



Configure Policies

- [Policy Overview, page 1](#)
- [Policy Dashboard, page 1](#)
- [Virtual Networks, page 2](#)
- [Group-Based Access Control Policies, page 4](#)
- [Traffic Copy Policies, page 8](#)

Policy Overview

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

Policy Dashboard

The **Policy Dashboard** window shows the number of virtual networks, group-based access control policies, traffic copy policies, and scalable groups that you have created. In addition, it shows the number of policies that have failed to deploy.

The **Policy Dashboard** window provides a list of policies and the following information about each policy:

- **Policy Name**—Name of policy.
- **Policy Type**—Type of policy. Valid types are access control and traffic copy policies.
- **Policy Version**—Iteration of policy. Each time a policy is changed and saved, it is incremented by one version. For example, you create a policy and save it. The policy is at version 1. If you change the policy and save it again, the version of the policy is incremented to version 2.
- **Modified By**—User who modified the particular version of a policy.
- **Description**—Word or phrase that identifies a policy.

- **Policy Scope**—User and device groups or applications that a policy affects.
- **Timestamp**—Date and time when a particular version of a policy was saved.

Virtual Networks

Virtual networks are isolated routing and switching environments. By default, hosts that exist within separate virtual networks cannot communicate with each other. You can use virtual networks to segment your physical network into multiple logical networks.

A typical use case is for segmenting guests, employees, and contractors into separate groups so that you can allow and restrict access to parts of the network. The different types of networks are:

- **Guest network**—Network connections provided by a company to enable their guests to gain access to the Internet and their own enterprise without compromising the security of the host enterprise network. Guests can access the Internet but cannot access internal applications that are hosted in the data center.
- **Employee network**—Network connections that allow access to the Internet and internal applications. This group can be segmented further to allow or restrict access within the enterprise network, for example, to specific internal applications, lab environments, and servers. For example, a finance employee does not need access to the development lab. Likewise, a developer does not need access to a sales forecasting application. These might be good candidates to segment into separate virtual networks.
- **Contractor network**—Network connections that allow users to access the Internet and contractor-specific applications within the enterprise network.

A virtual network may span across multiple site locations and across network domains (wireless, campus, and WAN).

Business Intent of a Virtual Network

Only the assigned user groups are allowed to enter a virtual network. Within a virtual network, users and devices can communicate with each other unless explicitly blocked by an access policy. Users across different virtual networks cannot communicate with each other. However, an exception policy can be created to allow some users to communicate across different virtual networks.

Network Rendering of a Virtual Network

By default, DNA Center has a single virtual network, and all users and endpoints belong to this virtual network. If DNA Center is integrated with Cisco Identity Services Engine (ISE), the default virtual network is populated with user groups and endpoints from Cisco ISE.

In DNA Center, the concept of virtual network is common across wireless, campus, and WAN networks. When a virtual network is created, it can be associated with sites that have any combination of wireless, wired, or WAN deployments. For example, if a site has a campus fabric deployed that includes wireless and wired devices, the virtual network creation process triggers the creation of the Service Set Identifier (SSID) and Virtual Routing and Forwarding (VRF) in the campus fabric. If the site also has WAN fabric deployed, the VRF extends from the campus to WAN as well.

During site design and initial configuration, you can add wireless devices, wired switches, and WAN routers to the site. DNA Center detects that the virtual network and the associated policies have been created for the site, and applies them to the different devices.

Guidelines and Limitations for Virtual Networks

Virtual networks have the following limitation:

- You can create only one guest virtual network.

Configure Virtual Networks


This section provides information about how to create, edit, and delete a virtual network.

Create a Virtual Network

You can create virtual network to segment your physical network into multiple logical networks.

Procedure

Step 1 From the DNA Center home page, choose **Policy > Virtual Network**.

Step 2 Click  and enter the following information:

- **Network Name**—Name of the virtual network.
- **Guest Virtual Network**—Devices that are configured with special rules, which allow guests limited access. Check this check box to configure the virtual network as a guest network. You can create only one guest virtual network.
- **Available Groups**—Scalable groups that you can choose to include in the virtual network. Drag and drop groups from the **Available Groups** area to the **Groups in the Virtual Network** area.
- **Groups in the Virtual Network**—Scalable groups that are in the virtual network. Drag and drop groups from the **Available Groups** area to the **Groups in the Virtual Network** area.

Step 3 Click **Save**.


Edit or Delete a Virtual Network

If you move a scalable group from one custom virtual network to another custom virtual network, the mappings for the scalable groups are changed. Be aware that users or devices in the group might be impacted by this change.

Procedure

Step 1 From the DNA Center home page, click **Policy > Virtual Network**.

Step 2 Do one of the following tasks:

- Select the virtual network that you want to edit, make the changes, and click **Save**. For field definitions, see [Create a Virtual Network, on page 3](#).
 - Delete the virtual network by clicking  and confirming the deletion.
-

Group-Based Access Control Policies

Group-based access control policies are Security Group Access Control Lists (SGACLs). DNA Center integrates with Cisco ISE to simplify the process of creating and maintaining SGACLs.

During the initial DNA Center and Cisco ISE integration, scalable groups and policies that are present in Cisco ISE are propagated to DNA Center and placed in the default virtual network.



Note

DNA Center does not support access control policies with logging as an action. Therefore, Cisco ISE does not propagate any such policies to DNA Center.

Depending on your organization's configuration and its access requirements and restrictions, you can segregate the scalable groups into different virtual networks to provide further segmentation.

The access contracts that you create in DNA Center define the rules that make up the group-based access control policies. They define the actions (permit/deny) performed when traffic matches a specific port or protocol and the implicit actions (permit/deny) performed when no other rules match.

After you create a group-based access control policy, DNA Center translates the policy into an SGACL, which is ultimately deployed on a device.

The following example shows the process of authentication and access control that a user experiences when logging in to the network:

- 1 A user connects to a port on a switch and provides his or her credentials.
- 2 The switch contacts Cisco ISE.
- 3 Cisco ISE authenticates the user and downloads the SGACLs to the port to which the user is connected.
- 4 The user is granted or denied access to specific users or devices (servers) based on the access granted in the SGACLs.

Prerequisite for Creating Access Control Policies

Make sure that Cisco ISE is integrated with DNA Center. Verify that the scalable groups have been propagated to DNA Center from Cisco ISE. To do this, from the DNA Center home page, choose **Policy > Virtual Network**. You should see scalable groups populated in the **Available Scalable Groups** area. If you do not see any scalable groups, check that Cisco ISE was integrated correctly. For more information, see the *Cisco Digital Network Architecture Center Installation Guide*.

Scalable Groups

Scalable groups comprise a grouping of users, end point devices, or resources that share the same access control requirements. These groups (known in Cisco ISE as security groups or SGs) are defined in the Cisco ISE. A scalable group may have as few as one item (one user, one end-point device, or one resource) in it.

Access Contracts

An access contract is a Security Group Access Control List (SGACL). It defines the set of rules that govern the network interaction between the source and destination in an access control policy.

Configure Access Control Policies

The following topics help you create and manage access-control policies.

Workflow to Configure a Group-Based Access Control Policy

Before You Begin

Make sure that you have integrated Cisco ISE with DNA Center. For more information, see [Prerequisite for Creating Access Control Policies](#), on page 4.

Procedure

	Command or Action	Purpose
Step 1	Create virtual networks. Depending on your organization's configuration and its access requirements and restrictions, you can segregate your groups into different virtual networks to provide further segmentation.	(Optional) For more information, see Create a Virtual Network , on page 3.
Step 2	Create scalable groups. After you integrate with Cisco ISE, the scalable groups that exist in ISE are propagated to DNA Center. If a scalable group that you need does not exist, you can create it.	(Optional) For more information, see Create a Scalable Group , on page 6.
Step 3	Create an access control contract. A contract defines a set of rules that dictate the action (allow or deny) that network devices perform based on traffic matching particular protocols or ports.	For more information, see Create an Access Control Contract , on page 6.
Step 4	Create a group-based access control policy. The access control policy defines the access control contract that governs traffic between source and destination scalable groups.	For information, see Create a Group-Based Access Control Policy , on page 7

Create a Scalable Group

You can access Cisco ISE through the DNA Center interface to create scalable groups. After you have added the group in Cisco ISE, it is synchronized with the DNA Center database so that you can use it in an access policy. You cannot edit scalable groups in DNA Center; you need to edit them in Cisco ISE. For more information, see [Scalable Groups](#), on page 5.

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Registry > Scalable Groups**. All of the scalable groups that have been created in Cisco ISE appear in the registry.
- Step 2** Click **Add**.
DNA Center opens a direct connection to the Cisco ISE server, where you can add the scalable group.
- Step 3** In Cisco ISE, create scalable groups (called security groups in Cisco ISE).
For more information, see the *Cisco Identity Services Engine Administrator Guide* .
- Step 4** Return to DNA Center.
-

Create an Access Control Contract

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Contracts > Access Contracts**.
- Step 2** Click **Add Contract**.
- Step 3** In the **Contract Editor** dialog box, 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 drop-down list in the **Action** column, choose either **Deny** or **Permit**.
- Step 6** From the drop-down list in the **Port/Protocol** column, choose a port or protocol.
Note If DNA Center does not have the port or protocol that you need, you can create your own by clicking **Add Port/Protocol**, configuring the fields, and clicking **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 Access Control Contract



Note If you edit a contract that is used in a policy, the policy's state changes to **MODIFIED** in the **Policy Administration** 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.

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Contracts > Access Contracts**.
- 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**.
- Note** If you made changes to a contract that is used in a policy, you need to deploy the modified policy by choosing **Policy Administration > Group-Based Access Control Policies**, checking the check box next to the policy name, and clicking **Deploy**.
- To delete the contract, click **Delete**.

Create a Group-Based Access Control Policy

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Policy Administration > Group-Based Access Control Policies**.
- Step 2** Click **Add Policy**.
- Step 3** Enter the following information:
- **Policy Name**—Name of the policy. The name can be up to 255 alphanumeric characters in length, including hyphens (-) and underscore (_) characters.
 - **Description**—Word or phrase that identifies the policy.
 - **Contract**—Rules that govern the network interaction between the source and destination scalable groups. Click **Add Contract** to choose a 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.
 - **Enable Policy**—Determines whether or not the policy is active. If it is not active, check the check box. To disable the policy, uncheck the check box. When the policy is disabled, it is saved only to DNA Center; it is not synchronized with Cisco ISE or deployed in the network.
 - **Enable Bi-directional**—Configures the relationship of the traffic flow between the source and destination scalable groups. To enable the contract for traffic flowing in both directions (from the source to the

destination and from the destination to the source), check the **Enable Bi-directional** check box. To enable the contract for traffic flowing only from the source to the destination, uncheck the **Enable Bi-directional** check box.

- Step 4** To define the source scalable groups, drag and drop the scalable groups from the **Available Security Groups** area to the **Source Scalable Groups** area.
- Step 5** To define the destination scalable groups, drag and drop scalable groups from the **Available Security Groups** area to the **Destination Scalable Groups** area.
- Step 6** Click **Save**.
-

Edit or Delete a Group-Based Access Control Policy

You can edit or delete only policies that you created in DNA Center. Policies that were imported from Cisco ISE during the DNA Center and Cisco ISE integration cannot be edited or deleted from DNA Center. You need to edit or delete these policies from Cisco ISE.



Note If you edit a policy, the policy's state changes to **MODIFIED** on the **Policy Administration** page. 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, redeploy the policy to the network.

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Policy Administration > Group-Based Access Control 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 tasks:
- To make changes, click **Edit**, make the changes, and click **Save**.

Note If you make changes to the policy, deploy the modified policy by checking the check box next to the policy name and clicking **Deploy**.
 - To delete the group, click **Delete**.
-

Traffic Copy Policies

Using 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 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

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 can be comprised of 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 that receives a copy of the traffic flow for 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.

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 the traffic analysis.

Guidelines and Limitations of Traffic Copy Policy

The traffic copy policy feature has the following limitations:

- You create up to eight traffic copy policies, 16 copy contracts, and 16 copy destinations.
- The same interface cannot be used by more than one traffic copy destination.
- 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.

Configure Traffic Copy Policies

The following topics help you create and manage traffic copy policies.

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. For information about mapping a scalable group to a switch interface, see [Configure Ports Within the Fabric Domain](#).
- 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 10.

Procedure

	Command or Action	Purpose
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 11.
Step 2	Create a traffic copy contract. The contract defines the copy destination.	For information, see Create a Traffic Copy Contract , on page 12.
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 12.

Create an IP Network Group

Procedure

-
- Step 1** From the DNA Center home page, choose **Policy > Registry > IP Network Groups**.
 - Step 2** Click **Add**.
 - Step 3** In the **Add IP Network Group** dialog box, enter a name and description for the group.
 - Step 4** In the **IP Address or IP/CIDR** field, enter an IP address or an IP address with Classless InterDomain Routing (CIDR) notation. (CIDR allows the assignment of Class C IP addresses in multiple contiguous blocks. It also allows you to add a large number of clients that exist in a subnet range by configuring a single client object.)
 - Step 5** Click **Save**.
-

Edit or Delete an IP Network Group

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Registry > 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 10.
 - To delete the group, click **Delete** and then click **Yes** to confirm.
-

Create a Traffic Copy Destination

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Contracts > 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

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Contracts > 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 group, click **Delete**.
-

Create a Traffic Copy Contract

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Contracts > Traffic Copy Contracts**.
- 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 11](#)
- Step 5** Click **Save**.
-

Edit or Delete a Traffic Copy Contract

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Contracts > Traffic Copy Contracts**.
- 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

Procedure

- Step 1** From the DNA Center home page, chooo **Policy > Policy Administration > Traffic Copy Policies**.
- Step 2** Enter the following information:
- **Policy Name**—Name of the policy.
 - **Description**—Word or phrase that identifies the policy.

- Step 3** In the **Contract** field, click **Add Contract**
 - Step 4** Click the radio button next to the contract that you want to use and then click **Save**.
 - Step 5** Drag and drop groups from the **Available Groups** area to the **Source** area.
 - Step 6** Drag and drop groups from the **Available Groups** area to the **Destination** area.
 - Step 7** Click **Save**.
-

Edit or Delete a Traffic Copy Policy

Procedure

- Step 1** From the DNA Center home page, choose **Policy > Policy Administration > 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**.
-

