

Configure Group-Based Access Control Policies and Analytics

- Group-based access control, on page 1
- Cisco Group-Based Policy Analytics, on page 15

Group-based access control

Catalyst Center implements Software-Defined Access (SD-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 these benefits:

- Rich identity-based access control functionality with network automation and assurance benefits.
- Granular access control.
- Security 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 security 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 Catalyst Center, see the *Catalyst Center Administrator Guide*.

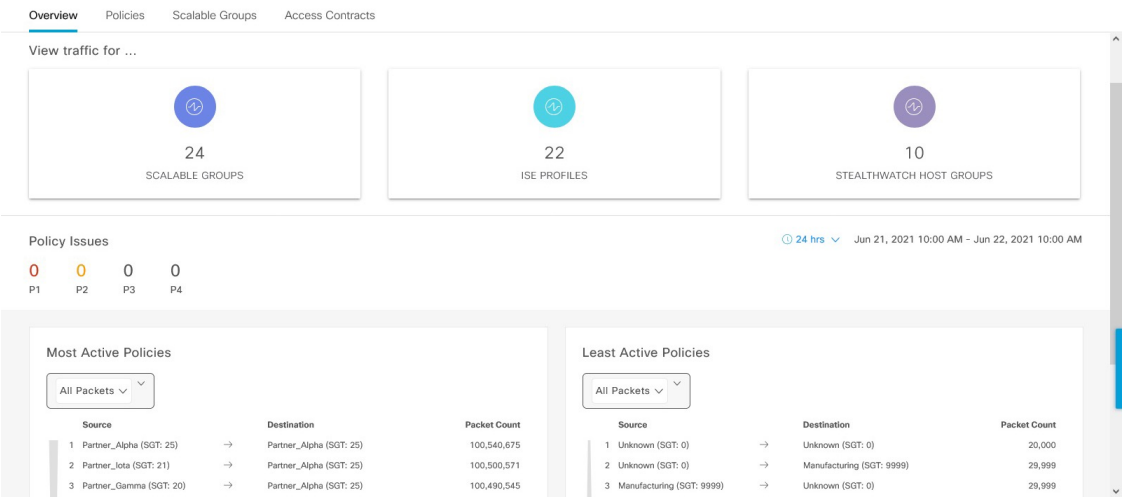
For information about configuring Catalyst Center for Cisco ISE, see the *Catalyst Center Installation Guide*.

For information about configuring Cisco ISE for Catalyst 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. From the main menu, choose **Policy** > **Group-Based Access Control** > **Overview** to view this dashboard.

Figure 1: Group-Based Access Control Policy dashboard



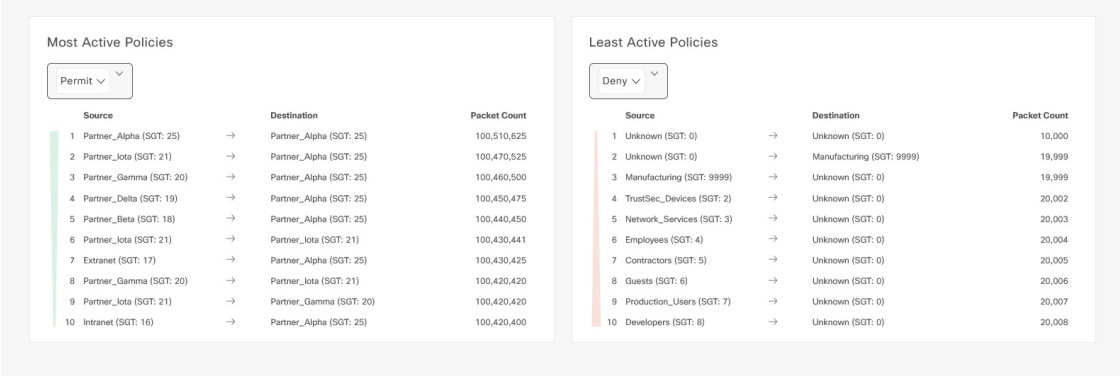
You can view these details in this dashboard:

- **View Traffic**: You can view the traffic for security 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 15.
- **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 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 Active Policies and Least Active Policies dashlets



Note 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

Access control policies define which network traffic can pass from a source security group to a destination security group.

- **Security Group**: A classification category to which you can assign users, network devices, or resources. Security groups are used in access control policies. You can associate security 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 security groups. In other words, a contract is a traffic filter definition. Access contracts define the actions (permit or deny) that are 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.

  Security groups and access contracts are the basic building blocks of access control policy. While creating an access control policy, you can use the security groups and contracts that you have created earlier, or create new security 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 security 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 security group, you can create an access control policy with single destination and multiple source groups.

You can specify the default policy to be used when no contract is specified for a source and destination security 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 corner of the **Group-Based Access Control** window to launch the **List** view.

- **Source View**: Displays a list of existing policies that are 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 that are 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 security group, use the **Source** view. To see which source groups can access the Finance Servers destination security group, use the **Destination** view.

You can also view the policy enforcement statistics data in the policies listing table. The total number of permitted and denied policies display 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.

Consider these points while using the policy enforcement statistics data:

- Policy enforcement statistics data is available only when the Group-Based Policy Analytics package is deployed.
- Telemetry subscription is added as part of base provisioning for both fabric and nonfabric network devices. The TrustSec enforcement action is invoked when a new network device is added to Catalyst Center and assigned to a site.
- Software-Defined Access (SD-Access) 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 supports TDL streaming data.
- NETCONF must be enabled on the network devices.

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

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

- After upgrading, you will see this 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 the network devices with site assigned.

Matrix view

Click the **Grid** icon at the top-right corner of the **Group-Based Access Control** window to launch the Matrix view. The Matrix view is a core policy view that provides an overview of all the policies for all the security groups (whether explicit or default). You can use the Matrix view to view all the 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 security groups.
- Destination axis: The horizontal axis lists all the destination security groups.

Place the cursor over a cell to view the policy for a given source security group and a destination security group. The color of a cell is based on the policy that applies to that cell. Colors indicate which policies are applied to each cell, including:

- **Permit**: Green
- **Deny**: Red
- **Custom**: Gold
- **Default**: Gray

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

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

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

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

You can navigate through the matrix by dragging the cursor over the matrix content area, or by using the 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 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 your cursor over 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.

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

Policy creation overview

1. Define the categorizations for your organization or the portion of your organization that you plan to start with.
2. Create security groups for the categorizations that you identified.
3. Create access contracts for the types of network traffic that 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 a security group

Before you begin

To do this task, you must be a Super Admin or Network Admin.

Procedure

Step 1 From the main menu, choose **Policy** > **Group-Based Access Control** > **Security Groups**.

Step 2 Click **Create Security Group**.

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

Note These characters are supported for the **Name** field:

- alphanumeric characters
- underscore (_)

The security group name must start with an alphabetic character.

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

Step 4 From the **Virtual Networks** drop-down list, choose the virtual networks to be associated with this security group. By default, the default virtual network is selected.

Note When Catalyst Center 2.3.3 or later is integrated with Cisco ISE 3.2 or later, security groups are not associated with virtual networks, and the **Virtual Networks** field do not display for these releases. However, if you are using Cisco ISE 3.1 or earlier, the security group and virtual network association details display.

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

Step 6 Choose whether you want to create the security group now or schedule it for later.

If the **Automation Events for ITSM (ServiceNow)** bundle is enabled, the **Save Now** option is disabled, and only the **Schedule Later** option is enabled for group-based policy changes. The scheduled task must be approved in IT Service Management (ITSM) before the scheduled time. If the task is not approved before the scheduled time, the task fails. For information on how to integrate ITSM with Catalyst Center, see the *Cisco Catalyst Center ITSM Integration Guide*.

You can view the total number of upcoming, in-progress, and failed tasks at the top-right corner of the **Security Groups** window. Click the task status link to view the task details in **Activities** > **Tasks**. You can edit or cancel a task before it is executed.

Note You cannot create a security group with the name ANY or the tag value 0xFFFF/65535. Security Group ANY/65535 is a reserved internal security group that is used for the Catalyst Center default policy.

Edit a security group

Before you begin

To do this task, you must be a Super Admin or Network Admin.

Procedure

Step 1 From the main menu, choose **Policy** > **Group-Based Access Control** > **Security Groups**.

Step 2 In the **Security Groups** window, check the check box next to the security group that you want to edit, and then click **Edit**.

Step 3 In the **Edit Security Group** slide-in pane, after making the necessary changes:

- Click **Save Now** to save the changes immediately.
- Click **Schedule Later** to schedule the update at a specific time. In the **Scheduler** slide-in pane, specify the start time, date, and time zone, and then click **Apply**.

When you update the security groups, you must deploy the changes on the network devices. Click **Deploy Now** to deploy the changes immediately, or click **Deploy Later** to deploy the changes later.

Delete a security group

Before you begin

To do this task, you must be a Super Admin or Network Admin.

Procedure

Step 1 From the main menu, choose **Policy** > **Group-Based Access Control** > **Security Groups**.

Step 2 Check the check box next to the security group that you want to delete.

Step 3 Choose one of these options:

- To delete the security group immediately, click **Delete Now**.
- To delete the security group later, click **Delete Later**. In the **Schedule Delete** slide-in pane, specify the start time, date, and time zone, and then click **Apply**.



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

Synchronization of security groups between Catalyst Center and Cisco ISE

While synchronizing the security groups in Catalyst Center with Cisco ISE:

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

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

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

The **Associated Contracts** column shows the associated contracts for the security 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 security group configuration is updated in Cisco ISE. A new EEPG is created in ACI when a security group is created in Cisco ISE.

Create an access 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 security groups. Access contracts define the actions (permit or deny) that are performed when the traffic matches a network application, protocol, and port.

Before you begin

To do this task, you must be a Super Admin or Network Admin.

Procedure

Step 1 From the main menu, 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 the required details.

The **Modeled Access Contract** check box is enabled by default. This enables Catalyst Center to generate the valid commands for the underlying Security Group ACLs (SGACLs). When this option is enabled, the access contract is based on a model that allows you to create and edit without the need to know the underlying command line syntax.

Uncheck the **Modeled Access Contract** check box if you want to enter the SGACL command lines directly and store the access contract as text. Syntax checking is not done for the command line text that you enter. You must ensure that the command syntax is valid.

Note

- You can enable or disable this option only at the time of creating the access contracts. You cannot update this option for the existing access contracts.
- Some of the advanced SGACL commands might not be supported on all Cisco network devices.

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 Choose whether you want to create the access contract now or schedule it for later.

If the **Automation Events for ITSM (ServiceNow)** bundle is enabled, the **Save Now** option is disabled, and only the **Schedule Later** option is enabled for group-based policy changes. The scheduled task must be approved in IT Service Management (ITSM) before the scheduled time. If the task is not approved before the scheduled time, the task fails. For information on how to integrate ITSM with Catalyst Center, see the Cisco Catalyst Center ITSM Integration Guide.

You can view the total number of upcoming, in-progress, and failed tasks at the top-right corner of the **Access Contract** window. Click the task status link to view the task details in **Activities > Tasks**. You can edit or cancel a task before it is executed.

Edit an access contract

Before you begin

To do this task, you must be a Super Admin or Network Admin.

Procedure

Step 1 From the main menu, choose **Policy** > **Group-Based Access Control** > **Access Contracts**.

Step 2 In the **Access Contracts** window, check the check box next to the access contract that you want to edit.

Step 3 Choose **Actions > Edit**.

Step 4 In the **Edit Access Contract** window, after making the necessary changes, choose whether you want to update the access contract now or schedule it for later.

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

You can duplicate an existing access contract and create a new access contract by editing the required details. When you duplicate an access contract, all information in the existing access contract is copied and the copied contract has the existing contract name with the string **Copy** appended at the end. Click **Save Now** to create the duplicate contract immediately, or click **Schedule Later** to create the duplicate contract later.

When you update the security 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 Catalyst Center. To resolve this situation, you must deploy the updated policies on the network devices. Click **Deploy Now** to deploy the changes immediately, or click **Deploy Later** to deploy the changes later.

Cisco ISE provides the runtime policy platform for providing policy download to the network devices on behalf of Catalyst 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.

Delete an access contract

Before you begin

To do this task, you must be a Super Admin or Network Admin.

Procedure

Step 1 From the main menu, choose **Policy** > **Group-Based Access Control** > **Access Contracts**.

Step 2 In the **Access Contracts** window, check the check box next to the access contract that you want to delete, and then choose whether you want to delete the access contract now or schedule it for later.

You can 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 link in the **Policies** column of an access 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.

Synchronization of access contracts between Catalyst Center and Cisco ISE

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

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

An orange triangle icon displays next to an access 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 access contracts that are learned from ACI, but you can use them in the policies while using the ACI-learned security groups. While creating or updating a policy from the Matrix view, if you select an ACI-learned security group as the destination group, the associated access contracts are displayed in the **Preferred Contracts** tab. You can view all the access contracts in the **All Contracts** tab.

Create group-based access control policy

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

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, 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 security 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 security 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.

Procedure

Step 1 In 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 security group that you want to select.

If the security group that you want does not exist, click **Create Security Group** to create a new security group. This option is not available if the **Automation Events for ITSM (ServiceNow)** bundle is enabled.

b) Click **Next**.

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

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



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

d) Click **Next**.

e) Click the radio button next to the contract that you want to select. You can view and edit the contract details, if necessary.

If the contract that you want does not exist, click **Create Contract** to create a new contract. This option is not available if the **Automation Events for ITSM (ServiceNow)** bundle is enabled.



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 security groups and contract.

g) Choose whether you want to create the policy now or schedule it for later.

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

a) Click the radio button next to the destination security group that you want to select.

If the security group that you want does not exist, click **Create Security Group** to create a new security group. This option is not available if the **Automation Events for ITSM (ServiceNow)** bundle is enabled.

b) Click **Next**.

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

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

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

d) Click **Next**.

e) Click the radio button next to the contract that you want to select.

If the contract that you want does not exist, click **Create Contract** to create a new contract. This option is not available if the **Automation Events for ITSM (ServiceNow)** bundle is enabled.

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 security groups and contract.

g) Choose whether you want to create the policy now or schedule it for later.

If the **Automation Events for ITSM (ServiceNow)** bundle is enabled, the **Save Now** option is disabled, and only the **Schedule Later** option is enabled for group-based policy changes. The scheduled task must be approved in IT Service Management (ITSM) before the scheduled time. If the task is not approved before the scheduled time, the task fails. For information on how to integrate ITSM with Catalyst Center, see the Cisco Catalyst Center ITSM Integration Guide.

You can view the total number of upcoming, in-progress, and failed tasks at the top-right corner of the **Policies** window. Click the task status link to view the task details in **Activities** > **Tasks**. You can edit or cancel a task before it is executed.

Update a group-based access control policy based on traffic flows

Procedure

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

Step 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.

Step 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, use the **View Traffic** option for any rule to see the list of flows matching that rule.

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 the 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 the custom access contract, you can edit the selected access contract.

Step 4 After making the required changes, choose one of these options:

- **Save the changes to the existing contract. Changes affect all the 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.**

Synchronization of policies between Catalyst Center and Cisco ISE

While synchronizing the policies in Catalyst Center with Cisco ISE:

- If a policy is present in Catalyst 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 Catalyst Center, it is created in Catalyst Center.
- If a policy contract is different in Cisco ISE, Catalyst 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). Catalyst 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 Catalyst 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

About 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 these questions:

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

You can purchase one of these types of licenses for Catalyst Center:

- Essentials
- Advantage
- Premier

The Advantage and Premier licenses contain the Group-Based Policy Analytics package. This package consists of these archives (.tar.gz files):

- Backend
- User Interface
- Summarizer Pipeline
- Aggregation definitions

Install Group-Based Policy Analytics

Cisco Group-Based Policy Analytics is a part of Catalyst Center, but it is not installed by default.

To install Group-Based Policy Analytics:

Procedure

Step 1 From the main menu, choose **System** > **Software Management**.

Step 2 Scroll down to the **Available Applications for 2.3.x.x-xxxxx** area and select **Group-Based Policy Analytics**.

Step 3 Click **Install** to install the application.

Hardware and software compatibility

Platform support

Cisco Group-Based Policy Analytics is supported on these 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 table lists the performance metrics that Catalyst 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.

Note This table lists the performance metrics for a standalone deployment. These values might vary based on the number of nodes in the cluster and the number of installed packages.

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; 13,000 APs
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. This 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 Catalyst Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow configurable using the CLI Template tool in the Catalyst 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 Catalyst Center UI (Flexible NetFlow or Application Visibility and Control Based NetFlow)	NetFlow configurable using the CLI Template tool in the Catalyst 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

Catalyst Center supports Cisco ISE 2.4 Patch 7 and later, Cisco ISE 2.6 Patch 1 and later, and Cisco ISE 2.7 and later.

Cisco Stealthwatch

Catalyst Center supports Cisco Stealthwatch 7.x or later.

Understand connectors

Cisco Group-Based Policy Analytics gathers telemetry from various 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 19 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 Session Directory, security 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 Session Directory service. Other services, like security 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 security 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 that 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 Catalyst Center. NetFlow is collected and aggregated natively by Catalyst 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 the 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

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

Procedure

Step 1 From the main menu, choose **Policy** > **Group-Based Access Control** > **Overview**. The **Create policies with more confidence** window displays.

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

Step 3 Click **Let's Do It**.

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



Note If the Cisco ISE version is earlier than the version required for running Cisco Group-Based Policy Analytics, an error message displays.

Step 4 Click **Configure** at the bottom of the connector that you want to configure.
A new window opens, redirecting you to the Catalyst 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. A green dot displays 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 displays.

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

- Provision NetFlow on the Catalyst Center device interface manually.
- Click **CLI Templates** to configure NetFlow using the **CLI Templates** tool in Catalyst 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

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

Multiple groups to multiple groups

When you click the number that displays in the **Security Groups** box in the **Overview** window, the **Explore Security Groups** window displays. In this window, you see a summary of all the group-to-group communication among security groups. By default, the time range for this view is the last available 24 hours of data.

Note 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 security groups and their corresponding interactions, starting with the source security 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 security groups for the selected source security group and the unique flow count for each destination security 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.

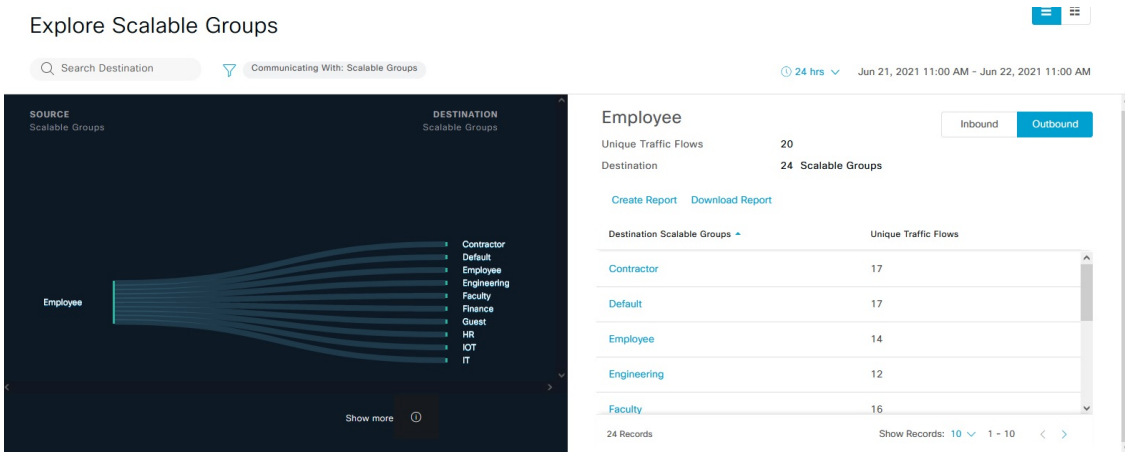
When you click the number displayed in the **ISE Profiles** box in the **Overview** window, the **Explore ISE Profiles** window displays. In this window, you can see a summary of all the communication from ISE Profiles as the source and security groups as the destination. In order to focus on the group-based policy decisions, either the source or destination category must be the security 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 displays. In this window, you can see a summary of all the communication, with Stealthwatch Host Groups as the source and the security groups as the destination. In order to focus on the group-based policy decisions, either the source or destination category must be the security 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 security group. By default, the time range for this view is the last available 24 hours of data, and the default number of links or records shown is 10.



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

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

Click any column to sort it 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.

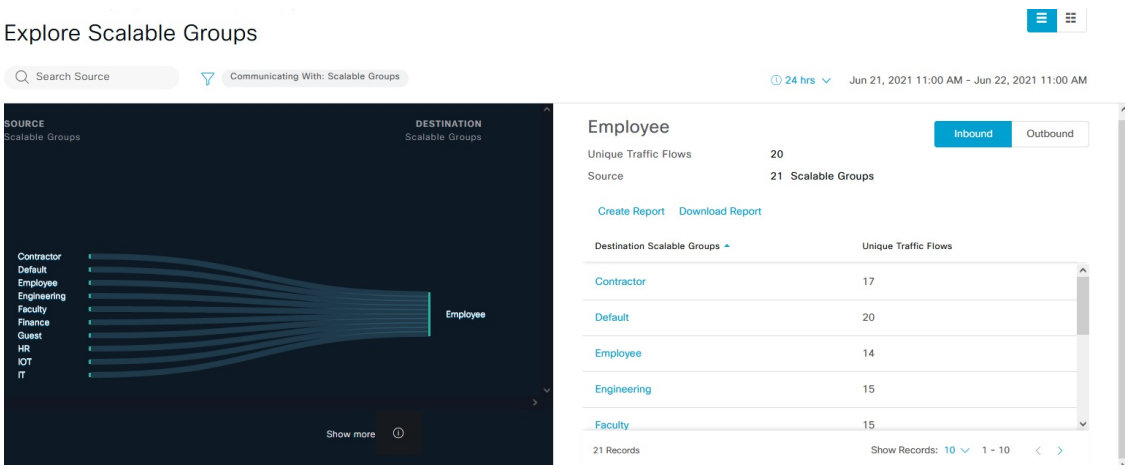
When you hover your cursor over a link, it is highlighted, and a tooltip shows the number of unique traffic flows. If you click this link, it takes you to the **Single Group to Single Group** window.

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.

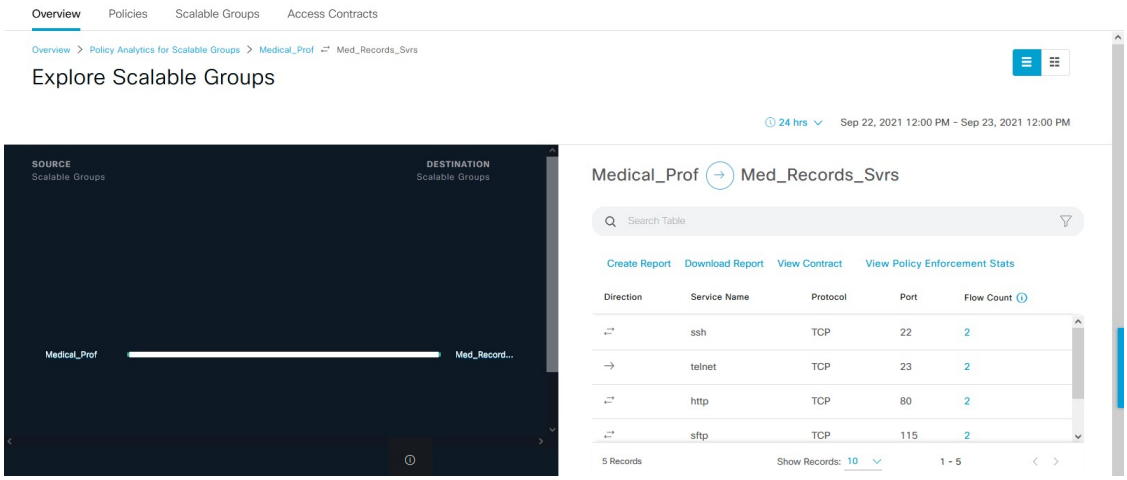
Single Group to Multiple Groups: Inbound

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



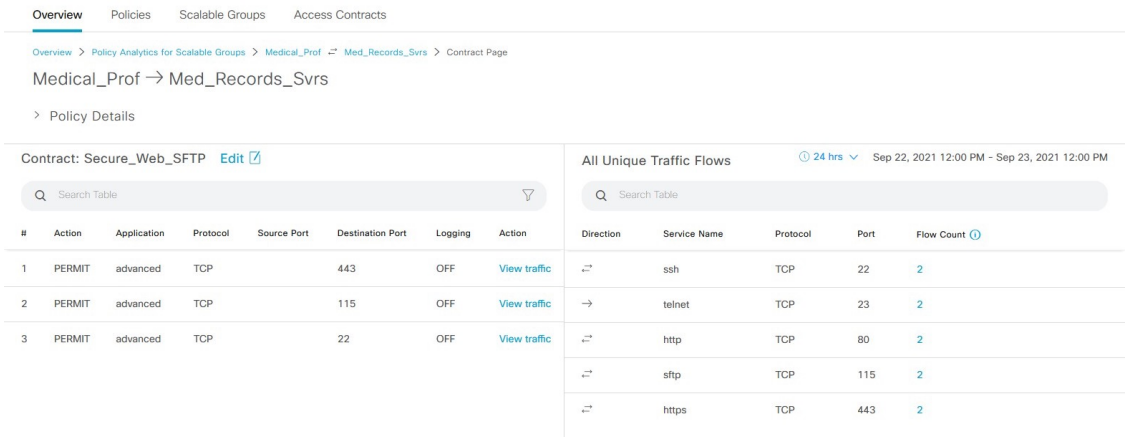
Single group to single group

This window shows the activity between a source group and a destination group. Either the source group, the destination group, or both must be a security 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.

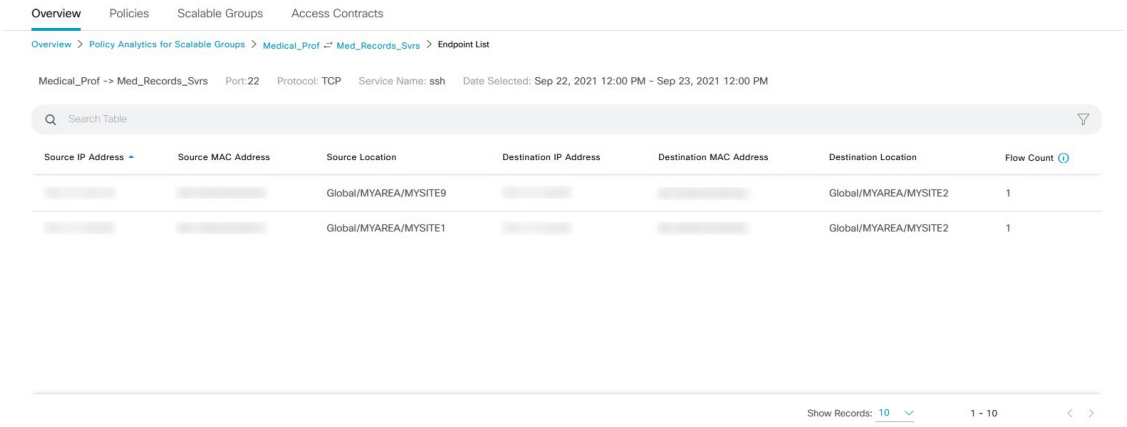


When you click the directional arrow displayed between the source and destination groups, the source and destination groups are interchanged in this view.

Click **View Contract** to view a side-by-side comparison of traffic flows with the access contract rules that are in effect for this source and destination group pair.

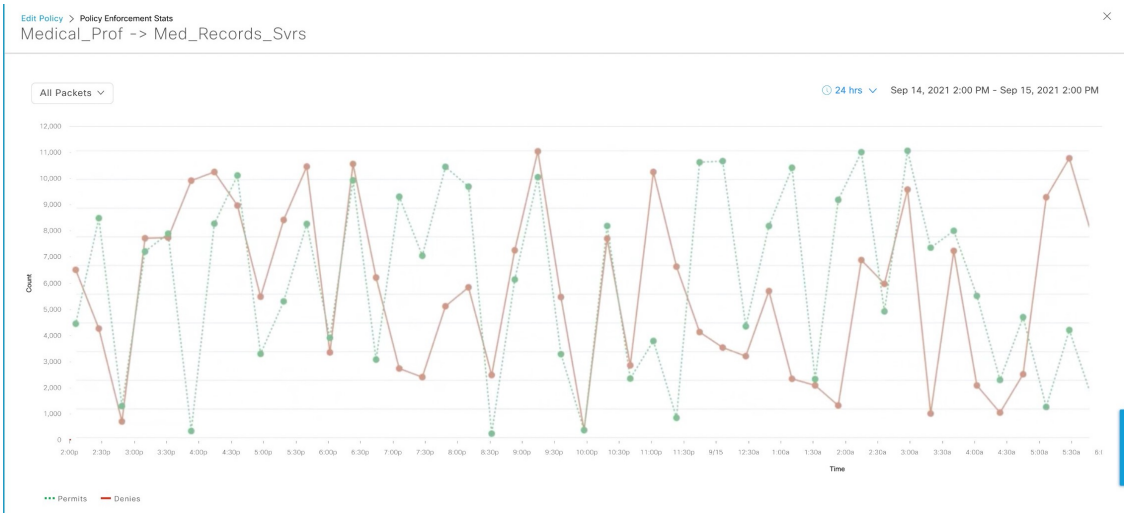


The left pane in the **View Contract** window displays the rules for permitted and denied traffic between the source and destination groups. You can view the traffic flows that match any selected rule in the right pane. You can view the flow direction, service name, flow count, ports, and protocol details in the right pane. The **Flow Count** column displays the number of flows detected for that particular service, port, and protocol combination for the selected time period. You can click the flow count link to view the flow details for each endpoint.



Note When you sort the **Traffic Flows** table based on the flow count, only 1000 records display.

Click **View Policy Enforcement Stats** to view a time-series graph of the permit and deny counts for any source and destination group pair. It provides per-policy enforcement statistics visibility. You can use the **All Packets** drop-down list to select only the permitted or dropped packets. Graph data points are displayed for each 15-minute data collection period. You can hover over any data point to view the number of permits and denies. You can click a data point or time period to view the contract and traffic flow details for the selected time period.



Note The selected time period is the hour that contains the 15-minute interval corresponding to the selected data point because the flow data aggregation is done every 60 minutes.

The **Traffic Flows** table can also be accessed from the **Policy Details** slide-in pane while creating or editing a policy.

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.

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.

Access contracts

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

View a contract

To launch the **View Contract** window, from the **Explore Security 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. From the main menu, 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 an 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 + 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.

Saving a newly created or edited contract includes these options:

- **Update current policy only**: A duplicate of the contract creates and applies to the current policy. Other policies that reference this contract are not affected.

- **Update contract for all referenced policies**: The contract updates and applies 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 a contract

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

Edit a contract

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

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

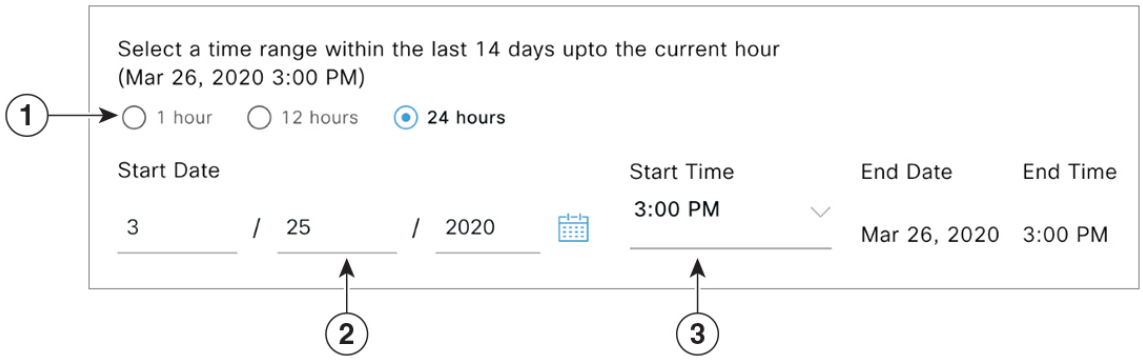
- **Update current policy only**: A duplicate of the contract creates and applies to the current policy. Other policies that reference this contract are not affected.
- **Update contract for all referenced policies**: The contract updates and applies to the current policy and other policies that reference this contract.
- **Create a new contract with no policies affected**: A duplicate of the contract creates but doesn't apply 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 to specify the data in 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



1. Select one of the options. The **End Time** adjust 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 security 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 security groups, ISE profiles, and Stealthwatch host groups, and up to three results are displayed for each group type. For MAC addresses, the relevant characters are hexadecimal and colon.

Cisco Group-Based Policy Analytics supports both IPv4 and IPv6 addresses for endpoints. You can search and filter the endpoints using an IPv4 or IPv6 address.

- These characters can be used to search and filter IPv4 addresses:
  - Numbers (0-9)
  - Dot (.)

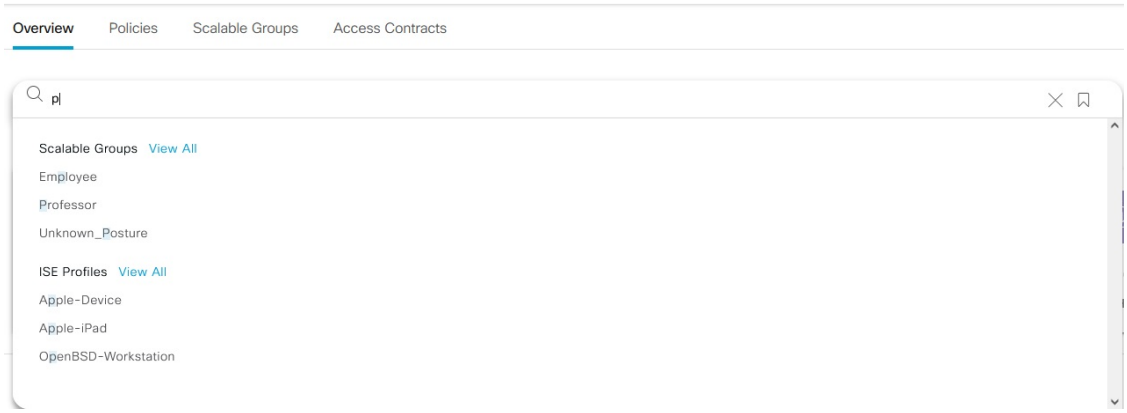
  You can enter up to 15 characters in the filter field.
- These characters can be used to search and filter IPv6 addresses:
  - Numbers (0-9)
  - Lowercase and uppercase alphabetic characters (a-f, A-F)
  - Colon (:)

  You can enter up to 39 characters in the filter field.

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. For more information, see Role-Based Access Control, on page 28.

Figure 4: Search window



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 filter 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 bookmark icon, and use the **Save Current Search** option to save the current displayed search.

To delete a saved search, click the bookmark icon. Hover your cursor over the name of the saved search, and click the cross 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 (RBAC). 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 configure the data connectors.
- A read-only user cannot export data because exporting data is an HTTPS POST operation.
- A read-only user can only perform a search by group and is restricted from other search functions because they involve HTTPS POST operations.