Configure IP-Based Access Control Policies

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 the 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 & URL 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. For more information, see Configure Global Network Servers.
  - Device credentials, such as CLI, SNMP, HTTP, and HTTPS. For more information, see Global Device Credentials Overview.
  - IP address pools. For more information, see Configure IP Address Pools.
  - Wireless settings, such as SSIDs, wireless interfaces, and wireless radio frequency profiles. For more information, see Configure Global Wireless Settings.

Step 1 Create IP network groups.

For more information, see Create an IP Network Group, on page 3.

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 3.

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 4.

Configure Global Network Servers

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

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

Step 1 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 Click the menu icon (☰) and choose **Policy** > **IP & URL 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 Click the menu icon (☰) and choose **Policy** > **IP & URL 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 more information about field definitions, see Create an IP Network Group, on page 3. 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 Click the menu icon (☰) and choose **Policy** > **IP & URL 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 Click the menu icon (≡) and choose **Policy** > **IP & URL 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 more information about field definitions, see Create an IP-Based Access Control Contract, on page 3.

  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 & URL Based Access Control** > **IP & URL 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 the 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 the Cisco Wireless Controller 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 the status as **Modified**, indicating that it is Stale and requires a redeployment for the new configurations to be pushed to the device.

Step 1 Click the menu icon (☰) and choose **Policy** > **IP & URL Based Access Control** > **IP & URL Access Control Policies**.

Step 2 Click **Add Policy**.

Step 3 Complete the following fields:

- Policy Name - Name of the Policy.
- Description - Word or phrase that identifies the policy.
- 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 a 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 a 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 the wired devices in the site scope. Likewise, if you configure a wireless policy for an SSID, the policy is applied to all of the wireless devices with the SSID defined in the scope. For more information, see Site Scope.
- 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 is displayed: `IP-Based Access Control Policy has been created and deployed successfully`. 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 Click the menu icon (☰) and choose **Policy** > **IP & URL Based Access Control** > **IP & URL 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 more information about field definitions, see Create an IP-Based Access Control Policy, on page 4.
- 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 Click the menu icon (☰) and choose **Policy** > **IP & URL Based Access Control** > **IP & URL 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.