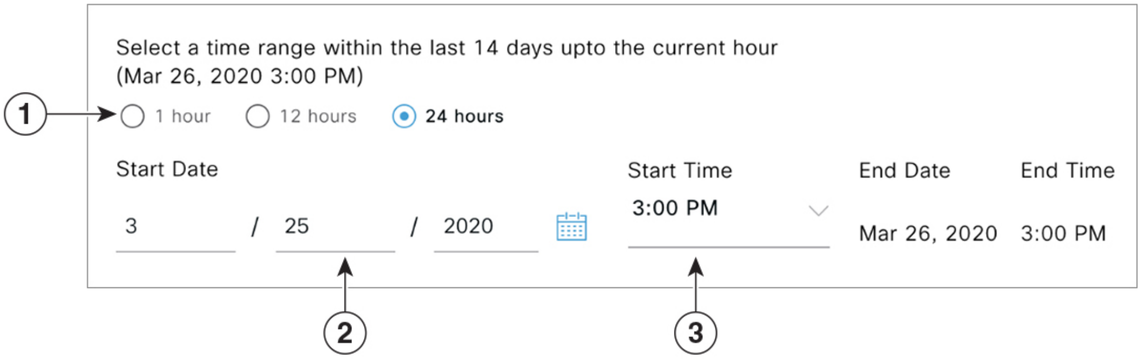
- **Update current policy only**: A duplicate of the contract is created and applied to the current policy. Other policies that reference this contract are not affected.
- **Update contract for all referenced policies**: The contract is updated and applied to the current policy and other policies that reference this contract.
- **Create a new contract with no policies affected**: A duplicate of the contract is created but not applied to any policy.

After choosing the appropriate option, enter a name and description (if you select the first or third option), and then click **Confirm**.

Date and Time Selector

You can select the time period for which you want to see the connection summary. You can select a time range within the last 14 days up to the current hour.

Figure 3: Date and Time Selector



Select a time range within the last 14 days upto the current hour
(Mar 26, 2020 3:00 PM)

○ 1 hour ○ 12 hours ● 24 hours

Start Date: 3 / 25 / 2020

Start Time: 3:00 PM

End Date: Mar 26, 2020

End Time: 3:00 PM

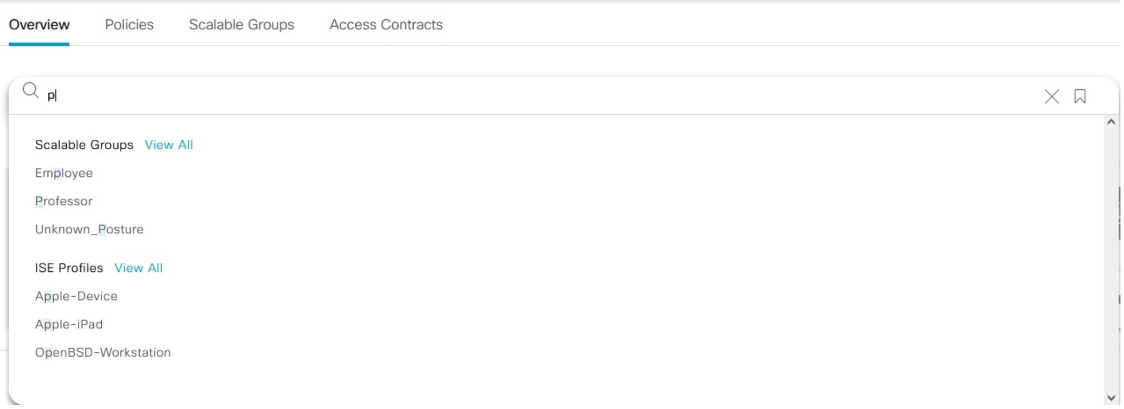
1. Select one of the options. The **End Time** will be adjusted automatically.
2. Specify the **Start Date** by entering the month, day, and year manually or by using the calendar icon.
3. Choose the **Start Time** from the drop-down menu.

Use Search

The **Overview** window has a **Search** field that can search across the data for scalable groups, ISE profiles, Stealthwatch host groups, IP addresses, or MAC addresses.

As you start entering the characters in the search field, an automatic search is performed for scalable groups, ISE profiles, and Stealthwatch host groups, and up to three results are displayed for each group type. For IP addresses, the relevant characters are whole numbers and period. For MAC addresses, the relevant characters are hexadecimal and colon.

Figure 4: Search Window



Note

- The **Search Results** window does not open until you click the **View All** link.
- A read-only user cannot search for an IP address or a MAC address. See Role-Based Access Control for more information.

From the **Focus** drop-down list, choose the required option to change your search criteria.

The filter icon (▽) is used in advanced filtering, and is available only when you search for a MAC address or an IP address. When you click the ▽ icon, each column is provided with a search field on top of the column name.

For each column, you can enter up to three search criteria. When entering more than one criterion per column, you can specify an OR operation or an AND operation. The resultant query performs an AND operation across the columns.

Click the 🔖 icon and use the **Save Current Search** option to save the current displayed search.

To delete a saved search, click the 🔖 icon. Hover your cursor over the name of the saved search and click the ✕ icon. Click **Yes** in the **Delete Saved Filter** dialog box to permanently delete the filter.

Role-Based Access Control

Cisco Group-Based Policy Analytics supports Role-Based Access Control. It differentiates between a read-write user and a read-only user. However, because Cisco Group-Based Policy Analytics is primarily based on visibility, which does not make any changes to the system, there are only a few limitations for a read-only user:

- A read-only user cannot save search queries.
- A read-only user cannot makes changes in the Initial Configuration of Cisco Group-Based Policy Analytics, on page 17 window.
- A read-only user cannot export data because exporting data is an HTTPS POST operation.
- A read-only user can only perform search by group and is restricted from other search functions as they involve HTTPS POST operations.

IP-Based Access Control Policies

An IP-based access control policy controls the traffic going into and coming out of a Cisco device in the same way that an Access Control List (ACL) does. As with an ACL, an IP-based access control policy contains lists of permit and deny conditions that are applied to traffic flows based on various criteria, including protocol type, source IP address, destination IP address, or destination port number.

IP-based access control policies can be used to filter traffic for various purposes, including security, monitoring, route selection, and network address translation.

An IP-based access control policy has two main components:

- **IP Network Groups**: IP network groups comprise IP subnets that share the same access control requirements. These groups can be defined only in Cisco DNA Center. An IP network group may have as few as one IP subnet in it.
- **Access Contract**: An access contract is a common building block that is used in both IP-based and group-based access control policies. It defines the rules that make up the access control policies. These rules specify the actions (permit or deny) performed when traffic matches a specific port or protocol and the implicit actions (permit or deny) performed when no other rules match.

Workflow to Configure an IP-Based Access Control Policy

Before you begin

- Cisco ISE is not mandatory if you are adding groups within the **Policy** > **IP Based Access Control** > **IP Network Groups** window while creating a new IP-based access control policy.
- Make sure that you have defined the following global network settings and provision the device:
    - Network servers, such as AAA, DHCP, and DNS servers: See Configure Global Network Servers.
    - Device credentials, such as CLI, SNMP, HTTP, and HTTPS: See About Global Device Credentials.
    - IP address pools: See Configure IP Address Pools.

- Wireless settings as SSIDs, wireless interfaces, and wireless radio frequency profiles: See Configure Global Wireless Settings.
- Provision devices: See Provisioning.

Step 1 Create IP network groups.

For more information, see Create an IP Network Group, on page 26.

Step 2 Create an IP-based access control contract.

An IP-based access control contract defines a set of rules between the source and destination. These rules dictate the action (allow or deny) that network devices perform based on the traffic that matches the specified protocols or ports. For more information, see Create an IP-Based Access Control Contract, on page 26.

Step 3 Create an IP-based access control policy. The access control policy defines the access control contract that governs traffic between the source and destination IP network groups.

For more information, see Create an IP-Based Access Control Policy, on page 27.

Configure Global Network Servers

You can define global network servers that become the default for your entire network.

Note You can override global network settings on a site by defining site-specific settings.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Design** > **Network Settings** > **Network**.

Step 2 In the **DHCP Server** field, enter the IP address of a DHCP server.

Note You can click the plus icon and enter both IPv4 and IPv6 addresses.

You must define at least one DHCP server in order to create IP address pools.

Step 3 In the **DNS Server** field, enter the domain name of a DNS server.

Note You can click the plus icon and enter both IPv4 and IPv6 addresses.

You must define at least one DNS server in order to create IP address pools.

Step 4 Click **Save**.

Create an IP Network Group

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **IP Based Access Control** > **IP Network Groups**.

Step 2 Click **Add Groups**.

Step 3 In the **Name** field, enter a name for the IP network group.

Step 4 In the **Description** field, enter a word or phrase that describes the IP network group.

Step 5 In the **IP Address or IP/CIDR** field, enter the IP addresses that make up the IP network group.

Step 6 Click **Save**.

Edit or Delete an IP Network Group

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **IP Based Access Control** > **IP Network Groups**.

Step 2 In the **IP Network Groups** table, check the check box next to the group that you want to edit or delete.

Step 3 Do one of the following tasks:

- To make changes to the group, click **Edit**. For field definitions, see Create an IP Network Group, on page 26. Make the desired changes and click **Save**.
- To delete the group, click **Delete** and then click **Yes** to confirm.

Create an IP-Based Access Control Contract

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **IP Based Access Control** > **Access Contract**.

Step 2 Click **Add Contract**.

Step 3 Enter a name and description for the contract.

Step 4 From the **Implicit Action** drop-down list, choose either **Deny** or **Permit**.

Step 5 From the **Action** drop-down list in the table, choose either **Deny** or **Permit**.

Step 6 From the **Port/Protocol** drop-down list, choose a port or protocol.

a) If Cisco DNA Center does not have the port or protocol that you need, click **Add Port/Protocol** to create your own.

b) In the **Name** field, enter a name for the port or protocol.

c) From the **Protocol** drop-down list, choose **UDP**, **TDP**, or **TCP/UDP**.

d) In the **Port Range** field, enter the port range.

e) If you want Cisco DNA Center to configure the port or protocol as defined, and not report any conflicts, check the **Ignore Conflict** check box.

f) Click **Save**.

Step 7 (Optional) To include more rules in your contract, click **Add** and repeat Step 5 and Step 6.

Step 8 Click **Save**.

Edit or Delete an IP-Based Access Control Contract

If you edit a contract that is used in a policy, the policy's state changes to **MODIFIED** in the **IP Based Access Control Policies** window. A modified policy is considered to be stale because it is inconsistent with the policy that is deployed in the network. To resolve this situation, you need to redeploy the policy to the network.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **IP Based Access Control** > **Access Contract**.

Step 2 Check the check box next to the contract that you want to edit or delete and do one of the following tasks:

- To make changes to the contract, click **Edit**, make the changes, and, click **Save**. For field definitions, see Create an IP-Based Access Control Contract, on page 26.

  Note If you make changes to a contract that is used in a policy, you need to deploy the modified policy by choosing **Policy** > **IP Based Access Control** > **IP Based Access Control Policies**, checking the check box next to the policy name, and clicking **Deploy**.

- To delete the contract, click **Delete**.

Create an IP-Based Access Control Policy

Create an IP-based access control policy to limit traffic between IP network groups.

- Multiple rules can be added to a single policy with different configurations.
- For a given combination of IP groups and contract classifiers, rules are created and pushed to the devices. This count cannot exceed 64 rules as Cisco WLC limits an ACL to have a maximum of 64 rules.
- If a custom contract or the IP group that is used in a **Deployed** policy is modified, the policy is flagged with status as **Modified**, indicating that it is Stale and requires a redeployment for the new configurations to be pushed to the device.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **IP Based Access Control** > **IP Based Access Control Policies**.

Step 2 Click **Add Policy**.

Step 3 Complete the following fields:

Field	Description
Policy Name	Name of the policy.
Description	Word or phrase that identifies the policy.

Field	Description
SSID	Lists FlexConnect SSIDs and non-FlexConnect SSIDs that were created during the design of SSIDs. If the selected SSID is configured in a FlexConnect mode, then the access policy is configured in FlexConnect mode. Otherwise, it will be configured in a regular way. **Note** If an SSID is part of one policy, that SSID will not be available for another policy. A valid site-SSID combination is required for policy deployment. You will not be able to deploy a policy if the selected SSID is not provisioned under any devices.
Site Scope	Sites to which a policy is applied. If you configure a wired policy, the policy is applied to all wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices with the SSID defined in the scope. For more information, see Site Scope, on page 31.
Source	Origin of the traffic that is affected by the contract. From the **Source** drop-down list, choose an IP network group. If the IP network that you want is not available, click **+Group** to create one.
Contract	Rules that govern the network interaction between the source and destination in an ACL. Click **Add Contract** to define the contract for the policy. In the dialog box, click the radio button next to the contract that you want to use. Alternatively, you can select the permit (permit all traffic) or deny (deny all traffic) contract.
Destination	Target of the traffic that is affected by the contract. Click the **Destination** drop-down list, choose an IP network group. If the IP network that you want is not available, click **+Create IP Network Group** to create one.
Direction	Configures the relationship of the traffic flow between the source and destination. To enable the contract for traffic flowing from the source to the destination, select **One-Way**. To enable the contract for traffic flowing in both directions (from the source to the destination and from the destination to the source), select **Bi-directional**.

Step 4 (Optional) To create an IP network group, click **Create IP Network Group**.

Step 5 (Optional) To add another rule, click the plus sign.

Note To delete a rule, click **x**.

Step 6 (Optional) To reorder the sequence of the rules, drag and drop a rule in the order you want.

Step 7 Click **Deploy**.

The success message `IP-Based Access Control Policy has been created and deployed successfully` is displayed. Depending on the SSID selected, either a FlexConnect policy or a standard policy is created with different levels of mapping information and deployed. The **Status** of the policy is shown as **DEPLOYED**. A wireless icon next to the **Policy Name** shows that the deployed access policy is a wireless policy.

Edit or Delete an IP-Based Access Control Policy

If you need to, you can change or delete an IP-based access control policy.

Note If you edit a policy, the policy's state changes to **MODIFIED** on the **IP Based Access Control Policies** window. A modified policy is considered to be stale because it is inconsistent with the policy that was deployed in the network. To resolve this situation, you need to redeploy the policy to the network.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **IP Based Access Control** > **IP Based Access Control Policies**.

Step 2 Check the check box next to the policy that you want to edit or delete and do one of the following tasks:

- To make changes, click **Edit**. When you are done, click **Save**. For field definitions, see Create an IP-Based Access Control Policy, on page 27.
- To delete the policy, click **Delete**.

Step 3 If you make changes to the policy, deploy the modified policy by checking the check box next to the policy name and clicking **Deploy**.

Deploy an IP-Based Access Control Policy

If you make changes that affect a policy's configuration, you need to redeploy the policy to implement these changes.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **IP Based Access Control** > **IP Based Access Control Policies**.

Step 2 Locate the policy that you want to deploy.

Step 3 Check the check box next to the policy.

Step 4 Click **Deploy**.
You are prompted to deploy your policy immediately or to schedule it for a later time.

Step 5 Do one of the following:

- To deploy the policy immediately, click the **Run Now** radio button and click **Apply**.
- To schedule the policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment.

  Note The site time zone setting is not supported for scheduling application policy deployments.

Application Policies

Quality of Service (QoS) refers to the ability of a network to provide preferential or deferential service to selected network traffic. By configuring QoS, you can ensure that network traffic is handled in such a way that makes the most efficient use of network resources while still adhering to the objectives of the business, such as guaranteeing that voice quality meets enterprise standards, or ensuring a high Quality of Experience (QoE) for video.

You can configure QoS in your network using application policies in Cisco DNA Center. Application policies comprise these basic parameters:

- **Application Sets**: Sets of applications with similar network traffic needs. Each application set is assigned a business relevance group (business relevant, default, or business irrelevant) that defines the priority of its traffic. QoS parameters in each of the three groups are defined based on Cisco Validated Design (CVD). You can modify some of these parameters to more closely align with your objectives.
- **Site Scope**: Sites to which an application policy is applied. If you configure a wired policy, the policy is applied to all the wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices with the SSID defined in the scope.

Cisco DNA Center takes all of these parameters and translates them into the proper device CLI commands. When you deploy the policy, Cisco DNA Center configures these commands on the devices defined in the site scope.

Note Cisco DNA Center configures QoS policies on devices based on the QoS feature set available on the device. For more information about a device’s QoS implementation, see the corresponding device's product documentation.

CVD-Based Settings in Application Policies

The default QoS trust and queuing settings in application policies are based on the Cisco Validated Design (CVD) for Enterprise Medianet Quality of Service Design. CVDs provide the foundation for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Each one has been comprehensively tested and documented by Cisco engineers to ensure faster, more reliable, and fully predictable deployment.

The latest validated designs relating to QoS are published in the Cisco Press book, *End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks*, 2nd Edition, available at: http://www.ciscopress.com/store/end-to-end-qos-network-design-quality-of-service-for-9781587143694. For additional information, see the following Cisco documentation:

- Cisco Validated Designs
- Enterprise Medianet Quality of Service Design 4.0
- Medianet Campus QoS Design 4.0
- Medianet WAN Aggregation QoS Design 4.0

Site Scope

A site scope defines the sites to which an application policy is applied. When defining a policy, you configure whether a policy is for wired or wireless devices. You also configure a site scope. If you configure a wired policy, the policy is applied to all the wired devices in the site scope. Likewise, if you configure a wireless policy for a selected service set identifier (SSID), the policy is applied to all of the wireless devices in the site scope with the SSID defined in the scope.

This allows you to make tradeoffs as necessary to compensate for differences in the behaviors between wired and wireless network segments. For example, wireless networks typically have lower bandwidth, lower speed, and increased packet loss in comparison to wired networks. Individual wireless segments may exhibit further variation due to local conditions of RF interference, congestion, and other factors, such as the varying capabilities of network devices. The ability to apply per-segment policies to individual wireless segments enables the adjustment of traffic-handling rules to ensure that the highest-priority traffic is least affected by degradation of the wireless network.

Business-Relevance Groups

A business-relevance group classifies a given application set according to how relevant it is to your business and operations.

Business-relevance groups are Business Relevant, Default, and Business Irrelevant, and they essentially map to three types of traffic: high priority, neutral, and low priority.

- **Business Relevant**: (High-priority traffic) The applications in this group directly contribute to organizational objectives, and as such, may include a variety of applications, including voice, video, streaming, and collaborative multimedia applications, database applications, enterprise resource applications, email, file transfers, content distribution, and so on. Applications designated as business relevant are treated according to industry best-practice recommendations, as prescribed in Internet Engineering Task Force (IETF) RFC 4594.

- **Default**: (Neutral traffic) This group is intended for applications that may or may not be business relevant, for example, generic HTTP or HTTPS traffic may contribute to organizational objectives at times, while at other times, such traffic may not. You may not have insight into the purpose of some applications, for instance, legacy applications or even newly deployed applications. Therefore, the traffic flows for these applications should be treated with the Default Forwarding service, as described in IETF RFC 2747 and 4594.

- **Business Irrelevant**: (Low-priority traffic) This group is intended for applications that have been identified as having no contribution towards achieving organizational objectives. They are primarily consumer-oriented or entertainment-oriented or both in nature. We recommend that this type of traffic be treated as a *Scavenger* service, as described in IETF RFCs 3662 and 4594.

Applications are grouped into application sets and sorted into business-relevance groups. You can include an application set in a policy as-is, or you can modify it to meet the needs of your business objectives and your network configuration.

For example, YouTube is member of the consumer-media application set, which is business-irrelevant (by default), because most customers typically classify this application this way. However, this classification may not be the true for all companies, for example, some businesses may be using YouTube for training purposes. In such cases, an administrator can move the YouTube application into the streaming-video application set, which is business relevant by default.

Consumers and Producers

You can configure relationships between applications such that when traffic from one application is sent to another application (thus creating a specific a-to-b traffic flow), the traffic is handled in a specific way. The applications in this relationship are called producers and consumers, and are defined as follows:

- **Producer**: Sender of the application traffic. For example, in a client/server architecture, the application server is considered the producer because the traffic primarily flows in the server-to-client direction. In the case of a peer-to-peer application, the remote peer is considered the producer.
- **Consumer**: Receiver of the application traffic. The consumer may be a client end point in a client/server architecture or it may be the local device in a peer-to-peer application. Consumers may be end-point devices, but may, at times, be specific users of such devices (typically identified by IP addresses or specific subnets). There may also be times when an application is the consumer of another application's traffic flows.

Setting up this relationship allows you to configure specific service levels for traffic matching this scenario.

Marking, Queuing, and Dropping Treatments

Cisco DNA Center bases its marking, queuing, and dropping treatments on IETF RFC 4594 and the business relevance category that you have assigned to the application. Cisco DNA Center assigns all of the applications in the Default category to the Default Forwarding application class and all of the applications in the Irrelevant Business category to the Scavenger application class. For applications in the Relevant Business category, Cisco DNA Center assigns traffic classes to applications based on the type of application. The following table lists the application classes and their treatments.

Table 3: Marking, Queuing, and Dropping Treatments

Business Relevance	Application Class	Per-Hop Behavior	Queuing and Dropping	Application Description
Relevant	VoIP[1]	Expedited Forwarding (EF)	Priority Queuing (PQ)	VoIP telephony (bearer-only) traffic; for example, Cisco IP phones.
	Broadcast Video	Class Selector (CS) 5	PQ	Broadcast TV, live events, video surveillance flows, and similar inelastic streaming media flows; for example, Cisco IP Video Surveillance and Cisco Enterprise TV. (Inelastic flows refer to flows that are highly drop sensitive and have no retransmission or flow-control capabilities or both.)
	Real-time Interactive	CS4	PQ	Inelastic high-definition interactive video applications and audio and video components of these applications; for example, Cisco TelePresence.
	Multimedia Conferencing	Assured Forwarding (AF) 41	Bandwidth (BW) Queue and Differentiated Services Code Point (DSCP) Weighted Random Early Detect (WRED)	Desktop software multimedia collaboration applications and audio and video components of these applications; for example, Cisco Jabber and Cisco WebEx.
	Multimedia Streaming	AF31	BW Queue and DSCP WRED	Video-on-Demand (VoD) streaming video flows and desktop virtualization applications,such as Cisco Digital Media System.
	Network Control	CS6	BW Queue only[2]	Network control-plane traffic, which is required for reliable operation of the enterprise network, such as EIGRP, OSPF, BGP, HSRP, IKE, and so on.
	Signaling	CS3	BW Queue and DSCP	Control-plane traffic for the IP voice and video telephony infrastructure.
	Operations, Administration, and Management (OAM)	CS2	BW Queue and DSCP[3]	Network operations, administration, and management traffic, such as SSH, SNMP, syslog, and so on.
	Transactional Data (Low-Latency Data)	AF21	BW Queue and DSCP WRED	Interactive (foreground) data applications, such as enterprise resource planning (ERP), customer relationship management (CRM), and other database applications.
	Bulk Data (High-Throughput Data)	AF11	BW Queue and DSCP WRED	Noninteractive (background) data applications, such as email, file transfer protocol (FTP), and backup applications.

Business Relevance	Application Class	Per-Hop Behavior	Queuing and Dropping	Application Description
Default	Default Forwarding (Best Effort)	DF	Default Queue and RED	Default applications and applications assigned to the default business-relevant group. Because only a small number of applications are assigned to priority, guaranteed bandwidth, or even to differential service classes, the vast majority of applications continue to default to this best-effort service.
Irrelevant	Scavenger	CS1	Minimum BW Queue (Deferential) and DSCP	Nonbusiness related traffic flows and applications assigned to the business-irrelevant group, such as data or media applications that are entertainment-oriented. Examples include YouTube, Netflix, iTunes, and Xbox Live.

[1] VoIP signaling traffic is assigned to the Call Signaling class.
[2] WRED is not be enabled on this class because network control traffic should not be dropped.
[3] WRED is not enabled on this class because OAM traffic should not be dropped.

Service Provider Profiles

Service provider (SP) profiles define the class of service for a particular WAN provider. You can define 4-class, 5-class, 6-class, and 8-class models.

When application policies are deployed on the devices, each SP profile is assigned a certain service-level agreement (SLA) that maps each SP class to a DSCP value and a percentage of bandwidth allocation.

You can customize the DSCP values and the percentage of bandwidth allocation in a SP profile when configuring an application policy.

After you create the SP profile, you need to configure it on the WAN interfaces.

Table 4: Default SLA Attributes for SP Profiles with 4 Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Voice	EF	Yes	10	—
Class 1 Data	AF31	—	—	44
Class 2 Data	AF21	—	—	25
Default	0	—	—	31

Table 5: Default SLA Attributes for SP Profiles with 5 Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Voice	EF	Yes	10	—
Class 1 Data	AF31	—	—	44
Class 2 Data	AF21	—	—	25
Class 3 Data	AF11	—	—	1
Default	Best Effort	—	—	30

Table 6: Default SLA Attributes for SP Profiles with 6 Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Class 1 Data	AF31	—	—	10
Class 3 Data	AF11	—	—	1
Video	AF41	—	—	34
Voice	EF	Yes	10	—
Default	0	—	—	30
Class 2 Data	AF21	—	—	25

Table 7: Default SLA Attributes for SP Profiles with 8 Classes

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Network-Control Management	CS6	—	—	5
Streaming Video	AF31	—	—	10
Call Signalling	CS3	—	—	4
Scavenger	CS1	—	—	1
Interactive Video	AF41	—	—	30
Voice	EF	Yes	10	—

Class Name	DSCP	Priority Class	SLA	
			Bandwidth (%)	Remaining Bandwidth (%)
Default	0	—	—	25
Critical Data	AF21	—	—	25

Queuing Profiles

Queuing profiles allow you to define an interface's bandwidth allocation based on the interface speed and the traffic class.

Note Queuing profiles do not apply to WAN-facing interfaces that are connected to a service provider profile.

The following interface speeds are supported:

- 100 Gbps
- 10/40 Gbps
- 1 Gbps
- 100 Mbps
- 10 Mbps
- 1 Mbps

If the speed of an interface falls between two interface speeds, Cisco DNA Center treats the interface at the lower interface speed.

Note Cisco DNA Center attempts to detect the operational speed of the interface in order to apply the correct policy. However, if a switch port is administratively down, Cisco DNA Center cannot detect the speed. In this case, Cisco DNA Center uses the interface's supported speed.

You define a queuing policy as part of an application policy. When you deploy the application policy, the devices in the sites that are selected in the site scope are configured with the assigned LAN queuing policy. If no LAN queuing policy is assigned, the application policy uses the default CVD queuing policy.

If you change the queuing policy in an application policy that has already been deployed, the policy becomes stale, and you need to redeploy the policy for the changes to be configured on the devices.

Note the following additional guidelines and limitations of queuing policies:

- You cannot delete a LAN queuing profile if it is used in a policy.
- If you update a queuing profile that is associated with a policy, the policy is marked as stale. You need to redeploy the policy to provision the latest changes.

- Traffic class queuing customization does not affect interfaces on Cisco service provider switches and routers. You should continue to configure these interfaces without using Cisco DNA Center.

Table 8: Default CVD LAN Queuing Policy

Traffic Class	Default Bandwidth (Total = 100%)[4]
Business Relevant Voice	10%
Business Relevant Broadcast Video	10%
Business Relevant Real-Time Interactive	13%
Business Relevant Multimedia Conferencing	10%
Business Relevant Multimedia Streaming	10%
Business Relevant Network control	3%
Business Relevant Signaling	2%
Business Relevant OAM	2%
Business Relevant Transactional Data	10%
Business Relevant Bulk Data	4%
Business Relevant Scavenger	1%
Business Relevant Best Effort	25%

[4] We recommend that the total bandwidth for Voice, Broadcast Video, and Real-Time Interactive traffic classes equals no more than 33%.

Processing Order for Devices with Limited Resources

Some network devices have a limited memory (called TCAM) for storing network ACLs and access control entries (ACEs). So, because ACLs and ACEs for applications are configured on these devices, the available TCAM space is used. When the TCAM space is depleted, QoS settings for additional applications cannot be configured on that device.

To ensure that QoS policies for the most important applications get configured on these devices, Cisco DNA Center allocates TCAM space in the following order:

1. **Rank**: Number assigned to custom and favorite applications, but not to existing, default NBAR applications. The lower the rank number, the higher the priority. For example, an application with rank 1 has a higher priority than an application with rank 2, and so on. Having no rank is the lowest priority.

Note

- Custom applications are assigned rank 1 by default.
- If we mark the NBAR application as favorite, the rank is set to 1000.

2. **Traffic Class**: Priority based on the following order: Signaling, Bulk Data, Network Control, Operations Administration Management (Ops Admin Mgmt), Transactional Data, Scavenger, Multimedia Streaming, Multimedia Conferencing, Real Time Interactive, Broadcast Video, and VoIP Telephony.
3. **Popularity**: Number (1–10) that is based on CVD criteria. The popularity number cannot be changed. An application with a popularity of 10 has a higher priority than an application with a popularity of 9, and so on.

Note

- Custom applications are assigned popularity 0.
- Default NBAR applications are assigned a popularity number (1–10) that is based on CVD criteria. When you mark an application as a favorite, this does not change the popularity number; only the rank is changed.

4. **Alphabetization**: If two or more applications have the same rank and popularity number, they are sorted alphabetically by the application's name, and assigned a priority accordingly.

For example, let us assume that you define a policy that has the following applications:

- Custom application, custom_realtime, which has been assigned rank 1 and popularity 10 by default.
- Custom application, custom_salesforce, which has been assigned rank 1 and popularity 10 by default.
- Application named corba-iiop, which is in the transactional data traffic class, and you have designated as a favorite, giving that application a ranking of 10,000 and popularity of 9 (based on CVD).
- Application named gss-http, which is in the Ops Admin Mgmt traffic class, and you have designated as a favorite, giving that application a ranking of 10,000 and popularity of 10 (based on CVD).
- All other, default NBAR applications, which have no rank, but will be processed according to their traffic class and default popularity (based on CVD).

According to the prioritization rules, the applications are configured on the device in this order:

Application Configuration Order	Reason
1. Custom application, custom_realtime	Custom applications are given highest priority. Given that the custom_salesforce and custom_realtime applications have the same rank and popularity, they are sorted alphabetically, custom_realtime before custom_salesforce.
2. Custom application, custom_salesforce	
3. Favorite application, gss-http	Because both of these applications have been designated as favorites, they have the same application ranking. So, Cisco DNA Center evaluates them according to their traffic class. Because gss-http is in the Ops Admin Mgmt traffic class, it is processed first, followed by the corba-iiop application, which is in the Trasactional Data traffic class. Their popularity does not come into play because the processing order has been determined by their traffic class.
4. Favorite application, corba-iiop	

Application Configuration Order	Reason
5. All other, default NBAR applications	All other applications are next and are prioritized according to traffic class and then popularity, with the applications having the same popularity being alphabetized according to the application's name.

Policy Drafts

When you create a policy, you can save it as a draft without having to deploy it. Saving it as a draft allows you to open the policy later and make changes to it. You can also make changes to a deployed policy, and save it as a draft.

Note After you save or deploy a policy, you cannot change its name.

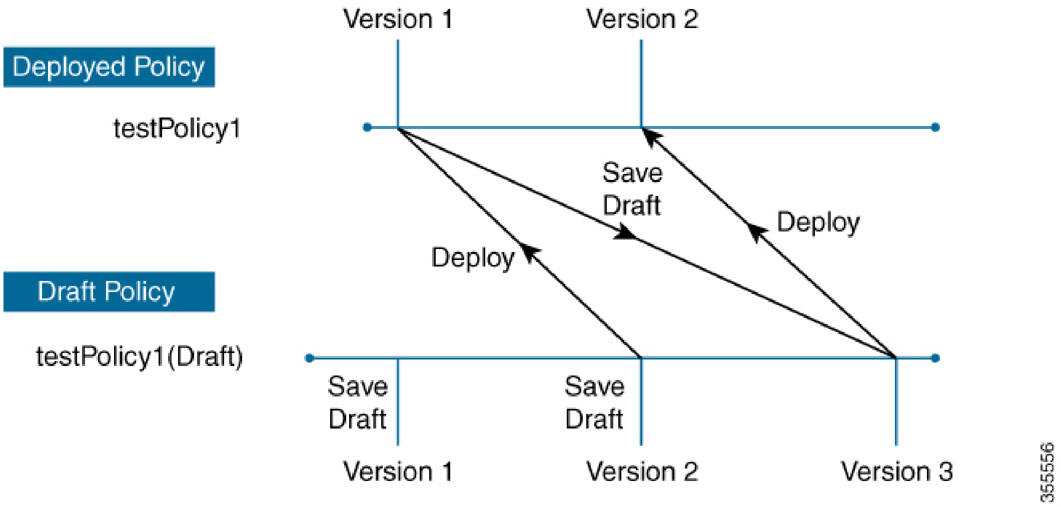
Draft policies and deployed policies are related to one another, but they have their own versioning.

When you save a policy as a draft, Cisco DNA Center appends the policy name with (Draft), and increments the version number. When you deploy a policy, Cisco DNA Center increments the version number of the deployed policy.

For example, as shown in the following figure, you create a policy named testPolicy1 and save it as a draft. The policy is saved as testPolicy1 (Draft), version number 1. You make a change to the draft and save it again. The policy has the same name, testPolicy1 (Draft), but its version number is incremented to 2.

You decide you like the policy, and you deploy it to the network. The policy is deployed with the name testPolicy1 and its version number is 1. You make a change to the deployed policy and save it as a draft. The draft policy, testPolicy1 (Draft), is incremented to version number 3. When you ultimately deploy that version, testPolicy1 is incremented to version 2.

Figure 5: Deployed Policy and Draft Policy Versioning



Any time you modify and save either a draft policy or a deployed policy, the draft policy version number is incremented. Similarly, any time you deploy either a draft policy or a modified deployed policy, the deployed policy version is incremented.

Just as with deployed policies, you can display the history of draft policies and roll them back to previous versions.

For more information about viewing the history of policy versions and rolling back to a previous version, see Policy Versioning, on page 40.

Policy Preview

Before you deploy a policy, you can generate the CLI that will be applied to a device.

The Preview operation generates the CLI commands for a policy, compares them with the CLI commands in the running configuration on the device, and returns only the remaining CLI commands that are required to configure the policy on the device.

After reviewing the preview output, you can deploy the policy to all of the devices in the scope, or you can continue to make changes to the policy.

Policy Precheck

When you create an application policy, you can verify if it will be supported on the devices in the site scope before you deploy it. The precheck function verifies if the device type, model, line cards, and software images support the application policy that you created. If any of these components are not supported, Cisco DNA Center reports a failure for the device. Cisco DNA Center also provides possible ways to correct the failures. If these remedies do not fix the failure, you can remove the device from the site scope.

If you deploy the application policy as-is, the policy will fail to deploy on the devices that reported a failure during the precheck process. To avoid the failure, you can remove the device from the site scope or update the device components to a level that the application policy supports. For a list of supported devices, see the Cisco DNA Center Supported Devices document.

Policy Scheduling

After you create or change a policy, you can deploy or redeploy the policy to the devices associated with it. You can deploy or redeploy a policy immediately or at a specific date and time, for example, on a weekend during off-peak hours. You can schedule a policy deployment for wired or wireless devices.

After you have scheduled a policy to be deployed, the policy and site scope are locked. You can view the policy, but you cannot edit it. If you change your mind about deploying the policy, you can cancel it.

Note When the scheduled event occurs, the policy is validated against the various policy components, for example, applications, application sets, and queuing profiles. If this validation fails, the policy changes are lost.

Policy Versioning

Policy versioning allows you to do the following tasks:

- Compare a previous version to the current (latest) one to see the differences.
- Display previous versions of a policy and select a version to reapply to the devices in a site scope.

Editing one version of a policy does not affect other versions of that policy or the components of the policy, such as the application sets that the policy manages. For example, deleting an application set from a policy does not delete the application set from Cisco DNA Center, other versions of that policy, or even other policies. Because policies and application sets exist independent of each other, it is possible to have a policy version that contains application sets that no longer exist. If you attempt to deploy or roll back to an older version of a policy that references an application set that no longer exists, an error occurs.

Note Policy versioning does not capture changes to applications (such as rank, port, and protocol), application set members, LAN queuing profiles, and sites.

Original Policy Restore

The first time that you deploy a policy to devices, Cisco DNA Center detaches the device's original Cisco Modular QoS CLI policy configurations, but leaves them on the device. Cisco DNA Center stores the device's original NBAR configurations in Cisco DNA Center. This allows you to restore the original Modular QoS CLI policies and NBAR configuration onto the devices later, if needed.

Note Because the Modular QoS CLI policies are not deleted from the device, if you remove these policies, you will not be able to restore them using the Cisco DNA Center original policy restore feature.

When you restore the original policy configuration onto a device, Cisco DNA Center removes the existing policy configuration that you deployed and reverts to the original configuration that was on the device.

Any Modular QoS CLI policy configurations that existed before you deployed application policies are reattached to the interfaces. However, queuing policies, such as multilayer switching (MLS) configurations, are not restored; instead, the devices retain the MLS configurations that were last applied through Cisco DNA Center.

After you restore the original policy configuration to the device, the policy that is stored in Cisco DNA Center is deleted.

Note the following additional guidelines and limitations for this feature:

- If the first attempt to deploy a policy to a device fails, Cisco DNA Center automatically attempts to restore the original policy configurations onto the devices.
- If a device is removed from an application policy after that policy has been applied to the device, the policy remains on the device. Cisco DNA Center does not automatically delete the policy or restore the QoS configuration on the device to its original (pre-Cisco DNA Center) configuration.

Stale Application Policies

An application policy can become stale if you change the configuration of something that is referenced in the policy. If an application policy becomes stale, you need to redeploy it for the changes to take affect.

An application policy can become stale for any of the following reasons:

- Change to applications referenced in an application set.
- Change to interfaces, such as SP Profile assignment, WAN subline rate, or WAN or LAN marking.
- Change to the queuing profile.
- New site added under a parent site in the policy.
- Device added to a site that is referenced by the policy.
- Devices moved between sites in the same policy.
- Change in interfaces exclusion/inclusion.
- Change in device Controller-Based Application Recognition (CBAR) status.

Application Policy Guidelines and Limitations

- Cisco DNA Center cannot learn multiple WLANs with the same SSID name on a wireless controller. At any point, Cisco DNA Center has only one entry for a WLAN with a unique name, although it is possible for the WLC to contain multiple entries with the same name and different WLAN profile names.

  You might have duplicate SSID names per WLC by design, or you might have inadvertently added a WLC with a duplicate SSID name using Cisco DNA Center. In either case, having duplicate SSID names per WLC is problematic for several features:

  - **Learn Config**: Cisco DNA Center learns only one randomly chosen SSID name per WLC and discards any remaining duplicate SSID names. (**Learn Config** is typically used in a brownfield scenario.)
  - **Application Policy**: When deploying an application policy, Cisco DNA Center randomly applies the policy to only one of the duplicate SSID names and not the others. In addition, policy restore, CLI preview, EasyQoS Fastlane, and PSK override features either fail or have unexpected outcomes.
  - **Multiscale Network**: In a multiscale network, multiple duplicate SSID names on multiple devices can cause issues. For example, one device has a WLAN configured as a nonfabric SSID, and a second device has the same WLAN, but it is configured as a fabric SSID. When you perform a **Learn Config**, only one SSID name is learned. The other SSID name from the other device is discarded. This behavior can cause conflicts, especially if the second device supports only fabric SSID names, but Cisco DNA Center is trying to perform operations on the device with nonfabric SSID names.
  - **IPACL Policy**: When deploying an IPACL policy, Cisco DNA Center randomly applies the policy to only one of the duplicate SSIDs. In addition, scenarios involving Flex Connect are also impacted.

- Cisco DNA Center does not recommend out-of-band (OOB) changes to device configurations. If you make OOB changes, the policy in Cisco DNA Center and the one configured on the device become inconsistent. The two policies remain inconsistent until you deploy the policy from Cisco DNA Center to the device again.
- The QoS trust functionality cannot be changed.
- Custom applications are not supported on the wireless controller. Therefore, custom applications are not selected while creating a wireless application policy.

- Make sure you delete the corresponding wireless application policy before deleting an SSID from design and reprovisioning the wireless controller.
- Wireless application for eWLC is not supported on SSID provisioned through learned configuration.
- Cisco DNA Center provides ACL-based Application Policy support for Cisco Catalyst IE 3300 Rugged Series switches and Cisco Catalyst IE 3400 Heavy Duty Series switches. You can deploy a maximum of eight port-based custom applications. However, there is no restriction for DSCP-based applications.

Note Cisco DNA Center does not support FlexConnect Local Switching mode for AireOS and eWLC platforms.

Manage Application Policies

The following sections provide information about how to manage application policies.

Prerequisites

To configure Application policies, make sure that you address the following requirements:

- Cisco DNA Center supports most of the Cisco LAN, WAN, WLAN devices. To verify whether the devices and software versions in your network are supported, see *Cisco DNA Center Supported Devices*.
- Make sure that your Cisco network devices, such as the ISR-G2, the ASR 1000, and Wireless LAN Controller, have the AVC (Application Visibility and Control) feature license installed. For information, see the *NBAR2 (Next Generation NBAR) Protocol Pack FAQ*.
- AVC support is available for switches running IOS-XE version 16.9 only if auto-QoS is not configured on the switches. You must upgrade the switches with auto-QOS configuration to IOS-XE version 16.11 or later to get AVC support.
- For Cisco DNA Center to identify the WAN interfaces that need policies, you must specify the interface type (WAN), and optionally, its subline rate and service-provider Class-of-Service model. For more information, see Assign a Service Provider Profile to a WAN Interface, on page 55.
- Verify that the device roles that were assigned to devices during the Discovery process are appropriate for your network. If necessary, change the device roles that are not appropriate. For more information, see Change the Device Role (Inventory).

Create an Application Policy

This section provides information about how to create an application policy.

Before you begin

- Define your business objectives. For example, your business objective might be to improve user productivity by minimizing network response times or to identify and deprioritize nonbusiness applications. Based on these objectives, decide which business relevance category your applications fall into.
- Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

- Verify that the device roles that were assigned to devices during the Discovery process are appropriate for your network. If necessary, change the device roles that are not appropriate. For more information, see Change the Device Role (Inventory).
- Add devices to sites. For more information, see Add a Device to a Site.
- If you plan to configure this policy with an SP profile for traffic that is destined for an SP, make sure that you have configured an SP profile. After creating the application policy, you can return to the SP profile and customize its SLA attributes and assign the SP profile to WAN interfaces. For more information, see Configure Service Provider Profiles.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Click **Add Policy**.

Step 3 In the **Application QoS Policy Name** field, enter a name for the policy.

Step 4 Click either the **Wired** or **Wireless** radio button.

Step 5 For wireless networks, select an SSID that is provisioned from the **SSID** drop-down list.

Step 6 Click **Site Scope** and check the check box next to the sites where you want to deploy the policy.

Note For policies of wired devices, you cannot select a site that is already assigned to another policy. For policies of wireless devices, you cannot select a site that is already assigned to another policy with the same SSID.

Step 7 For policies of wired devices, you can exclude devices or specific interfaces from being configured with the policy:

a) From the **Site Scope** pane, click ⚙ next to the site you are interested in.

A list of devices in the selected scope is displayed.

b) Locate the device that you want to exclude and click the toggle button in the corresponding **Policy Exclusions** column.

c) To exclude specific interfaces, click **Exclude Interfaces**.

d) From the list of **Applicable Interfaces**, click the toggle button next to the interfaces that you want to exclude.

By default, only the **Applicable Interfaces** are shown. You can choose **All** from the **Show** drop-down list to view all the interfaces.

e) Click **< Back to Devices in *Site-Name***.

f) Click **< Back to Site Scope**.

Step 8 For WAN devices, you can configure specific interfaces:

a) From the **Site Scope** pane, click ⚙ next to the desired site.

b) From the list of devices in the site, click **Configure** in the **SP Profile Settings** column next to the desired device.

Note This option is only available for routers.

c) In the **WAN Interface** column, from the **Select Interface** drop-down list, choose an interface.

d) In the **Role** column, from the **Select Role** drop-down list, choose a role according to the type of interface you are configuring:

- Physical interface: Choose **WAN**. This role is the only valid role for a physical interface.
- Tunnel interface: Choose either **DMVPN Branch** or **DMVPN Hub**. If you choose **DMVPN Hub**, you can also define the bandwidth to its corresponding branches.

Note Make sure that the tunnel interfaces have been created on the devices before deploying these policy settings.

e) In the **Service Provider Profile** column, from the **Select Profile** drop-down list, choose an SP profile.
f) (Optional) If necessary, in the **Sub-Line Rate (Mbps)** column, enter the upstream bandwidth that the interface requires.
g) (Optional) To configure additional WAN interfaces, click **+** and repeat Step c through Step f.
h) Click **Save**.
i) Click **< Back to Site Scope**.

Step 9 From the **Site Scope** pane, click **OK**.

Step 10 (Optional) If the CVD queuing profile (CVD_QUEUING_PROFILE) does not meet your needs, create a custom queuing profile.

a) Click **Queuing Profiles**.
b) Select a queuing profile from the list in the left pane.
c) Click **Select**.

Step 11 (Optional) If this policy is for traffic that is destined for an SP, customize the SP profile SLA attributes:

a) Click **SP Profile**.
b) Choose an SP profile.
c) Customize the SLA attributes (**DSCP**, **SP Bandwidth %**, and **Queuing Bandwidth %**).

Step 12 (Optional) Configure the business relevance of the application sets used in your network.

Cisco DNA Center comes with application sets that are preconfigured into business-relevancy groups. You can keep this configuration or modify it by dragging and dropping an application set from one business-relevancy group to another.

Applications marked as a favorites are listed at the top of the application set. To change favorites, go to the Applications registry.

Step 13 (Optional) Customize applications by creating consumers and assigning them to applications, or by marking an application as bidirectional:

a) Expand the application group.
b) Click the gear icon ⚙ next to the desired application.
c) From the **Traffic Direction** area, click the **Unidirectional** or **Bi-directional** radio button.
d) To choose an existing consumer, from the **Consumer** drop-down list, choose the consumer that you want to configure. To create a new consumer, click **+ Add Consumer** and define the **Consumer Name**, **IP/Subnet**, **Protocol**, and **Port/Range**.
e) Click **OK**.

Step 14 Configure host tracking. Click the **Host Tracking** toggle button to turn host tracking on or off.

When deploying an application policy, Cisco DNA Center automatically applies ACL entries to the switches to which collaboration endpoints (such as Telepresence units or Cisco phones) are connected.

The ACE matches the voice and video traffic generated by the collaboration endpoint, ensuring that the voice and video traffic are correctly marked.

When host tracking is turned on, Cisco DNA Center tracks the connectivity of the collaboration endpoints within the site scope and to automatically reconfigure the ACL entries when the collaboration endpoints connect to the network or move from one interface to another.

When host tracking is turned off, Cisco DNA Center does not automatically deploy policies to the devices when a collaboration endpoint moves or connects to a new interface. Instead, you need to redeploy the policy for the ACLs to be configured correctly for the collaboration endpoints.

Step 15 (Optional) Preview the CLI commands that will be sent to devices. For more information, see Preview an Application Policy, on page 51.

Step 16 (Optional) Precheck the devices on which you plan to deploy the policy. For more information, see Precheck an Application Policy, on page 51.

Step 17 Do one of the following tasks:

- Save the policy as a draft by clicking **Save Draft**. For more information, see Policy Drafts, on page 39.
- Deploy the policy by clicking **Deploy**. You can deploy the policy now or schedule it for a later time.

  To deploy the policy now, click the **Now** radio button and click **Apply**.

  To schedule the policy deployment for a later date and time, click the **Later** radio button and define the date and time of the deployment. For more information, see Policy Scheduling, on page 40.

  Note Site time zone setting is not supported for scheduling application policy deployments.

View Application Policy Information

You can display various information about the application policies that you have created and deployed.

Before you begin

You must have at least one deployed application policy.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Sort the policies by name, or filter them by name, status, or queuing profile.

Step 3 View the list of policies and the following information about each:

- **Policy Name**: Name of the policy.
- **Version**: Iteration of the policy. Each time a policy is deployed or saved as a draft, it is incremented by one version. For example, when you create a policy and deploy it, the policy is at version 1. If you change the policy and deploy it again, the version of the policy is incremented to version 2. For more information, see Policy Drafts, on page 39 and Policy Versioning, on page 40.
- **Policy Status**: State of the policy. If the policy applied on Cisco Catalyst 3850, Catalyst 4500, and Catalyst 9000 devices and is impacted by the port channel update (create/modify/delete), an alert is shown in the policy status.
- **Deployment Status**: State of the last deployment (per device). Presents a summary of the following
  - Devices that were successfully provisioned.
  - Devices that failed to be provisioned.
  - Devices that were not provisioned due to the deployment being terminated.

Clicking the state of the last deployment displays the Policy Deployment window, which provides a filterable list of devices on which the policy is deployed. For each device, the following information is displayed:

  - Device details (name, site, type, role, and IP address)
  - Success deployment status. Clicking the gear icon next to the status launches the **Effective Marking Policy** window that shows the **Business Relevant** and **Business Irrelevant** applications and the traffic class queue in which they end up. For devices that have limited TCAM resources or an old NBAR protocol pack, only a subset of the applications that are included in the policy can be provisioned, and they are shown in the view.
  - Failure status shows the reason for the failure.

- **Scope**: Number of sites (not devices) that are assigned to the policy. For policies of wireless devices, the name of the SSID to which the policy applies is included.
- **LAN Queuing Profile**: Name of the LAN queuing profile that is assigned to the policy.

Edit an Application Policy

You can edit an application policy.

Before you begin

You must have created at least one policy.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to edit.

Step 3 Click the radio button next to corresponding policy.

Step 4 From the **Actions** drop-down list, choose **Edit**.

Step 5 Make changes to the application policy, as needed.

Step 6 You can change the business relevance of an application by moving application set between business relevant, business irrelevant, and default groups.

For information about the application policy settings, see Create an Application Policy, on page 43.

Step 7 To update the queuing profile, click **Queuing Profiles**, and select a queuing profile from the list in the left pane.

Step 8 Click **Select**.

Step 9 Do one of the following tasks:

- Save the policy as a draft by clicking **Save Draft**. For more information, see Policy Drafts, on page 39.
- Deploy the policy by clicking **Deploy**. You can deploy the policy now or schedule it for a later time.

  To deploy the policy now, click the **Run Now** radio button and click **Apply**.

  To schedule policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment. For more information, see Policy Scheduling, on page 40.

Note The site time zone setting is not supported for scheduling application policy deployments.

Save a Draft of an Application Policy

When creating, editing, or cloning a policy, you can save it as a draft so that you can continue to modify it later. You can also make changes to a deployed policy and save it as a draft.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Create, edit, or clone a policy.

Step 3 Click **Save Draft**.

For more information, see Policy Drafts, on page 39.

Deploy an Application Policy

If you make changes that affect a policy's configuration, such as adding a new application or marking an application as a favorite, you should redeploy the policy to implement these changes.

Note Before deploying the policy, Auto-QoS config is automatically removed from Cisco Catalyst 3850, Catalyst 3650, and Catalyst 9000 devices with IOS version 16.x or later.

After creating the custom applications, if CBAR is enabled for a device, the custom applications automatically gets configured on the device. You must wait for the synchronization to the latest Application Registry to be completed before proceeding to deploy Application Policy on the device. You can view the synchronization status in **Provision** > **Services** > **Service Catalog** > **Application Visibility**.

If CBAR is enabled for a device, while deploying Application Policy only the attribute sets and maps will be configured on the device as the custom applications are configured through CBAR.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to deploy.

Step 3 Click the radio button next to the policy that you want to deploy.

Step 4 From the **Actions** drop-down list, choose **Deploy**.

a) If you redeploy the policy, you will be prompted to take an appropriate actions for the devices that were removed from the policy scope. Choose any one of the following appropriate actions.

- Delete policy from the devices (Recommended)
- Remove devices from policy scope
- Remove devices from policy scope and restore devices to brownfield configuration

b) Click **Apply**.

Step 5 You are prompted to deploy your policy now or to schedule it for a later time. Do one of the following:

- To deploy the policy now, click the **Run Now** radio button and click **Apply**.
- To schedule policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment.

Note The site time zone setting is not supported for scheduling application policy deployments.

Cancel a Policy Deployment

After you click **Deploy**, Cisco DNA Center begins to configure the policy on the devices in the site scope. If you realize that you made a mistake, you can cancel the policy deployment.

The policy configuration process is performed as a batch process, in that it configures 40 devices at a time. If you have 40 devices or fewer and you cancel a policy deployment, your devices might be configured anyway, because the deployment to the first batch of devices would have already taken place. However, if you have hundreds of devices, canceling the policy deployment can be useful when needed.

When you click **Abort**, Cisco DNA Center cancels the configuration process on devices whose configuration has not yet started, and changes the device status to **Policy Aborted**. Cisco DNA Center does not cancel the deployments that are in the process of being completed or have been completed. These devices retain the updated policy configuration and reflect the state of the policy configuration, whether it is Configuring, Successful, or Failed.

During a policy deployment, click **Abort** to cancel the policy configuration process.

Delete an Application Policy

You can delete an application policy if it is no longer needed.

Deleting policy deletes class maps, policy map, and association of policy map with wireless policy profile.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to delete.

Step 3 Click the radio button next to the policy that you want to delete.

Step 4 From the **Actions** drop-down list, choose **Undeploy Policy**.

Step 5 In the **Undeploy Policy** window, click the **Delete policy from devices** radio button and click **Apply**.

Step 6 To confirm the deletion, click **OK**. Otherwise, click **Cancel**.

Step 7 When the deletion confirmation message appears, click **OK** again.

You can view the deletion status of the policies in the **Application QoS Policies** page. If the status shows deletion failed, do the following:

a) Click the failed state link under **Deployment Status** in the **Application QoS Policies** page.

b) In the **Undeployment Status** window, click **Retry** to delete the policy.

Clone an Application Policy

If an existing application policy has most of the settings that you want in a new policy, you can save time by cloning the existing policy, changing it, and then deploying it to a different scope.

Before you begin

You must have created at least one policy.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to clone.

Step 3 Click the radio button next to the policy that you want to clone.

Step 4 From the **Actions** drop-down list, choose **Clone**.

Step 5 Configure the application policy, as needed. For information about the application policy settings, see Create an Application Policy, on page 43.

Step 6 Do one of the following tasks:

- Save the policy as a draft by clicking **Save Draft**. For more information, see Policy Drafts, on page 39.
- Deploy the policy by clicking **Deploy**. You can deploy the policy now or schedule it for a later time.

  To deploy the policy now, click the **Run Now** radio button and click **Apply**.

  To schedule the policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment. For more information, see Policy Scheduling, on page 40.

  Note The site time zone setting is not supported for scheduling application policy deployments.

Restore an Application Policy

If you create or make changes to a policy and then decide that you want to start over, you can restore the original QoS configuration that was on the device before you configured it using Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to reset.

Step 3 Click the radio button next to the policy.

Step 4 From the **Actions** drop-down list, choose **Undeploy Policy**.

Step 5 In the **Undeploy Policy** window, click the **Restore devices to original configurations** radio button and click **Apply**.

Step 6 Click **OK** to confirm the change or **Cancel** to cancel it.

You can view the restoration status of the policies in the **Application QoS Policies** page. If the status shows restoration failed, do the following:

a) Click the failed state link under **Deployment Status** in the **Application QoS Policies** page.

b) In the **Undeployment Status** window, click **Retry** to restore the policy.

Reset the Default CVD Application Policy

The CVD configuration is the default configuration for applications. If you create or make changes to a policy and then decide that you want to start over, you can reset the applications to the CVD configuration. For more information about the CVD configuration, see Application Policies, on page 30.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to reset.

Step 3 Click the radio button next to the policy.

Step 4 From the **Actions** drop-down list, choose **Edit**.

Step 5 Click **Reset to Cisco Validated Design**.

Step 6 Click **OK** to confirm the change or **Cancel** to cancel it.

Step 7 Do one of the following tasks:

- To save a draft of the policy, click **Save Draft**.
- To deploy the policy, click **Deploy**.

Preview an Application Policy

Before you deploy a policy, you can generate the CLI that will be applied to a device and preview the configuration.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Create or edit a policy, as described in Create an Application Policy, on page 43 or Edit an Application Policy, on page 47.

Step 3 Before deploying the policy, click **Preview**.

A list of the devices in the scope appears.

Step 4 Click **Generate** next to the device that you are interested in.

Cisco DNA Center generates the CLIs for the policy.

Step 5 Click **View** to view the CLIs or copy them to the clipboard.

Precheck an Application Policy

Before you deploy an application policy, you can check whether the devices in the site scope are supported. The precheck process includes validating a device's model, line cards, and software image.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Create or edit a policy, as described in Create an Application Policy, on page 43 or Edit an Application Policy, on page 47.

Step 3 Click **Pre-check**.

Cisco DNA Center checks the devices and reports failures, if any, in the **Pre-Check Result** column. The **Errors** tab shows the devices that do not support this policy. The **Warnings** tab shows the restrictions or features that are not supported if you chose to deploy this policy in the device. You can still deploy the policy for the devices listed under **Warnings** tab. To resolve the failures, bring the devices into compliance with the specifications listed in Cisco DNA Center Supported Devices.

Display Application Policy History

You can display the version history of an application policy. The version history includes the series number (iteration) of the policy and the date and time on which the version was saved.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Click the radio button next to the policy that interests you.

Step 3 From the **Actions** drop-down list, choose **History**.

Step 4 From the **Policy History** dialog box, you can do the following:

- To compare a version with the current version, click **Difference** next to the version that interests you.
- To roll back to a previous version of the policy, click **Rollback** next to the version that you want to roll back to.

Roll Back to a Previous Policy Version

If you change a policy configuration, and then realize that it is incorrect, or that is not having the desired affect in your network, you can revert to a policy that is up to five versions back.

Before you begin

You must have created at least two versions of the policy to roll back to a previous policy version.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Click the radio button next to the policy that interests you.

Step 3 From the **Actions** drop-down list, choose **Show History**.

Previous versions of the selected policy are listed in descending order, with the newest version (highest number) at the top of the list and the oldest version (lowest number) at the bottom.

Step 4 (Optional) To view the differences between the selected version and the latest version of a policy, click **Difference** in the **View** column.

Step 5 When you determine the policy version that you want to roll back to, click **Rollback** for that policy version.

Note If the selected site scope changed between policy versions, rollback is not done on the current (latest) selected site. Only the policy content is rolled back.

Step 6 Click **Ok** to confirm the rollback procedure.

The rolled back version becomes the newest version.

Manage Queuing Profiles

The following sections provide details about the various tasks that you can perform to manage queuing profiles.

Create a Queuing Profile

Cisco DNA Center provides a default CVD queuing profile (CVD_QUEUING_PROFILE). If this queuing profile does not meet your needs, you can create a custom queuing profile.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Queuing Profiles**.

Step 2 Click **Add Profile**.

Step 3 In the **Profile Name** field, enter a name for the profile.

Step 4 Configure the bandwidth for each traffic class by using the slider, clicking the plus (+) or minus (-) sign, or entering a specific number in the field.

The number indicates the percentage of the total interface bandwidth that will be dedicated to the selected application class. Because the total bandwidth equals 100, adding bandwidth to one application class subtracts bandwidth from another application class.

An open lock icon indicates that you can edit the bandwidth for the application class. A closed lock indicates that you cannot edit it.

If you make a mistake, you can return to the CVD settings by clicking **Reset to Cisco Validated Design**.

The graph in the middle helps you visualize the amount of bandwidth that you are setting for each application class.

Step 5 (For advanced users) To customize the DSCP code points that Cisco DNA Center uses for each of the traffic classes, from the **Show** drop-down list, choose **DSCP Values** and configure the value for each application class by entering a specific number in the field.

To customize the DSCP code points required within an SP cloud, configure an SP profile.

Step 6 Click **Save**.

Edit or Delete a Queuing Profile

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Queuing Profiles**.

Step 2 From the **Queuing Profile** pane, click the radio button next to the queuing profile that you want to edit or delete.

Step 3 Do one of the following tasks:

- To edit the profile, change the field values, except the profile name, and click **Save**. For information about the fields, see Create a Queuing Profile, on page 53.
- To delete the profile, click **Delete**.

You cannot delete a queuing profile if it is referenced in an application policy.

Manage Application Policies for WAN Interfaces

The following sections provide details about the various tasks that you can perform to manage application profiles for WAN interfaces.

Customize Service Provider Profile SLA Attributes

If you do not want to use the default SLA attributes assigned to your SP profile by its class model, you can customize the SP profile SLA attributes to fit your requirements. For more information about the default SP profile SLA Attributes, see Service Provider Profiles, on page 34.

Before you begin

Make sure that you have devices in your inventory. If not, discover devices using the Discovery feature.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to change.

Step 3 Select the radio button next to the policy.

Step 4 From the **Actions** drop-down list, choose **Edit**.

Step 5 Click **SP Profiles** and select an SP profile.

Step 6 You can modify the information in the following fields:

- **DSCP**: Differentiated Services Code Point (DSCP) value. Valid values are from 0 to 63.
  - Expedited Forwarding (EF)
  - Class Selector (CS): CS1, CS2, CS3, CS4, CS5, CS6
  - Assured Forwarding: AF11, AF21, AF41
  - Default Forwarding (DF)

  For more information about these DSCP values, see Marking, Queuing, and Dropping Treatments, on page 32.

- **SP Bandwidth %**: Percentage of bandwidth allocated to a specific class of service.
- **Queuing Bandwidth %**: Percentage of bandwidth allocated to each of the traffic classes. You can make one of the following changes:
  - To customize the queuing bandwidth, unlock the bandwidth settings by clicking the lock icon and adjust the bandwidth percentages.
  - To calculate the queuing bandwidth automatically from the SP bandwidth, lock the queuing bandwidth settings by clicking the lock icon and then clicking **OK** to confirm. By default, Cisco DNA Center automatically distributes the queuing bandwidth percentage such that the sum of the queuing bandwidth for all of the traffic classes in an SP class aligns with the SP bandwidth percentage of that class.

Step 7 Click **OK**.

Assign a Service Provider Profile to a WAN Interface

If you have already created an application policy and now want to assign SP profiles to WAN interfaces, you can edit the policy and perform this configuration, including setting the subline rate on the interface, if needed.

Before you begin

If you have not created a policy, you can create a policy and assign SP profiles to WAN interfaces at the same time. For more information, see Create an Application Policy, on page 43.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Application QoS** > **Application Policies**.

Step 2 Use the **Filter** field to locate the policy that you want to edit.

Step 3 Click the radio button next to the policy.

Step 4 From the **Actions** drop-down list, choose **Edit**.

Step 5 From the **Site Scope** pane, click the gear icon next to the site you are interested in.

Step 6 Click **Configure** in the **SP Profile Settings** column for the device you are interested in.

Step 7 In the **WAN Interface** column, from the **Select Interface** drop-down list, choose an interface.

Step 8 In the **Role** column, from the **Select Role** drop-down list, choose a role according to the type of interface you are configuring:

- **Physical interface**: Choose **WAN**. This role is the only valid role for a physical interface.
- **Tunnel interface**: Choose either **DMVPN Branch** or **DMVPN Hub**. If you choose **DMVPN Hub**, you can also define the bandwidth to its corresponding branches.

  Note Make sure that the tunnel interfaces have been created on the devices before deploying these policy settings.

Step 9 In the **Service Provider Profile** column, click the **Select Profile** drop-down field and choose an SP profile.

Step 10 If necessary, in the **Sub-Line Rate (Mbps)** column, enter the upstream bandwidth that the interface requires.

Step 11 To configure additional WAN interfaces, click **+** and repeat Step 7 through Step 10.

Step 12 Click **Save**.

Step 13 Click **< Back to Site Scope**.

Step 14 Click **OK**.

Step 15 Click **Deploy**.

You are prompted to deploy your policy now or to schedule it for a later time.

Step 16 Do one of the following:

- To deploy the policy now, click the **Run Now** radio button and click **Apply**.
- To schedule policy deployment for a later date and time, click the **Schedule Later** radio button and define the date and time of the deployment.

Note The site time zone setting is not supported for scheduling application policy deployments.

Traffic Copy Policies

Using Cisco DNA Center, you can set up an Encapsulated Remote Switched Port Analyzer (ERSPAN) configuration such that the IP traffic flow between two entities is copied to a specified destination for monitoring or troubleshooting.

To configure ERSPAN using Cisco DNA Center, create a traffic copy policy that defines the source and destination of the traffic flow that you want to copy. You can also define a traffic copy contract that specifies the device and interface where the copy of the traffic is sent.

Note Because traffic copy policies can contain either scalable groups or IP network groups, throughout this guide, we use the term *groups* to refer to both scalable groups and IP network groups, unless specified otherwise.

Sources, Destinations, and Traffic Copy Destinations

Cisco DNA Center simplifies the process of monitoring traffic. You do not have to know the physical network topology. You only have to define a source and destination of the traffic flow and the traffic copy destination where you want the copied traffic to go.

- **Source**: One or more network device interfaces through which the traffic that you want to monitor flows. The interface might connect to end-point devices, specific users of these devices, or applications. A source group comprises Ethernet, Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, or port channel interfaces only.
- **Destination**: The IP subnet through which the traffic that you want to monitor flows. The IP subnet might connect to servers, remote peers, or applications.
- **Traffic Copy Destination**: Layer 2 or Layer 3 LAN interface on a device that receives, processes, and analyzes the ERSPAN data. The device is typically a packet capture or network analysis tool that receives a copy of the traffic flow for analysis.

  Note At the destination, we recommend that you use a network analyzer, such as a Switch Probe device, or other Remote Monitoring (RMON) probe, to perform traffic analysis.

  The interface type can be Ethernet, Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet interfaces only. When configured as a destination, the interface can be used to receive only the copied traffic. The interface can no longer receive any other type of traffic and cannot forward any traffic except that required by the traffic copy feature. You can configure trunk interfaces as destinations. This configuration allows the interfaces to transmit encapsulated traffic.

Note There can be only one traffic copy destination per traffic copy contract.

Guidelines and Limitations of Traffic Copy Policy

The traffic copy policy feature has the following limitations:

- You can create up to 8 traffic copy policies, 16 copy contracts, and 16 copy destinations.
- The same interface cannot be used by more than one traffic copy destination.
- Cisco DNA Center does not show a status message to indicate that a traffic copy policy has been changed and is no longer consistent with the one that is deployed in the network. However, if you know that a traffic copy policy has changed since it was deployed, you can redeploy the policy.
- You cannot configure a management interface as a source group or traffic copy destination.

Workflow to Configure a Traffic Copy Policy

Before you begin

- To be monitored, a source scalable group that is used in a traffic copy policy needs to be statically mapped to the switches and their interfaces.
- A traffic copy policy destination group needs to be configured as an IP network group. For more information, see Create an IP Network Group, on page 26.

Step 1 Create a traffic copy destination.

This is the interface on the device where the traffic flow will be copied for further analysis. For information, see Create a Traffic Copy Destination, on page 57.

Step 2 Create a traffic copy contract.

The contract defines the copy destination. For information, see Create a Traffic Copy Contract, on page 58.

Step 3 Create a traffic copy policy.

The policy defines the source and destination of the traffic flow and the traffic copy contract that specifies the destination where the copied traffic is sent. For information, see Create a Traffic Copy Policy, on page 59.

Create a Traffic Copy Destination

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Policy** > **Traffic Copy** > **Traffic Copy Destination**.

Step 2 Enter a name and description for the traffic copy destination.

Step 3 Select the device and one or more ports.

Step 4 Click **Save**.

Edit or Delete a Traffic Copy Destination

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Traffic Copy** > **Traffic Copy Destination**.

Step 2 Check the check box next to the destination that you want to edit or delete.

Step 3 Do one of the following:

- To make changes, click **Edit**, make the necessary changes, and click **Save**.
- To delete the destination, click **Delete**.

Create a Traffic Copy Contract

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Traffic Copy** > **Traffic Copy Contract**.

Step 2 Click **Add**.

Step 3 In the dialog box, enter a name and description for the contract.

Step 4 From the **Copy Destination** drop-down list, choose a copy destination.

Note You can have only one destination per traffic copy contract.

If no copy destinations are available for you to choose, you can create one. For more information, see Create a Traffic Copy Destination, on page 57.

Step 5 Click **Save**.

Edit or Delete a Traffic Copy Contract

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Traffic Copy** > **Traffic Copy Contract**.

Step 2 Check the check box next to the contract that you want to edit or delete.

Step 3 Do one of the following:

- To make changes, click **Edit**, make the necessary changes, and click **Save**.
- To delete the contract, click **Delete**.

Create a Traffic Copy Policy

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Traffic Copy** > **Traffic Copy Policies**.

Step 2 Click **Add Policy**.

Step 3 In the **Policy Name** field, enter a name.

Step 4 In the **Description** field, enter a word or a phrase that identifies the policy.

Step 5 In the **Contract** field, click **Add Contract**.

Step 6 Click the radio button next to the contract that you want to use and then click **Save**.

Step 7 Drag and drop groups from the **Available Groups** area to the **Source** area.

Step 8 Drag and drop groups from the **Available Groups** area to the **Destination** area.

Step 9 Click **Save**.

Edit or Delete a Traffic Copy Policy

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Policy** > **Traffic Copy** > **Traffic Copy Policies**.

Step 2 Check the check box next to the policy that you want to edit or delete.

Step 3 Do one of the following:

- To make changes, click **Edit**, make the necessary changes, and click **Save**.
- To delete the policy, click **Delete**.