



CHAPTER 17

Managing Authorization Policies and Profiles

This chapter introduces the authorization policies that are used when creating the authorization profiles in the Cisco Identity Services Engine (ISE). Using the ISE user interface menus, tabs, and options, you can create an authorization policy, which form the basis of authorization profiles.

An authorization policy is where an overall authorization policy is generated, which is composed of authorization rules. Authorization rules have three elements: name, attributes, and permissions. It is the permissions function that maps to an authorization profile.

This chapter provides a description of authorization policies and provides example procedures for the following authorization policy-related tasks:

- [Understanding Authorization Policies, page 17-1](#)
- [Cisco ISE Authorization Policies and Profiles, page 17-5](#)
- [Configuring Authorization Policies, page 17-14](#)
- [Configuring Policy Elements Conditions, page 17-17](#)
- [Configuring Permissions for Authorization Profiles, page 17-27](#)

Understanding Authorization Policies

Authorization policies are a component of the Cisco ISE network authorization service that allows you to define authorization policies and configure authorization profiles for specific users and groups of users that access your network resources.

Network authorization policies associate rules with specific user and group identities to create the corresponding profiles. Whenever these rules match the configured attributes, the corresponding authorization profile that grants permission is returned by the policy, network access is authorized accordingly.

Authorization policies can contain conditional requirements that combine one or more identity groups using a compound condition that includes authorization checks that can return one or more authorization profiles. In addition, conditional requirements can exist apart from the use of a specific identity group (such as in using the default “Any”). Cisco ISE is an attribute-based policy system, with identity groups being one of the many important attributes.

For example, authorization profiles can include a range of permissions that are contained in the following types:

- Standard profiles
- Exception profiles
- Device-based profiles

Profiles consist of attributes chosen from a set of resources, which are stored in a dictionary and these are returned when the compound condition for the specific authorization policy matches. Because authorization policies can include compound conditions mapping to a single network service rule, these can also include a list of authorization checks.

For simple scenarios, all authorization checks are made using the AND Boolean operator within the rule. For advanced scenarios, any type of authorization verification expression can be used, but all these authorization verifications must comply with the authorization profiles to be returned. Authorization verifications typically comprise one or more conditions, including a user-defined name that can be added to a library, which can then be reused by other authorization policies.

For more information:

- For information about policy terminology, see [Understanding Authorization Policy Terminology, page 17-3](#).
- For policy and profile information, see [Cisco ISE Authorization Policies and Profiles, page 17-5](#).
- For information about configuring policies, see [Configuring Authorization Policies, page 17-14](#).
- For information about configuring policy elements conditions, see [Configuring Policy Elements Conditions, page 17-17](#).
- For information about configuring permissions for profiles, see [Configuring Permissions for Authorization Profiles, page 17-27](#).
- For information about configuring permissions for DACLs, see [Configuring Permissions for Downloadable ACLs, page 17-32](#).

Understanding Authorization Policy Terminology

Table 17-1 defines and describes basic terminology for Cisco ISE authorization policies and profiles.

Table 17-1 *Cisco ISE Basic Authorization Policy and Profile Terminology*

Term	Description
Network Authorization	Authorization is an important requirement to ensure which users can access the Cisco ISE network and its resources. Network authorization controls user access to the network and its resources and what each user can do on the system with those resources. The Cisco ISE network defines sets of permissions that authorize read, write, and execute privileges. Cisco ISE lets you create a number of different authorization policies to suit your network needs. This release supports only Remote Authentication Dial-In User Service (RADIUS) access to the Cisco ISE network and its resources.
Policy Elements	<p>Policy elements are components that define the authorization policy. The policy elements are as follows:</p> <ul style="list-style-type: none">• Rule name• Identity groups• Condition(s)• Permissions <p>These policy elements are referenced when you create policy rules and your choice of conditions and attributes can create specific types of authorization profiles.</p>
Authorization Profile	<p>An authorization profile acts as a container where a number of specific permissions allow access to a set of network services. The authorization profile is where you define a set of permissions to be granted for a network access request and can include:</p> <ul style="list-style-type: none">• A profile name• A profile description• An associated DACL• An associated VLAN• An associated SGACL• Any number of other dictionary-based attributes

Table 17-1 *Cisco ISE Basic Authorization Policy and Profile Terminology (continued)*

Term	Description
Authorization Policy	<p>An authorization policy can consist of a single rule or a set of rules that are user-defined. These rules act to create a specific policy. For example, a standard policy can include the rule name using an If-Then convention that links a value entered for identity groups with specific condition(s) or attributes to produce a specific set of permissions that create a unique authorization profile. There are two authorization policy options you can set:</p> <ul style="list-style-type: none"> • First Matched Rules Apply • Multiple Matched Rule Applies <p>These two options direct Cisco ISE to use either the first matched or the multiple matched rule type listed in the standard policy table when it matches the user's set of permissions. These are the two types of authorization policies that you can configure:</p> <ul style="list-style-type: none"> • Standard • Exception <p>Standard policies are policies created to remain in effect for long periods of time, to apply to a larger group of users or devices or groups, and allow access to specific or all network endpoints. Standard policies are intended to be stable and apply to a large groups of users, devices, and groups that share a common set of privileges.</p> <p>Standard policies can be used as templates in which you modify the original values to serve the needs of a specific identity group, using specific conditions or permissions to create another type of standard policy to meet the needs of new divisions, or groups of users, devices, or groups in your network.</p> <p>By contrast, exception policies are appropriately named because this type of policy acts as an exception to the standard policies. Exception policies are intended for authorizing limited access that is based on a variety of factors (short-term policy duration, specific types of network devices, network endpoints or groups, or the need to meet special conditions or permissions or an immediate requirement).</p> <p>Exception policies are created to meet an immediate or short-term need such as authorizing a limited number of users, devices, or groups to access network resources. An exception policy lets you create a specific set of customized values for an identity group, condition, or permission that are tailored for one user or a subset of users. This allows you to create different or customized policies to meet your corporate, group, or network needs.</p>
Access Control Lists	<p>An ACL in the Cisco ISE system is a list of permissions attached to a specific object or network resource. An ACL specifies which users or groups are granted access to an object, as well as what operations are allowed on a given object or network resource. Each entry in a typical ACL specifies a subject and an operation or provides the state (for example, Permit or Deny). A DACL represents a downloadable ACL.</p>

Cisco ISE Authorization Policies and Profiles

This section describes the authorization policies and authorization profiles used in Cisco ISE. Using the Cisco ISE user interface (Authorization Policy and Authorization Profile pages), you can manage all of your authorization policies and profiles by performing the following policy management operations:

- Displaying existing policies
- Creating new policies
- Duplicating existing policies (for use as templates that you can modify to create new policies)
- Modifying existing policies (create customized policies by changing desired rules or permissions)
- Deleting existing policies

For more information:

Descriptions of the components and elements in the Authorization Policy and Authorization Profile pages that you use to create policies and profiles are in the following topics:

- For information about the user interface elements you can use to create authorization policies, see [Authorization Policy Page, page 17-5](#) and [Authorization Policy and Profile User Interface, page 17-10](#).
- For information about the user interface elements you can use to create authorization profiles, see [Authorization Profile Page, page 17-8](#) and [Authorization Policy and Profile User Interface, page 17-10](#).
- For guidelines about creating authorization policies and profiles, see [Authorization Policy and Profile Guidelines, page 17-9](#).

Next Steps:

To configure authorization policies and profiles, see the following topics:

- [Configuring Authorization Policies, page 17-14](#)
- [Configuring Policy Elements Conditions, page 17-17](#)
- [Configuring Permissions for Authorization Profiles, page 17-27](#)
- [Configuring Permissions for Downloadable ACLs, page 17-32](#)

Authorization Policy Page

To display the Authorization Policy page, choose **Policy > Authorization**. The Authorization Policy page is your starting point for creating the following types of Cisco ISE authorization policies:

- **Exception:** Exception policies are, like the name implies, exceptions to a standard policy, which is designed for use by large numbers of users or groups, or to remain in effect for an extended period. Exception policies are instead designed for a custom purpose, for a short period of time, or for use by one or more users or a group for a specific purpose.
- **Standard:** Standard policies are those that you create for use for an extended period of time, by large numbers of users or groups, and that provide a standard set of permissions and rules tailored for standard network needs.

**Note**

The Cisco ISE user interface provides a Status indicator for each authorization policy that can be set to display one of the three following states: Enabled, Disabled, or Monitor Only.

When managing authorization policies, you can display existing exception or standard policies, or create, modify, or delete these policies to meet specific user or group requirements in your network. To create a new Exception or Standard authorization policy, you must complete the following sequence of tasks to configure these following four policy element values:

- Rule Name—This is where you define a unique name for the authorization policy.
- Identity Groups—This is where you select an existing identity group from a list of available choices.
- Other Conditions—This is where you select a simple condition (or a compound condition) from existing Condition Name dictionary choices (or you can select an attribute from existing Attribute dictionary choices).
- Permissions—This is where you select a profile from an existing Profiles dictionary choices.

You can create a new authorization policy by choosing and combining values for these four policy elements using the Cisco ISE user interface menus and options in the Authorization Policy page. Once you have selected your policy choices, click **Done**.

The policies that you create appear in the Authorization Policy page in a read-only mode.

You can click the **Edit** link in the authorization policy to edit the policy rules. After you have modified your policy choices, click **Done**.

When you add a new policy or edit an existing policy, a pencil icon appears next to the rule name. The pencil icon indicates that there are unsaved changes to the authorization policy. You must click **Save** to save your changes in the Cisco ISE system database.

Authorization policy rules are grouped by rank in the list, and you can change the position of rules in this ranked list by using the following options:

- Insert a new policy above or below a highlighted or selected policy.
- Insert a duplicate of a selected policy above or below a highlighted or selected policy.
- Delete a selected policy.

You can also drag and drop rules to change their rank in the list.

When you create a new authorization policy, it is populated with default values for all of the required policy fields. You will be prompted to do the following:

- To modify an existing authorization policy, choose any policy element you want to change, modify its value, and click **Save** to create the modified policy in the Cisco ISE system database.
- To delete an existing authorization policy, select it in the displayed list, and click **Delete** to remove this policy from the Cisco ISE system database. Normally, you would delete only those authorization policies that you no longer intend to support or use as templates for future policies.

**Note**

When you delete an existing authorization policy, Cisco ISE prompts you to confirm the deletion before the selected policy is deleted from the Cisco ISE system database. Any changes that you make to a policy without clicking **Save** are not sent to or registered in the Cisco ISE system database.

- To duplicate an existing policy, select its intended position (above or below) in the ranked list. Cisco ISE copies all of the policy values from the existing policy, and creates an identical policy except that it now has a different policy ID (Cisco ISE requires each policy ID to be unique). By starting with a duplicate of an existing policy, you can use it as a template, modify selected fields or attributes, and create a new authorization policy.

**Note**

You can set each exception or standard authorization policy that you create as Enabled, Disabled, or **Monitor Only**. To do this, check the green check box adjacent to the Rule Name column for each entry.

- To reuse a valid attribute when creating authorization policy conditions, select it from a dictionary that contains the supported attributes. For example, Cisco ISE provides an attribute named `AuthenticationIdentityStore`, which is located in the `NetworkAccess` dictionary. This attribute identifies the last identity source that was accessed during the authentication of a user:
 - When a single identity source is used during authentication, this attribute includes the name of the identity store to which the authentication succeeded.
 - When an identity source sequence is during authentication, this attribute includes the name of the last identity source accessed.

You can use the `AuthenticationStatus` attribute in combination with the `AuthenticationIdentityStore` attribute to define a condition that identifies the identity source to which a user has successfully been authenticated. For example, to check for the a Condition where a user authenticated using an LDAP directory (LDAP13) in the authorization policy, you can define the following reusable condition:

```
If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```

**Note**

The `AuthenticationIdentityStore` represents a text field that allows you to enter data for the condition. Ensure that you enter or copy the name correctly into this field. If the name of the identity source changes, you must ensure to modify this condition to match the change to the identity source.

- To define authorization conditions that are based on an endpoint identity group that has been previously authenticated, Cisco ISE supports authorization that was defined during endpoint identity group 802.1X authentication status. When Cisco ISE performs 802.1X authentication, it extracts the MAC address from the “Calling-Station-ID” field in the RADIUS request and uses this value to look up and populate the session cache for the device's endpoint identity group (defined as an `endpointIDgroup` attribute).

This process makes the `endpointIDgroup` attribute available for use in creating authorization policy conditions, and allows you to define an authorization policy based on endpoint identity group information using this attribute, in addition to user information.

The condition for the endpoint identity group can be defined in the ID Groups column of the authorization policy configuration page. Conditions that are based on user-related information need to be defined in the “Other Conditions” section of the authorization policy. If user information is based on internal user attributes, then use the ID Group attribute in the internal user dictionary. For example, you can enter the full value path in the identity group using a value like “User Identity Group:Employee:US”.

For more information:

- For more information on endpoint identity groups, see [Endpoint Identity Groups, page 4-71](#).

Authorization Policies and Supported Dictionaries

For simple condition-based policy scenarios, authorization checks are made using the AND Boolean operator within the rule. For compound condition-based policies, any type of authorization verification expression can be used. However, for both authorization policy types the verification must comply with the authorization profiles to be returned.

Verifications typically include one (or more) condition(s) that include a user-defined name that can then be added to a library and reused by other policies. You define conditions using the attributes from the Cisco ISE dictionary, which supports the following dictionaries:

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft
- RADIUS

where RADIUS is a system-defined dictionary and Airespace, Cisco, Cisco-BBSM, Cisco-VPN3000, and Microsoft are RADIUS-vendor dictionaries. See the [“Dictionaries and Dictionary Attributes” section on page 7-1](#) for more information on Cisco ISE dictionaries.

Authorization Profile Page

To display the Authorization Profile page, you start from the Policy tab (choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**). The Authorization Profile page is your starting point for managing the Cisco ISE standard authorization profiles. This is where you can display any existing profiles, create new profiles, or modify or delete existing authorization profiles to meet your specific user or group network needs.

To create a new authorization profile, you must define the profile name and access type. All other profile elements are optional. To configure values for these other profile elements, use the text fields, drop-down lists, and check boxes in the following Authorization Profile page columns:

- **Authorization Profile**

- Name
- Description
- Access Type

**Note**

The only profile elements required to create a new authorization profile are the profile Name and Access Type, which are marked with an asterisk (*). All other profile elements are optional elements.

- **Common Tasks**

This is where you can configure settings that support commonly-used attributes.

- DACL Name
- VLAN
- Voice Domain Permission

- Posture Discovery
- Centralized Web Authentication
- Auto SmartPort
- Filter-ID
- Reauthentication
- MACSec Policy
- NEAT
- Web Authentication (Local Web Auth)
- Wireless LAN Controller (WLC)
- ASA VPN

**Note**

For details about Common Task settings, see [Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-28](#).

- **Advanced Attributes Settings**

This is where you can configure advanced attributes settings using attributes contained in dictionaries you can access from the drop-down list.

- **Attributes Details**

This is where the attributes you configure in the Common Settings and Advanced Attribute group boxes are displayed.

After you have selected or entered your authorization profile choices, click **Submit** to create a new authorization profile.

To modify an existing authorization profile, check the check box corresponding to the profile you want to change, modify the profile settings as desired, and click **Save** to create a new modified authorization profile. Any changes that you make to a profile without clicking **Save** are not sent to or registered in the Cisco ISE system database.

To delete an existing authorization profile, check the check box corresponding to the profile you want to delete, and click **Delete**. For the procedures explaining how to create, modify, or delete authorization profiles, see [Configuring Permissions for Authorization Profiles, page 17-27](#).

Authorization Policy and Profile Guidelines

Observe the following guidelines when managing or administering authorization policies and profiles:

- Rule Names you create must use only the following supported character set:
 - Symbols: plus (+), hyphen (-), underscore (_), period (.), and a space ().
 - Alphabetic characters: A-Z and a-z.
 - Numeric characters: 0-9.
- Identity Groups default to “Any” (you can use this global default to apply to all users).
- Conditions allow you to set one or more policy values. However, conditions are optional and are not required to create an authorization policy. These are the two methods for creating conditions:
 - Choose an existing condition or attribute from a corresponding dictionary of choices.

- Create a custom condition that allows you to select a suggested value or use a text box to enter a custom value.
- Condition names you create must use only the following supported character set:
 - Symbols: hyphen (-), underscore (_), and period (.).
 - Alphabetic characters: A-Z and a-z.
 - Numeric characters: 0-9.
- Permissions are important when choosing an authorization profile to use for a policy. A permission can grant access to specific resources or allow you to perform specific tasks. For example, if a user belongs to a specific identity group (such as Device Admins), and the user meets the defined conditions (such as a site in Boston), then this user is granted the permissions associated with that group (such as access to a specific set of network resources or permission to perform a specific operation on a device).

**Note**

Make sure that you click **Save** to save the new or modified policy or profile in the Cisco ISE database.

Authorization Policy and Profile User Interface

To manage your authorization policies and authorization profiles, use the controls within each of the corresponding user interface pages. Use the following Cisco ISE user interface controls and elements needed to perform the following tasks:

- To configure an authorization policy—choose **Policy > Authorization > Standard** (or **Exception**)
- To configure an authorization profile—choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**

Authorization Policy, Rule, and Profile Configuration Defaults

The Cisco ISE software comes installed with a number of preinstalled default conditions, rules, and profiles that provide common settings that make it easier for you to create the rules and policies required in Cisco ISE authorization policies and profiles. These built-in configuration defaults contain specified values that are described in [Table 17-2](#).

Table 17-2 Authorization Policy, Profile, and Rule Configuration Defaults

Name	Path in the UI	Description	Additional Information
Authorization Policy Configuration Defaults			
Default Compound Conditions for Authorization Policies	Policy > Policy Elements > Conditions > Authorization	These are preinstalled configuration defaults for conditions, rules, and profiles to be used in authorization policies.	You can use the related attributes for creating authorization policies: <ul style="list-style-type: none">• Wired 802.1x• Wired MAB• Wireless 802.1x• Catalyst Switch Local Web authentication• WLC Web authentication

Table 17-2 Authorization Policy, Profile, and Rule Configuration Defaults (continued)

Name	Path in the UI	Description	Additional Information
Authorization Policy Configuration Defaults			
Wired 802.1X Compound Condition	Policy > Policy Elements > Conditions > Authorization > Compound Conditions	This compound condition checks for the following attributes and values: <ul style="list-style-type: none"> RADIUS:Service-Type = Framed RADIUS:NAS-Port-Type = Ethernet 	This compound condition is used in the Wired 802.1X authorization policy. Any request that matches the criteria specified in this policy would be evaluated based on the Wired 802.1X authorization policy.
Wired MAB Compound Condition	Policy > Policy Elements > Conditions > Authorization > Compound Conditions	This compound condition checks for the following attributes and values: <ul style="list-style-type: none"> RADIUS:Service-Type = Call-Check RADIUS:NAS-Port-Type = Ethernet 	This compound condition is used in the Wired MAB authorization policy. Any request that matches the criteria specified in this policy would be evaluated based on the Wired MAB authorization policy.
Wireless 802.1X Compound Condition	Policy > Policy Elements > Conditions > Authorization > Compound Conditions	This compound condition checks for the following attributes and values: <ul style="list-style-type: none"> RADIUS:Service-Type = Framed RADIUS:NAS-Port-Type = Wireless-IEEE802.11 	This compound condition is used in the Wireless 802.1X authorization policy. Any request that matches the criteria specified in this policy would be evaluated based on the Wireless 802.1X authorization policy.
Catalyst Switch Local Web Authentication Compound Condition	Policy > Policy Elements > Conditions > Authorization > Compound Conditions	This compound condition checks for the following attributes and values: <ul style="list-style-type: none"> RADIUS:Service-Type = Outbound RADIUS:NAS-Port-Type = Ethernet 	To use this compound condition, you must create an authorization policy that would check for this condition.
Wireless Lan Controller (WLC) Local Web Authentication Compound Condition	Policy > Policy Elements > Conditions > Authorization > Compound Conditions	This compound condition checks for the following attributes and values: <ul style="list-style-type: none"> RADIUS:Service-Type = Outbound RADIUS:NAS-Port-Type = Wireless-IEEE802.11 	To use this compound condition, you must create an authorization policy that would check for this condition.

Table 17-2 Authorization Policy, Profile, and Rule Configuration Defaults (continued)

Name	Path in the UI	Description	Additional Information
Authorization Rule Configuration Defaults			
Wireless Black List Default Authorization Rule	Policy > Authorization Policy	<p>This authorization policy uses a configuration default rule with the following values:</p> <ul style="list-style-type: none"> • Rule Name: Wireless Black List Default • Endpoint Identity Group: Blacklist • Conditions: Wireless_802.1X • Permissions/Authorization Profile: Blackhole_Wireless_Access 	This default rule is designed to appropriately provision “lost” user devices until they are either removed from the system or “reinstated.”
Profiled Cisco IP Phones Authorization Rule	Policy > Authorization Policy	<p>This authorization policy uses a configuration default rule with the following values:</p> <ul style="list-style-type: none"> • Rule Name: Profiled Cisco IP Phones • Endpoint Identity Group: Cisco-IP-Phones • Conditions: Any • Permissions/Authorization Profile: Cisco_IP_Phones 	This default rule uses Cisco IP Phones as its default endpoint identity group and the values listed in this table.
Default Authorization Rule	Policy > Authorization Policy	<p>This authorization policy uses a configuration default rule with the following values:</p> <ul style="list-style-type: none"> • Rule Name: Default • Endpoint Identity Group: Any • Conditions: Any • Authorization Profile: PermitAccess 	This default rule uses “any” as its default endpoint identity group and the values listed in this table.
Authorization Profile Configuration Defaults			
Blackhole_Wireless_Access	Policy > Policy Elements > Results > Authorization Profiles > Blackhole_Wireless_Access	<p>This authorization profile rejects access to devices that are blacklisted. All blacklisted devices are redirected to the following URL:</p> <p>url-redirect=https://ip:port/mydevices/blackhole.jsp</p>	This default authorization profile is applied for all endpoints that are declared as “lost” in the My Devices Portal.

Table 17-2 Authorization Policy, Profile, and Rule Configuration Defaults (continued)

Name	Path in the UI	Description	Additional Information
Cisco_IP_Phones	Policy > Policy Elements > Results > Authorization Profiles > Cisco_IP_Phones	<p>This authorization profiles uses a configuration default profile with the following values:</p> <ul style="list-style-type: none"> Name: Cisco IP Phones DACL: PERMIT_ALL_TRAFFIC VSA: cisco:av-pair:device-traffic-class=voice <p>This profile will evaluate requests that match the criteria specified in this profile.</p>	This default authorization profile uses the DACL and vendor-specific attribute (VSA) to authorize all “voice” traffic (PERMIT_ALL_TRAFFIC).

Configuring Authorization Policies

The Authorization Policy page lets you display, create, duplicate/modify, or delete authorization policies. The following topics provide procedures for performing these tasks:

- [Displaying Existing Authorization Policies and Setting the Matched Rule Policy, page 17-14](#)
- [Creating a New Authorization Policy, page 17-15](#)
- [Duplicating and Modifying an Existing Authorization Policy, page 17-16](#)
- [Deleting an Existing Authorization Policy, page 17-17](#)



Note

The following authorization policy profile sections reference example actions directed at a standard authorization policy. You can follow the same process for managing an exception authorization policy.

Displaying Existing Authorization Policies and Setting the Matched Rule Policy

Use this procedure to display all existing Exception or Standard authorization policies, choose the matched rule policy, or view the policy-based choices that can be made.

To display existing authorization policies and set the matched rule policy, complete the following steps:

Step 1 Choose **Policy > Authorization**.

The Authorization Policy page appears listing all existing configured authorization policies, including three default policies entitled “Default,” “Profiled Cisco IP Phones,” and “Black List Default” that you should see the first time you access this page.

Step 2 To set the matched rule policy for authorization policies, under Authorization Profiles click the drop-down arrow, and choose **First Matched Rule Applies** or **Multiple Matched Rule Applies**.

Creating a New Authorization Policy

Use this procedure to create a new authorization policy.

To create a new authorization policy, complete the following steps:

-
- Step 1** Choose **Policy > Authorization > Standard**.
- Step 2** Click the **action** icon (down arrow on the far-right) and select either **Insert New Rule Above** or **Insert New Rule Below**.
- A new policy entry appears in the position you designated in the Standard panel of the Authorization Policy page.
- Step 3** Enter values for the following authorization policy fields:
- Rule Name—You must define a rule name for the new policy.
 - Conditions (identity groups and other conditions)—Choose the types of conditions or attributes for the identity group associated with the policy. Click **+** next to Condition(s) to display the following list of condition and attribute choices that you can configure:
 - Click **+** (“plus” sign) next to the word “Any” to display a drop-down list of group choices, or choose **Any** for the policy for this identity group to include all users.
 - Choose a Condition Name option from the drop-down list (**Simple Conditions**, **Compound Conditions**, or **Time and Date Conditions**) as needed.
 - Choose one of the Attribute options as needed. This displays a list of dictionaries that contain specific attributes related to the dictionary type.

When you select an attribute, you can specify “Equals,” “Not Equals,” “Matches,” “Starts With,” or “Not Starts With” using a drop-down list of operator options, and select an “AND” or “OR” directive using a drop-down directive option.



Note Not all attributes you select will include the “Equals,” “Not Equals,” “Matches,” “Starts With,” or “Not Starts With” operator options.



Note The “Matches” operator supports and uses regular expressions (REGEX) not wildcards.

Example 1a: Equals—You select the RADIUS dictionary, and you select the Error-Cause value, which displays RADIUS:Error-Cause in the Expression field. You select the Equals operator in the second field (drop-down list). In the third field (drop-down list), you select the value that you want the RADIUS:Error-Cause to equal (for example, Unsupported Service), or choose another attribute type from the existing library using the drop-down arrow to the right of this field. This condition is configured as follows: RADIUS:Error-Cause EQUALS Unsupported Service.

Example 1b: Equals—You select the CERTIFICATE dictionary, and you select the Subject value, which displays CERTIFICATE:Subject in the Expression field. You select the Equals operator in the second field (drop-down list). In the third field (text field), you must configure the value properly that you want the CERTIFICATE:Subject to equal (for example, a username such as User123), or choose another attribute type from the existing library using the drop-down arrow to the right of this field. To achieve a match, this condition must be configured using the prefix of “cn=” as follows: CERTIFICATE:Subject EQUALS cn=User123.

Example 1c: Equals—You select the CERTIFICATE dictionary, and you select the Subject Alternative Name value, which displays CERTIFICATE:Subject Alternative Name in the Expression field. You select the Equals operator in the second field (drop-down list). In the third field (text field), you must configure the value properly that you want the CERTIFICATE:Subject Alternative Name to equal (for example, a username such as User123@acme.com), or choose another attribute type from the existing library using the drop-down arrow to the right of this field. To achieve a match, this condition must be configured as follows: CERTIFICATE:Subject Alternative Name EQUALS User123@acme.com.

Example 2: Not Equals—You select the RADIUS dictionary, and you select the User-Name value, which displays RADIUS:User-Name in the Expression field. You select the Not Equals operator in the second field (drop-down list). In the third field (text box), you enter the value that you want the RADIUS:User-Name to not equal (for example, guest113), or choose another attribute type from the existing library using the drop-down arrow to the right of this field. This condition is configured as: RADIUS:User-Name NOT_EQUALS guest113.

Example 3: Matches—You select the CERTIFICATE dictionary, and you select the Organization value, which displays CERTIFICATE:Organization in the Expression field. You select the Matches operator in the second field (drop-down list). In the third field (text box), enter a REGEX value to match Organization value, or choose another attribute type from the existing library using the drop-down arrow to the right of this field. The following are some common options for “Matches”:

- ‘Starts with’—for example, using the REGEX value of `^(Acme).*`—this condition is configured as CERTIFICATE:Organization MATCHES ‘Acme’ (any match with a condition that starts with “Acme”).
- ‘Ends with’—for example, using the REGEX value of `.*(mktg)$`—this condition is configured as CERTIFICATE:Organization MATCHES ‘mktg’ (any match with a condition that ends with “mktg”).
- ‘Contains’—for example, using the REGEX value of `.*(1234).*`—this condition is configured as CERTIFICATE:Organization MATCHES ‘1234’ (any match with a condition that contains “1234”, such as Eng1234, 1234Dev, and Corp1234Mktg).
- ‘Does not Contain’—for example, using the REGEX value of `.*((?!1234).)*$/s`—this condition is configured as CERTIFICATE:Organization MATCHES `.*((?!1234).)*$/s` (any match with a condition that does not contain “1234”).
- ‘Does not start with’—for example, using the REGEX value of `^(?!LDAP).*`—this condition is configured as CERTIFICATE:Organization MATCHES ‘LDAP’ (any match with a condition that does not start with “LDAP”, such as usLDAP or CorpLDAPmktg).
- Permissions—Choose the authorization profile to associate with this authorization policy.
 - Click **+** next to Permissions to display a drop-down list of profile choices. Select a profile option (for example, the Standard profile offers two default choices: DenyAccess or PermitAccess).

d. Click **Done**.

Step 4 Click **Save** to save your changes to the Cisco ISE system database and create this new authorization policy.

Duplicating and Modifying an Existing Authorization Policy

Use this procedure to duplicate an existing authorization policy and modify it to create a new policy based upon its initial set of existing values.

To duplicate and modify an existing authorization policy, complete the following steps:

-
- Step 1** Choose **Policy > Authorization > Standard**.
- Step 2** To choose the authorization policy you want to duplicate and modify, click the action icon and click **Duplicate above** or **Duplicate below**.
A duplicate policy entry appears in the Standard panel of the Authorization Policy page (either above or below the existing policy that you selected).
- Step 3** Enter a new name for this policy in the Rule Name field.
- Step 4** Modify the desired values to create the new authorization policy in the corresponding fields by selecting the desired set of option choices.
- Step 5** Click **Save** to save your changes to the Cisco ISE database, which creates this new authorization policy.
-

Deleting an Existing Authorization Policy

Use this procedure to delete an existing authorization policy and remove it from the Cisco ISE database.

To delete an existing authorization policy, complete the following steps:

-
- Step 1** Choose **Policy > Authorization > Standard**.
- Step 2** To select the authorization policy you want to delete, click **action** (icon) for that policy row and choose **Delete**.
A confirmation dialog appears in the Standard panel of the Authorization Policy page.
- Step 3** Click **Delete** to confirm that you want to delete the authorization policy.
- Step 4** Click **Save** to save your changes to the Cisco ISE system database and delete this authorization policy.



Note

If you do not click **Save**, you will only delete the authorization policy locally.

Configuring Policy Elements Conditions

Cisco ISE provides a way to create conditions that are individual, reusable policy elements that can be referred from other rule-based policies. You can create conditions from within the policy pages and as separate policy elements to be reused by other types of Cisco ISE policies such as Sponsor group or Client Provisioning policies. Whenever a policy is being evaluated, the conditions that comprise it are evaluated first.



Note

Under **Policy > Policy Elements > Conditions**, the initial Conditions page displays the following policy element condition options: Authentication, Authorization, Profiling, Posture, Guest, and Common.

Typically, policies consist of rules, where each rule consists of conditions that when met allow actions to be performed (such as access to network resources). Rule-based conditions form the basis of policies, the sets of rules used when evaluating requests.

Simple conditions consist of an attribute, an operator, and a value. You can create simple conditions from within the policy pages and also as separate policy elements that can be reused in policies. Cisco ISE allows you to create, edit, and delete simple authorization conditions. When authorized, Cisco ISE returns a permission.

Compound conditions are typically made up of two or more simple conditions. You can create compound conditions as reusable objects from within the policy creation page or from the Conditions page. This page lists all the compound conditions that you have defined in Cisco ISE.

Simple Conditions

Prerequisites:

- Before you begin any procedures, you should have a basic understanding of the rule-based authorization policies, the basic building blocks of identity groups, conditions, and permissions, and how these are used in the Cisco ISE user interface. See [Understanding Authorization Policy Terminology, page 17-3](#), [Authorization Policy Page, page 17-5](#), and [Configuring Policy Elements Conditions, page 17-17](#) for more information.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedures, you must have one of the following roles assigned: Super Admin or Policy Admin. See [Table 4-11](#) for more information on the various administrative roles and the privileges associated with each of them.

Simple Condition Format

This type uses the form *attribute operand value*. Rule-based conditions are essentially a comparison of values (the attribute with its value), and these can be saved and reused in other rule-based policies.

Simple conditions take the format of A operand B, where A can be any attribute from a Cisco ISE dictionary and B can be one of the values that attribute A can take. For example, simple conditions can take the following form:

- Network Access:Protocol Equals RADIUS.

Compound Conditions

Prerequisites:

- Before you begin any procedures, you should have a basic understanding of rule-based authorization policies, the basic building blocks of identity groups, conditions, and permissions, and how they are represented in the Cisco ISE user interface. See [Understanding Authorization Policy Terminology, page 17-3](#), [Authorization Policy Page, page 17-5](#), and [Configuring Policy Elements Conditions, page 17-17](#) for more information.
- Cisco ISE comes with predefined compound conditions for some of the most common use cases. See [Authorization Policy, Rule, and Profile Configuration Defaults, page 17-11](#) for more information on these predefined conditions. You can edit these predefined conditions to suit your requirements.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have any one of the following roles assigned: Super Admin or Policy Admin. See [Table 4-11](#) for more information on the various administrative roles and the privileges associated with each of them.

Compound Condition Format

This condition type comprises one or more simple conditions that use an AND or OR relationship. These are built on top of simple conditions and can be saved and reused in other rule-based policies. Compound conditions can take any of the following forms:

- (X operand Y) AND (A operand B) AND (X operand Z) AND ... (so on)
- (X operand Y) OR (A operand B) OR (X operand Z) OR ... (so on)

where X and A are attributes from the Cisco ISE dictionary and can include username and device type. For example, compound conditions can take the following form:

- DEVICE:Model Name Matches Catalyst6K AND Network Access:Use Case Equals Host Lookup.

Configuring Authorization Policy Conditions

Use the Policy Elements Conditions page to display, create, modify, delete, duplicate, and search authorization policy element conditions. The following topics provide procedures for performing these tasks:

- [Displaying Existing Authorization Policy Element Conditions, page 17-19](#)
- [Creating New Authorization Policy Element Conditions, page 17-19](#)
- [Modifying Existing Authorization Policy Element Conditions, page 17-20](#)
- [Duplicating Existing Authorization Policy Element Conditions, page 17-21](#)
- [Deleting Existing Authorization Policy Element Conditions, page 17-22](#)
- [Searching Existing Authorization Policy Element Conditions, page 17-22](#)



Note

For more information about simple and compound conditions, see [Configuring Policy Elements Conditions, page 17-17](#).

Displaying Existing Authorization Policy Element Conditions

Use this procedure to display all existing authorization policy element conditions (both simple or compound).

To display existing authorization policy element conditions, choose **Policy > Policy Elements > Conditions > Authorization > Simple Conditions** (or **Compound Conditions**).

The Conditions page appears listing all of the existing configured authorization policies (which correspond to the condition type you selected, simple or compound).

Creating New Authorization Policy Element Conditions

Use this procedure to create new authorization policy element conditions (simple or compound).

To create new authorization policy element conditions, complete the following steps:

- Step 1** Choose **Policy > Policy Elements > Conditions > Authorization > Simple Conditions** (or **Compound Conditions**).

The Conditions page appears listing all existing configured authorization policy element conditions.

Step 2 To create a new simple condition, click **Create**.

The Simple Conditions page appears.

Step 3 Enter values in the following fields to define a new simple condition:

- Name—Enter the name of the simple condition.
- Description—Enter the description of the simple condition.
- Attribute—Click to choose a dictionary from the drop-down list of dictionary options, and choose an attribute from the corresponding attribute choices.
- Operator—Enter **Equals** or **Not Equals**.
- Value—Enter a value that matches the selected attribute.

Step 4 Click **Submit** to save your changes to the Cisco ISE database and create this authorization condition.



Note

The Name, Attribute, Operator, and Value fields in simple conditions are required and are marked with an asterisk (*).



Note

Compound conditions consist of one or more simple conditions that include different “Equals,” “Not Equals,” “Matches,” “Starts With,” or “Not Starts With” operators, and “AND” and “OR” directives that are built upon existing simple conditions. The procedure for creating a new compound condition follows the same steps and processes that are used to create a simple condition. For more details about compound conditions, see [Compound Conditions](#), page 17-18.



Note

The “Matches” operator supports and uses regular expressions (REGEX) not wildcards.

Modifying Existing Authorization Policy Element Conditions

Use this procedure to modify existing authorization policy element conditions (simple or compound).

To modify existing authorization policy element conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Authorization > Simple Conditions** (or **Compound Conditions**).

The Conditions page appears listing all existing configured authorization policy element conditions.

Step 2 To edit an existing condition, check the check box corresponding to the condition you want to modify, and click **Edit**.

The Simple Conditions (or Compound Conditions) page appears. Modify the values as needed in the following fields:

- Name—Enter the name of the simple condition.
- Description—Enter the description of the simple condition.
- Attribute—Click to choose a dictionary from the drop-down list of dictionary options, and choose an attribute from the corresponding attribute choices.
- Operator—Enter **Equals** or **Not Equals**.

- Value—Enter a value that matches the selected attribute.

Step 3 Click **Save** to save your changes to the Cisco ISE system database and create this modified authorization condition.



Note The Name, Attribute, Operator and Value fields in simple conditions are required and marked with an asterisk (*).



Note Compound Conditions consist of one or more simple conditions that include different “Equals,” “Not Equals,” “Matches,” “Starts With,” or “Not Starts With” operators, and “AND” and “OR” directives that are built upon existing simple conditions. The procedure for creating a new compound condition follows the same sequence of steps used to create a simple condition. For more details about compound conditions, see [Compound Conditions, page 17-18](#).



Note The “Matches” operator supports and uses regular expressions (REGEX) not wildcards.

Duplicating Existing Authorization Policy Element Conditions

Use this procedure to duplicate existing authorization policy element conditions (simple or compound). This option provides a means for using an existing authorization policy as a template whereby you can:

- Change the name to create a duplicate policy with the same policy element conditions
- Change the name and modify one or more policy elements as desired



Note You must click **Submit** to save your changes to the Cisco ISE database in either case when you duplicate existing policy element conditions.

To duplicate existing authorization policy element conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Authorization > Simple Conditions (or Compound Conditions)**.

The Conditions page appears listing all existing configured authorization policy element conditions.

Step 2 To duplicate an existing simple condition authorization policy, check the check box corresponding to the condition you want to duplicate, and click **Duplicate**.

The Simple Conditions (or Compound Conditions) page appears. You can change the name for this policy:

- Name—Enter a new name for this simple condition, or you can modify one or more values as needed in the following fields to define a new simple condition policy:
- Description—Enter the description of the simple condition.
- Attribute—Click to choose a dictionary from the drop-down list of dictionary options, and choose an attribute from the corresponding attribute choices.
- Operator—Enter **Equals** or **Not Equals**.

- Value—Enter a value that matches the selected attribute.

Step 3 Click **Submit** to save your changes to the Cisco ISE database and create this authorization condition.



Note The Name, Attribute, Operator, and Value fields in simple conditions are required and are marked with an asterisk (*).



Note Compound conditions consist of one or more simple conditions that include different “Equals,” “Not Equals,” “Matches,” “Starts With,” or “Not Starts With” operators and “AND” and “OR” directives that are built upon existing simple conditions. The procedure for creating a new compound condition follows the same steps and processes that are used to create a simple condition. For more details about compound conditions, see [Compound Conditions, page 17-18](#).



Note The “Matches” operator supports and uses regular expressions (REGEX) not wildcards.

Deleting Existing Authorization Policy Element Conditions

Use this procedure to delete existing authorization policy element conditions.

To delete existing authorization policy element conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Authorization > Simple Conditions** (or **Compound Conditions**).

The Conditions page appears listing all existing configured authorization policy element conditions.

Step 2 To delete an existing condition, check the check box corresponding to the condition you want to delete, and click **Delete**.

- A confirmation dialog appears prompting if you want to delete the selected item(s).
- Click **Delete** to confirm that you want to delete the authorization condition (or click **Cancel** to end operation).

Searching Existing Authorization Policy Element Conditions

Use this procedure to search for existing authorization policy element conditions that match your desired search criteria.

To search existing authorization policy element conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Authorization > Simple Conditions** (or **Compound Conditions**).

The Conditions page appears listing all existing configured authorization policy element conditions.

Step 2 To search for a specific value in the existing authorization policy conditions, click **Filter** and choose either **Quick Filter** or **Advanced Filter**.

- If you choose Quick Filter, you can search for authorization policy conditions that match the condition name or description attribute value you specify:
 - Enter a value to search for in either the Name or Description field.
 - Any attribute matching the specified condition name or description appears in the Conditions table.
 - If you choose **Advanced Filter**, you can search using a variety of authorization policy conditions that match the attribute, operator, and value fields that you configure in the following search rule:
 - From the Filter drop-down list, choose either **Name** or **Description**.
 - From the operator drop-down list, choose from among the following options: **Contains**, **Does not contain**, **Does not equal**, **Ends with**, **Is empty**, **Is exactly (or equals)**, **Is not empty**, or **Starts with**.
 - Enter an attribute that matches the search values with which you want to filter. You can add additional rules.
 - Click **Go** to display any matches in the Conditions table.
-

Configuring Time and Date Conditions

Use the Policy Elements Conditions page to display, create, modify, delete, duplicate, and search time and date policy element conditions. Policy elements are shared objects that define a condition that is based on specific time and date attribute settings that you configure.

Time and date conditions let you set or limit permission to access Cisco ISE system resources to specific times and days as desired by the attribute settings you make. The following topics provide procedures for performing time and date attribute-related tasks:

- [Displaying Existing Time and Date Conditions, page 17-23](#)
- [Creating New Time and Date Conditions, page 17-23](#)
- [Modifying Existing Time and Date Conditions, page 17-24](#)
- [Deleting Existing Time and Date Conditions, page 17-25](#)
- [Duplicating Existing Time and Date Conditions, page 17-25](#)
- [Searching Existing Time and Date Conditions, page 17-26](#)

Displaying Existing Time and Date Conditions

Use this procedure to display all existing time and date policy element conditions.

To display all existing time and date conditions, choose **Policy > Policy Elements > Conditions > Common > Time and Date**.

The Time and Date Conditions page appears listing all the existing configured time and date conditions.

Creating New Time and Date Conditions

Use this procedure to create new time and date policy element conditions.

To create new time and date conditions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Conditions > Common > Time and Date**.

The Time and Date Conditions page appears listing all the existing configured time and date conditions.

Step 2 To create a new time and date condition, click **Add**.

The Time and Date Condition page appears.

Step 3 Enter values in the following fields to define a new time and date condition:

- Condition Name—Enter the name of the time and date condition.
- Description—Enter a description of the time and date condition.



Note You can choose to create a time and date condition using the options in the Standard Settings or the Exceptions panes.

- If you choose to use the Standard Settings pane options—Choose the options corresponding to the time and date conditions you want to set:
 - All Day (the default option) or Specific Hours (this option provides drop-down lists you can use to configure hours, minutes, and AM/PM to set a to-and-from time range).
 - Every Day (the default option) or Specific Days (this option provides check boxes you can use to configure one or more specific days of the week).
 - No Start and End Dates (the default option), or Specific Date Range (this option provides drop-down lists you can use to configure the month, day, and year to set a to-and-from date range), or Specific Date (this option provides drop-down lists you can use to configure a specific month, day, and year).
- If you choose to use the Exceptions pane options—Choose the options corresponding to the time and date conditions you want to set:
 - Time Range (this option provides drop-down lists you can use to configure the hours, minutes, and AM/PM to set a to-and-from time range).
 - Week Days (this option provides check boxes you can use to configure one or more specific days of the week).
 - Date Range (this provides two options):
 - Specific Date Range—Provides drop-down lists you can use to configure a specific to-and-from date range by month, day, and year.
 - Specific Date—Provides drop-down lists you can use to configure a specific month, day, and year.

Step 4 Click **Submit** to save your changes to the Cisco ISE database and create this time and date condition.



Note The Condition Name field for time and date conditions is required and is marked with an asterisk (*).

Modifying Existing Time and Date Conditions

Use this procedure to modify existing time and date policy element conditions.

To modify existing time and date conditions, complete the following steps:

-
- Step 1** Choose **Policy > Policy Elements > Conditions > Common > Time and Date**.
- The Time and Date Conditions page appears listing all the existing configured time and date conditions.
- Step 2** To edit an existing time and date condition, check the check box corresponding to the condition you want to modify, and click **Edit**.
- The Time and Date Condition page appears. Modify the options and settings in the following fields as needed (see field and option descriptions in [Creating New Time and Date Conditions, page 17-23](#)):
- Condition Name
 - Description
 - Standard Settings or Exceptions (using the set of options in the panel you choose)
- Step 3** Click **Save** to save your changes to the Cisco ISE system database and create this modified time and date condition.



Note

The Condition Name field for time and date conditions is required and is marked with an asterisk (*).

Deleting Existing Time and Date Conditions

Use this procedure to delete existing time and date policy element conditions.

To delete existing time and date conditions, complete the following steps:

-
- Step 1** Choose **Policy > Policy Elements > Conditions > Common > Time and Date**.
- The Time and Date Conditions page appears listing all the existing configured time and date conditions.
- Step 2** To delete an existing condition, check the check box that corresponds to the time and date condition you want to delete, and click **Delete**.
- A confirmation dialog appears.
 - Click **OK** to confirm that you want to delete the selected time and date condition (or click **Cancel** to end operation).
 - A Condition(s) deleted successfully dialog appears.
-

Duplicating Existing Time and Date Conditions

Use this procedure to duplicate existing time and date policy element conditions, from which you can create a new time and date condition.

To duplicate existing time and date conditions, complete the following steps:

-
- Step 1** Choose **Policy > Policy Elements > Conditions > Common > Time and Date**.
- The Time and Date Conditions page appears listing all existing configured time and date conditions.

- Step 2** To duplicate an existing time and date condition, check the check box corresponding to the condition you want to duplicate, and click **Duplicate**.
- The Time and Date Conditions page appears. You can modify the following conditions in the upper panel as necessary:
- Name—Enter a new name for this condition, or you can modify one or more values as needed in the following fields to define a new time and date condition.
 - Description—Enter the description of the time and date condition.
- Step 3** In the Standard Settings panel, modify the following values as needed:
- All Day
 - Specific Hours (by setting the specific time range in HH:MM:AM/PM using the pull-down options)
 - Every Day
 - Specific Days (by checking the check box(es) that match your desired days)
 - No Start and End Date
 - Specific Date Range (by setting the specific Month:Date:Year from/to date range using the pull-down options)
 - Specific Date (by setting the specific Month:Date:Year date using the pull-down options)
- Step 4** Click **Save** to save your changes to the Cisco ISE database and create this authorization condition.

**Note**

The Condition Name field in time and date conditions is required and are marked with an asterisk (*).

Searching Existing Time and Date Conditions

Use this procedure to search existing date and time policy element conditions that match a desired search criteria.

To search existing time and date conditions, complete the following steps:

-
- Step 1** Choose **Policy > Policy Elements > Conditions > Common > Time and Date**.
- The Time and Date Conditions page appears listing all the existing configured time and date conditions.
- Step 2** To search for a specific value in the existing date and time conditions, click **Filter** and choose either **Quick Filter** or **Advanced Filter**.
- If you choose **Quick Filter**, you can search for time and date conditions that match the condition name or description attribute value you specify:
 - Type the desired search attribute value in the Condition Name or Description fields.
 - Any attribute matching the specified condition name or description appears in the Time and Date Conditions table.
 - If you choose **Advanced Filter**, you can search using a variety of time and date conditions that match the attribute values you specify:
 - Type the desired search attributes values in the appropriate fields.

- Any attributes that matches the search values you specified appears in the Time and Date Conditions table.

Configuring Permissions for Authorization Profiles

Before you start configuring permissions for authorization profiles, make sure you understand the relationship between authorization policies and profiles, are familiar with the Authorization Profile page, know the basic guidelines to follow when configuring policies and profiles, understand what comprises permissions in an authorization profile, and are aware of configuration default values that are described in the following topics:

- [Cisco ISE Authorization Policies and Profiles, page 17-5](#)
- [Authorization Profile Page, page 17-8](#)
- [Authorization Policy and Profile Guidelines, page 17-9](#)
- [Authorization Policy, Rule, and Profile Configuration Defaults, page 17-11](#)

Use the Results navigation pane as your starting point in the process for displaying, creating, modifying, deleting, duplicating, or searching policy element permissions for the different types of authorization profiles on your network. The following topics provide procedures for performing these tasks:

- [Displaying an Existing Authorization Profile and Permissions, page 17-27](#)
- [Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-28](#)
- [Modifying an Existing Authorization Profile, page 17-30](#)
- [Deleting an Existing Authorization Profile, page 17-30](#)
- [Duplicating an Existing Authorization Profile, page 17-31](#)
- [Searching an Existing Authorization Profile, page 17-31](#)

**Note**

The Results pane initially displays Authentication, Authorization, Profiling, Posture, Client Provisioning, and Security Group Access options.

Authorization profiles let you choose the attributes to be returned when a RADIUS request is accepted. Cisco ISE provides a mechanism where you can configure Common Tasks settings to support commonly-used attributes. You must enter the value for the Common Tasks attributes, which Cisco ISE translates to the underlying RADIUS values.

Displaying an Existing Authorization Profile and Permissions

Use this procedure to display the permissions for an existing authorization profile.

**Note**

The Results navigation pane displays Authorization Profiles, Downloadable ACL, and Inline Posture node options under Authorization.

To display existing permissions for an authorization profile, choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

The Authorization Profiles page appears listing all existing configured authorization profiles.

Creating and Configuring Permissions for a New Standard Authorization Profile

Use this procedure to create a new standard authorization profile and configure its permissions.

To create a new standard authorization profile and permissions, complete the following steps:

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

The Authorization Profiles page appears listing all existing configured authorization profiles.

Step 2 To create a new profile, choose one of the two following methods:

- In the Authorization pane, click **action** (icon) and click **Create Standard Authorization Profile** or
- In the Standard Authorization Profiles page, click **Add**

The Authorization Profiles > New Authorization profile page appears.

Step 3 Enter values in the following columns and fields as needed to create a new authorization profile:

- **Authorization Profile**
 - Name—Enter a name that identifies the new authorization profile.
 - Description—Enter a description of the authorization profile.
 - Access Type—Choose from the two drop-down list access type options (**ACCESS_ACCEPT** or **ACCESS_REJECT**).



Note The Name and Access Type fields are required and are marked with an asterisk (*).

- **Common Tasks**

- DACL Name—To choose, check the check box and choose existing downloadable ACL options from the drop-down list (for example, Cisco ISE provides two default values in the drop-down list: **PERMIT_ALL_TRAFFIC** or **DENY_ALL_TRAFFIC**). The drop-down list will include all current DACLs in the local database.
- VLAN—To choose, check the check box and enter an attribute value that identifies a virtual LAN (VLAN) ID that you want associated with the new authorization profile you are creating (both integer and string values are supported for the VLAN ID). The format for this entry would be *Tunnel-Private-Group-ID:VLANnumber*.



Note If you do not select a VLAN ID, Cisco ISE uses a default value of VLAN ID = 1. For example, if you only entered 123 as your VLAN number, the Attributes Details pane reflects the following value: Tunnel-Private-Group-ID = 1:123.

- Voice Domain Permission—To choose, check the check box to enable the vendor-specific attribute (VSA) of “cisco-av-pair” to be associated with a value of “device-traffic-class=voice”. In a multi-domain authorization mode, if the network switch receives this VSA, the endpoint is placed on to a voice domain after authorization.
- Posture Discovery—To choose, check the check box to enable a redirection process used for Posture discovery in Cisco ISE, and enter an ACL on the device that you want to associate with this authorization profile. For example, if the value you entered is ac1119, this is reflected in the

Attributes Details pane as: cisco-av-pair = url-redirect-acl = acl119. The Attributes Details pane also displays: cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionValueIdValue&action=cpp.

- **Centralized Web Authentication**—To choose, check the check box to enable a redirection process that is similar to Posture discovery, but it redirects guest user access requests to the Guest server in Cisco ISE. Enter an ACL on the device that you want to associate with this authorization profile, and select **Default** or **Manual** from the Redirect drop-down list. For example, if the value you entered is acl-999, this is reflected in the Attributes Details pane as: cisco-av-pair = url-redirect-acl = acl-99. The Attributes Details pane also displays: cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionValueIdValue&action=cwa.
- **Auto SmartPort**—To choose, check the check box to enable Auto SmartPort functionality and enter a corresponding event name value in the text box. This enables the VSA cisco-av-pair with a value for this option as “auto-smart-port=event_name”. Your choice is reflected in the Attributes Details pane.
- **Filter-ID**—To choose, check the check box to enable a RADIUS filter attribute that sends the ACL name that you define in the text box (which is automatically appended with “.in”). Your choice is reflected in the Attributes Details pane.
- **Reauthentication**—To choose, check the check box and enter a value in seconds for maintaining connectivity during reauthentication. You can also choose attribute values from the Timer drop-down list. You choose to maintain connectivity during reauthentication by choosing to use either the default (a value of 0) or **RADIUS-Request** (a value of 1) from the drop-down list. Setting this to the RADIUS-Request value maintains connectivity during the reauthentication process.
- **MACSec Policy**—To choose, check the check box to enable the MACSec encryption policy whenever a MACSec-enabled client connects to Cisco ISE, and choose one of the following three options from the corresponding drop-down list: **must-secure**, **should-secure**, or **must-not-secure**. For example, your choice is reflected in the Attributes Details pane as: cisco-av-pair = linksec-policy=must-secure.
- **NEAT**—To choose, check the check box to enable Network Edge Access Topology (NEAT), a feature that extends identity recognition between networks. Checking this check box displays the following value in the Attributes Details pane: cisco-av-pair = device-traffic-class=switch.
- **Web Authentication (Local Web Auth)**—To choose, check the check box to enable local web authentication for this authorization profile. This value lets the switch recognize authorization for web authentication by Cisco ISE sending a VSA along with a DACL. The VSA is cisco-av-pair = priv-lvl=15 and this is reflected in the Attributes Details pane.
- **Wireless LAN Controller (WLC)**—To choose, check the check box and enter an ACL name in the text field. This value is used in a required Airespace VSA to authorize the addition of a locally defined ACL to a connection on the WLC. For example, if you entered rsa-1188, this would be reflected in the Attributes Details pane as: Airespace-ACL-Name = rsa-1188.
- **ASA VPN**—To choose, check the check box to enable an Adaptive Security Appliances (ASA) VPN group policy. From the drop-down Attribute list, choose a value to configure this setting. For example, if you selected Cisco-BBSM, and then selected CBBSM-Bandwidth, this would be reflected in the Attributes Details pane as: Class = Cisco-BBSM:CBBSM-Bandwidth.



Note

The Name and Access Type fields are required and are marked with an asterisk (*).

• Advanced Attributes Settings

- Click the down-arrow icon to display the available options in the Dictionaries window. Click to select the desired dictionary and attribute to configure in the first field.
- Click the down-arrow icon to display the available options in the Attribute Values window. Click to select the desired attribute group and attribute value for the second field. This value matches the one selected in the first field. Any Advanced Attributes setting(s) that you configure will be displayed in the Attribute Details panel.



Note To modify or delete any of the read-only values that are displayed in the Attributes Details pane, you must modify or delete these values in the corresponding Common Tasks field or in the attribute that you selected in the Attribute Values text box in the Advanced Attributes Settings pane.

- **Attributes Details**

- This pane displays any of the configured attribute values that you set for the Common Tasks and Advanced Attributes.



Note The values displayed in the Attributes Details pane are read-only and cannot be edited or deleted in this pane.

Step 4 Click **Submit** to save your changes to the Cisco ISE system database to create an authorization profile.

Modifying an Existing Authorization Profile

Use this procedure to modify the permissions in an existing authorization profile.

To modify permissions in an existing authorization profile, complete the following steps:

- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.
The Authorization Profiles page appears listing all existing configured authorization profiles.
- Step 2** To edit permissions in an existing authorization profile, check the check box corresponding to the existing authorization profile you want to modify, and click **Edit**.
- Step 3** Modify the values in the Authorization Profile, Common Tasks, Advanced Attributes Settings, and Attributes Details columns as needed.
- Step 4** Click **Save** to save your changes to the Cisco ISE database to create an authorization profile.

For more information:

- For details about the values in the Authorization Profile, Common Tasks, Advanced Attributes Settings, and Attributes Details columns, see the descriptions in [Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-28](#).

Deleting an Existing Authorization Profile

Use this procedure to delete an existing authorization profile, which also deletes its corresponding policy element permissions.

To delete an existing authorization profile, complete the following steps:

-
- | | |
|---------------|---|
| Step 1 | Choose Policy > Policy Elements > Results > Authorization > Authorization Profiles .
The Authorization Profiles page appears listing all existing configured authorization profiles. |
| Step 2 | To delete an existing authorization profile, check the check box corresponding to the existing authorization profile you want to delete, and click Delete .
A confirmation deletion dialog appears alerting you that the authorization profile was deleted. |
| Step 3 | Click OK to confirm you want to delete this authorization profile from the Cisco ISE system database. |
-

Duplicating an Existing Authorization Profile

Use this procedure to duplicate an existing authorization profile, from which you can create a new authorization profile.

To duplicate an existing authorization profile, complete the following steps:

-
- | | |
|---------------|--|
| Step 1 | Choose Policy > Policy Elements > Results > Authorization > Authorization Profiles .
The Authorization Profiles page appears listing all existing configured authorization profiles. |
| Step 2 | To duplicate an existing authorization, check the check box corresponding to the authorization profile you want to duplicate, and click Duplicate .
The Authorization Profiles page appears. |
| Step 3 | Modify the values in the Authorization Profile, Common Tasks, Advanced Attributes Settings, and Attributes Details columns as needed. |
| Step 4 | Click Submit to save your changes to the Cisco ISE database and create this new authorization profile. |



Note

Values in the Name and Access Type fields are required and are marked with an asterisk (*).

For more information:

- For details about the values in the Authorization Profile, Common Tasks, Advanced Attributes Settings, and Attributes Details columns, see the descriptions in [Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-28](#).

Searching an Existing Authorization Profile

Use this procedure to search for existing authorization profile conditions that match a desired search criteria.

To search an existing authorization profile, complete the following steps:

-
- | | |
|---------------|--|
| Step 1 | Choose Policy > Policy Elements > Results > Authorization > Authorization Profiles .
The Authorization Profiles page appears listing all existing configured authorization profiles. |
|---------------|--|

Step 2 To search for a specific value in the existing authorization policy conditions, click **Filter** and choose between the **Quick Filter** or **Advanced Filter** options.

If you choose **Quick Filter**, you can search for authorization profile that matches the name or description value you specify:

- Enter a value to search for in the Name or Description fields.

Any attribute that matches the specified authorization profile name or description appears in the Conditions table.

- If you choose **Advanced Filter**, you can search for an authorization profile that matches the attribute, operator, and value fields that you configure in the following search rule:
 - From the Filter drop-down list, choose either **Name** or **Description**.
 - From the operator drop-down list, choose from the following options: **Contains**, **Does not contain**, **Does not equal**, **Ends with**, **Is empty**, **Is exactly (or equals)**, **Is greater than**, **Is greater than or equal to**, **Is less than**, **Is less than or equal to**, **Is not empty**, or **Starts with**.
 - Enter an attribute that matches the search values with which you want to filter. You can add additional rules.
- Click **Go** to display any matches in the Conditions table.

Configuring Permissions for Downloadable ACLs

To start the process where you can display, create, modify, or delete policy element permissions for downloadable ACLs (DACLS), you must locate its navigation pane in the Cisco ISE user interface. To do this, choose **Policy > Policy Elements > Results > Authorization** to display the Authorization navigation pane.

The Authorization navigation pane initially displays the following elements:

- Authorization Profiles
- Downloadable ACLs
- Inline Posture Node Profiles

For more information:

- For more information about configuring permissions for and managing DACLS, see [Configuring DACLS, page 17-32](#).

Configuring DACLS

The following topics provide procedures for configuring permissions for DACLS:

- [Displaying Existing DACLS, page 17-33](#)
- [Creating and Configuring a New DACL, page 17-33](#)
- [Modifying an Existing DACL, page 17-35](#)
- [Deleting an Existing DACL, page 17-35](#)
- [Duplicating an Existing DACL, page 17-35](#)
- [Searching an Existing DACL, page 17-36](#)

Displaying Existing DACLs

Use this procedure to display any existing DACLs.


To display existing DACL, choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.

The DACL Management page appears listing all existing configured DACLs.

Creating and Configuring a New DACL

Use this procedure to create a new DACL.

To configure a new DACL, complete the following steps:

-
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.
The DACL Management page appears listing all existing configured DACLs.
- Step 2** To create a new DACL, click **action** (icon) and select **Create DACL** or click **Add (+)** in the DACL Management page.
- Step 3** Enter values for the DACL in the following fields:
- Name—Enter a name that identifies the DACL.
 - Description—Enter a description of the DACL.
 - DACL Content—Enter the type of desired content in the ACL (IPPermit or IPDeny).
-  **Note** The Name and DACL Content fields require that values be entered and are marked with an asterisk (*).
-
- Step 4** Click **Submit** to save your configured values to the Cisco ISE database and create this DACL.
-

The following is the supported format for DACL referenced by an Inline Posture authorization profile:

- **ACTION** **PROTOCOL** **SOURCE_SUBNET** **WILDCARD_MASK** [**OPERATOR** [**PORT**]] **DEST_SUBNET** **WILDCARD_MASK** [**OPERATOR** [**PORT**]] [**ICMP_TYPE_CODE**]

Table 17-3 describes the options in the DACL format.

Table 17-3 *DACL Format - Options*

Option	Description
ACTION	Specifies whether the policy element permissions should permit or deny access.
PROTOCOL	Specifies any one of the following protocols: <ul style="list-style-type: none"> • ICMP • UDP • TCP • IP

Table 17-3 *DACL Format - Options (continued)*

Option	Description
SOURCE_SUBNET	Specifies any one of the following source subnet formats: <ul style="list-style-type: none"> any host x.x.x.x <subnet>
DEST_SUBNET	Specifies any one of the following destination subnet formats: <ul style="list-style-type: none"> any host x.x.x.x <subnet>
WILDCARD_MASK	Specifies the inverse of the subnet mask. For example, 0.0.0.255.
OPERATOR	Specifies any one of the following operators: <ul style="list-style-type: none"> eq lt gt neq range
<i>PORT</i>	Specifies the port. The valid range is from 1 to 65535.
<i>ICMP_TYPE_CODE</i>	Specifies any one of the following ICMP type codes: <ul style="list-style-type: none"> 0—Echo reply 8—Echo request 3:[0-15]—Destination unreachable 5:[0-3]—ICMP redirects

Examples of acceptable ACL Format:

permit tcp any host 192.168.1.100 eq 80—permits www traffic from anywhere to host 192.168.1.100

permit udp any eq 68 any eq 67—permits dhcp traffic

permit icmp any any 8, permit icmp any any 0—allows icmp echo-request and echo-reply

deny icmp any any 5:0—denies icmp network redirects

permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255—permits all traffic from 192.168.2.0 subnet to 192.168.1.0 subnet

permit udp any any range 16384 32767—permits voice traffic using range of udp ports

Examples of incorrect syntax:

permit ip 192.168.2.100 192.168.1.100—host/wildcard keyword missing

permit tcp host 192.168.2.100 host 192.168.1.100 eq 88 389 636 454 3268 3269 1025 1026

(You cannot club multiple ports using eq operator, and this ACL needs to be split into multiple lines one for each destination port)

**Note**

Ensure that there are no empty spaces or hidden characters in the DACL syntax. Any unknown characters, if exists in the DACL syntax, the Inline Posture node will not accept the DACL. For more information, refer to the Inline Posture logs.

Modifying an Existing DACL

Use this procedure to modify any existing DACL.

To modify an existing DACL, complete the following steps:

-
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.
The DACL Management page appears listing all existing configured DACLs.
- Step 2** To edit an existing DACL, check the check box corresponding to the DACL that you want to modify, and click **Edit**.
The DACL Management page appears.
- Step 3** Modify the values for the DACL as needed in the following fields:
- Name—Enter a name that identifies the DACL.
 - Description—Enter a description of the DACL.
 - DACL Content—Choose the type of desired content in the ACL (IPPermit or IPDeny).

**Note**

The Name and DACL Content fields require that values be entered and are marked with an asterisk (*).

-
- Step 4** Click **Submit** to save your configured values to the Cisco ISE database and create this modified DACL.
-

Deleting an Existing DACL

Use this procedure to delete an existing DACL.

To delete an existing ACL, complete the following steps:

-
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.
The DACL Management page appears listing all existing configured DACLs.
- Step 2** To delete an existing DACL, check the check box corresponding to the DACL that you want to delete, and click **Delete**.
A deletion confirmation dialog appears.
- Step 3** Click **OK** to confirm that you want to delete the DACL, or click **Cancel** to end the operation.
-

Duplicating an Existing DACL

Use this procedure to duplicate an existing DACL, from which you can create a new DACL.

To duplicate an existing DACL, complete the following steps:

-
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.
The DACL Management page appears listing all existing configured DACLs.
- Step 2** To duplicate an existing DACL, check the check box corresponding to the DACL you want to duplicate, and click **Duplicate**.
The Downloadable ACL page appears.
- Step 3** Modify the values in the Name, Description, DACL Content fields as needed.
- Step 4** Click **Submit** to save your changes to the Cisco ISE database and create this new authorization profile.



Note The Name and DACL Content fields require that values be entered and are marked with an asterisk (*).

Searching an Existing DACL

Use this procedure to search an existing DACL using criteria that searches for existing DACL values that match your settings.

To search an existing DACL, complete the following steps:

-
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.
The DACL Management page appears listing all existing configured DACLs.
- Step 2** To search for a specific value in the existing DACLs, click **Filter** and choose between the **Quick Filter** or **Advanced Filter** options.
- If you choose **Quick Filter**, you can search for DACL values that match the name or description value you specify:
- Enter a value to search for in the **Name** or **Description** fields.
- Any attribute that matches the specified DACL name or description appears in the Conditions table:
- If you choose **Advanced Filter**, you can search for a DACL that matches the attribute, operator, and value fields that you configure in the following search rule:
 - In the Filter drop-down list, select either **Name** or **Description**.
 - In the operator drop-down list, select from the following options: **Contains**, **Does not contain**, **Does not equal**, **Ends with**, **Is empty**, **Is exactly (or equals)**, **Is not empty**, or **Starts with**.
 - Enter an attribute that matches the search values with which you want to filter. You can add additional rules.
 - Click **Go** to display any matches in the Conditions table.
-

Configuring Policies for SGACLs

To learn how to configure policies for security group access control lists (SGACLs), which allow you to display, create, modify, or delete policy element permissions for SGACLs, see [Configuring Cisco Security Group Access Policies, page 23-1](#).

Machine Access Restriction and Active Directory Users

Cisco ISE contains a Machine Access Restriction (MAR) component that provides an additional means of controlling authorization for Microsoft Active Directory-authentication users. This form of authorization is based on the machine authentication of the computer used to access the Cisco ISE network. For every successful machine authentication, Cisco ISE caches the value that was received in the RADIUS Calling-Station-ID attribute (attribute 31) as evidence of a successful machine authentication.

Cisco ISE retains each Calling-Station-ID attribute value in cache until the number of hours that was configured in the “Time to Live” parameter in the Active Directory Settings page expires. Once the parameter has expired, Cisco ISE deletes it from its cache.

When a user authenticates from an end-user client, Cisco ISE searches the cache for a Calling-Station-ID value from successful machine authentications for the Calling-Station-ID value that was received in the user authentication request. If Cisco ISE finds a matching user-authentication Calling-Station-ID value in the cache, this affects how Cisco ISE assigns permissions for the user that requests authentication in the following ways:

- If the Calling-Station-ID value matches one found in the Cisco ISE cache, then the authorization profile for a successful authorization should be assigned.
- If the Calling-Station-ID value is not found to match one in the Cisco ISE cache, then the authorization profile for a successful user authentication without machine authentication should be assigned.

For more information

- For more details, see [Machine Authentication, page 5-5](#).

