Configure IP-Based and URL-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 4.

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 and URL-Based Access Control Policy, on page 5.

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 From the top-left corner, click the menu icon and choose **Design** > **Network Settings** > **Network**.

Step 2 Expand the **DHCP** area to specify one or more dedicated Dynamic Host Configuration Protocol (DHCP) servers for managing the client device networking configuration.

Step 3 Check the **Add DHCP servers** check box to view the fields.

Step 4 In the **IP Address** field, enter the IP address of a DHCP server. Click the icon to add an IP address.

Note
You can click the + icon and enter both IPv4 and IPv6 addresses. Click the icon to delete an IP address.

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

Step 5 Expand the **DNS** area to configure your network's domain name, and specify Domain Name System (DNS) servers for hostname resolution.

Step 6 Check the **Set a domain name** check box to enter the domain name of a DNS server.

Step 7 Check the **Add DNS servers** check box to enter the IP address.

Note
You can click the + icon and enter both IPv4 and IPv6 addresses. Click the icon to delete an IP address.

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

Step 8 Click **Save**.

Create an IP Network Group

Step 1 From the top-left corner, 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 From the top-left corner, 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

Use this procedure to create an IP-based access contract:

Step 1 From the top-left corner, click the menu icon and choose **Policy** > **IP & URL Based Access Control** > **Access Contract**.

Step 2 Click **Add Contract**.

Step 3 In the **Name** field of the **Add Contract** slide-in pane, enter a name for the access contract.

Step 4 (Optional) In the **Description** field, enter a description for the access contract.

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

Step 6 Click **Add** to add a port or protocol.

Step 7 In the **Add Port/Protocol** dialog box, do the following:

a) From the **Action** drop-down list, choose either **Deny** or **Permit**.
b) From the **Port/Protocol** drop-down list, choose a port or protocol.
c) Click **Save**.

Step 8 If Cisco DNA Center doesn't have the port or protocol that you need, click **Create Port/Protocol** to create a port and protocol, and do the following in the **Create Port/Protocol** dialog box:

a) In the **Name** field, enter a name for the port or protocol.
b) From the drop-down list, choose a protocol: **Any**, **AHP**, **ESP**, **IGMP**, **IP**, **NOS**, **PCP**, **TDP**, **UDP**, or **TCP/UDP**.
c) In the **Port Range** field, enter the port range.
d) 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.
e) Click **Save**.

Step 9 (Optional) To include more rules in the access contract, click **Add** and repeat Step 7, on page 4.

Step 10 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 From the top-left corner, 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 4.

  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 and URL-Based Access Control Policy

You can create a post authentication access control list (ACL) for your network. The ACL can be based on IPs, URLs, or both.

Before you begin

Create an IP-Based Access Control Contract, on page 4.

Step 1 From the top-left corner, click the menu icon and choose **Policy** > **IP & URL Based Access Control** > **IP & URL Access Control Policies**.

Step 2 Click **Add Policy**.

Alternatively, instead of the first two steps, you can click the menu icon and choose **Workflows** > **Create IP & URL-Based Access Control Policy**. If an **Overview** window opens, click **Let's Do it** to start the workflow.

Step 3 In the **Policy Name and Details** window:

a) Enter a name and description for the policy.

b) Under **Select ACL Type**, check the **IP** check box, the **URL** check box, or check both the **IP** and **URL** check boxes.

Step 4 In the **Select Site and SSID** window, choose the site where you want to apply the policy.

Make sure the site is already provisioned with a nonfabric SSID.

Step 5 If you checked the **IP** check box in the **Policy Name and Details** window, do the following in the **IP Access Control List** window:

a) Click **Add New Row** and choose **Source**, **Destination**, **Contracts**, or **Direction**.

b) Click **Add**.

Step 6 If you checked the **URL** check box in the **Policy Name and Details** window, do the following in the **URL Access Control List** window:

a. Enter the URL.

b. Click the **Actions** drop-down list and choose **Permit** or **Deny**.

Step 7 In the **Summary** window, review the configuration settings. (To make any changes, click **Edit**.)

Step 8 In the **Schedule Provision** window, depending on the Visibility and Control of Configurations settings, choose an available option.

- To immediately deploy the configuration, click **Now**.
- To schedule the deployment for a later date and time, click **Later**, and define the date, time, and time zone of the deployment.
- To preview the configurations, click **Generate configuration preview**.

If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see Visibility and Control of Wireless Device Configurations.

Step 9 Click **Next**.

If you chose **Now** or **Later** in the **Schedule Provision** window, the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 10 If you chose **Generate configuration preview** in the **Schedule Provision** window, in the **Preview Configuration** window, depending on the Visibility and Control of Configurations settings, do the following:

a. Review the device configurations.

For more information, see Visibility and Control of Wireless Device Configurations.

b. When you're ready, click **Deploy** or **Submit for Approval**. If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

c. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

d. Click **Submit**.

When the configurations are successfully submitted, a success message is displayed.

If you previewed and scheduled the task for deployment, you can view the task on the **Tasks** window.

If you submitted the configurations for ITSM approval, you can view the work item's status on the **Work Items** window. If it's not approved, you must resubmit the work item for ITSM approval. When it's approved, it will be deployed at the scheduled time, which you can view on the **Tasks** window.

Edit or Delete an IP-Based and URL-Based Access Control Policy

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

Step 1 From the top-left corner, click the menu icon and choose **Policy** > **IP & URL Based Access Control** > **IP & URL Access Control Policies**.

Step 2 To edit a policy, click the name of the policy that you want to edit, make the required changes, and click **Save & Schedule**. For more information, see Create an IP-Based and URL-Based Access Control Policy, on page 5.

Step 3 To delete a policy, check the check box next to the policy that you want to delete and click **Delete**.