Configure and Manage Policies

• Policy Sets, page 1
• Authentication Policies, page 21
• Authorization Policies, page 25
• Policy Conditions, page 32
• Special Network Access Conditions, page 47
• Policy Set Protocol Settings, page 51

Policy Sets

Cisco ISE is a policy-based, network-access-control solution, which offers network access policy sets, allowing you to manage several different network access use cases such as wireless, wired, guest, and client provisioning. Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type and similar parameters. When you install ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules.

When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for a variety of different vendors. Cisco ISE allows you to create conditions as individual policy elements that can be reused.

The network access service to be used per policy set to communicate with the network devices is defined at the top level of that policy set. Network access services include:

• Allowed protocols—the protocols configured to handle the initial request and protocol negotiation
• A proxy service—sends requests to an external RADIUS server for processing
From the Device Administration work center, you can also select a relevant TACACS server sequence for your policy set. Use the TACACS server sequence to configure a sequence of TACACS proxy servers for processing.

You can refer to the Control Device Administration Using TACACS+ chapter for more information on device administration.

Policy sets are configured hierarchically, where the rule on the top level of the policy set, which can be viewed from the Policy Set table, applies to the entire set and is matched before the rules for the rest of the policies and exceptions. Thereafter, rules of the set are applied in this order:

1. Authentication policy rules
2. Local policy exceptions
3. Global policy exceptions
4. Authorization policy rules

In order to configure customized policy sets, you can work with:

- Create and Manage Policy Sets, on page 20
- Authentication Policies, on page 21
- Authorization Policies, on page 25
- Authorization Policy Exceptions, on page 32
- Configure, Edit and Manage Policy Conditions, on page 42

Note: Policy Sets functionality is identical for network access and for device administration policies. All processes described in this chapter can be applied when working with both the Network Access and the Device Administration work centers. This chapter specifically discusses the Network Access work center policy sets. To access this work center, choose Work Centers > Network Access > Policy Sets.

Network Access Policy Terminology

The following are some of the commonly used terms in the policy set pages:

Access Control Lists

An access control list (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 (such as, Permit or Deny).
Allowed Protocols

Allowed protocols, configured on the top level of each policy set, define the set of protocols that Cisco ISE can use to communicate with the device that requests access to the network resources. You can configure a single allowed protocol per policy set, or alternatively, a server sequence that you define in advance.

Authentication Policy

Authentication policies are configured within policy sets. Each policy set can contain a single authentication policy with multiple rules. Priority of the authentication rules for processing is determined based on the order of those rules as they appear within the Authentication Policy table of the policy set itself (from the Set view page).

The authentication policy uses the allowed protocols configured on policy set at the top level. Identity source sequences define the order in which Cisco ISE looks for user credentials in different databases. Within the authentication policy under the main policy set, you can define condition-based rules that configure the identity sources or identity source sequences, as well as the identity methods, to be used for authentication.

Authorization Policy and Exceptions

An authorization policy consists of user-defined rules that determine the permissions for different user groups when accessing your network.

Authorization policies allow access to specific or all network endpoints and are created to apply to groups of users and devices that share a common set of privileges and can also be used as templates that you modify to serve the needs of another specific identity group, using specific conditions or permissions, to create another type of standard policy to meet the needs of new divisions, or user groups, devices, or network groups.

By contrast, 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.

Authentication Policy Result Options

You can define what course of action Cisco ISE should take if the authentication fails, the user is not found, or if the process fails. Authentication policy result options are configured on the authentication policy level.

Identity Source and Identity Source Sequences

Identity source, configured on the Authentication policy level, defines which database Cisco ISE should use for user authentication. The database can be an internal database or an external identity source, such as Active Directory or LDAP. You can add a sequence of databases to an identity source sequence and list this sequence as the identity source in your policy. Cisco ISE will search for the credentials in the order in which the databases are listed in this sequence.
Network Authorization

Network authorization controls user access to the network and its resources and what each user can do on the system with those resources. Activate network authorization from Cisco ISE by defining 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 RADIUS access to the Cisco ISE network and its resources.

Policy Rules

Policy rules act to create a specific policy. For example, a policy set can include a rule that indicates under which circumstances a certain allowed protocol should be used for network access. An authentication policy can include a rule that indicates under which circumstances Active Directory is to be used for authentication. A standard authorization policy can include the rule name using an If-Then convention that links a value entered for identity groups with specific conditions or attributes to produce a specific set of permissions that create a unique authorization profile.

Policy Sets

A policy set is an hierarchical container consisting of a single user-defined rule that indicates the allowed protocol or server sequence for network access, as well as authentication and authorization policies and policy exceptions, all also configured with user-defined condition-based rules.

Policy Evaluation

Policies consist of rules, where each rule consists of conditions to be satisfied that 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.

At run-time, Cisco ISE evaluates the policy conditions and then applies the result that you define based on whether the policy evaluation returns a true or a false value.

During policy-condition evaluation, Cisco ISE compares an attribute with a value. It is possible that where the attribute specified in the policy condition may not have a value assigned in the request. In such cases, if the operator that is used for comparison is “not equal to,” then the condition will evaluate to true. In all other cases, the condition will evaluate to false.

For example, in the condition Radius.Calling_Station_ID Not Equal to 1.1.1.1, if the Calling Station ID is not present in the RADIUS request, then this condition will evaluate to true. This evaluation is not unique to the RADIUS dictionary and occurs because of the usage of the “Not Equal to” operator.

In ISE, the Policy Sets table provides a list of all policy sets currently configured in the system. The order of the enabled policy sets determines the order by which the system searches for the relevant policy set every time an endpoint requests access. The last row in the Policy Set table from the Policy page is the default policy that will be applied if none of the rules match the request in any of the other configured policy sets. You can edit the allowed protocols and identity source selection in default policy set, but you cannot delete it.
Policy Set Evaluation Flow

The sequence of policy set and the authentication and authorization evaluation flow is as follows:

1. Evaluate policy set (by evaluating the policy set condition). As a result, one policy set is selected.
2. Evaluate allowed protocols rules of the selected policy set.
3. Evaluate ID store rules of the selected policy set.
4. Evaluate authorization rules of the selected policy set, based on the following paradigm:
   a. Evaluate the local exception policy if it is defined
   b. If no match is found in Step a above, evaluate global exception policy if defined
   c. If no match is found in Step b above, evaluate authorization rules

If none of the policy sets match, the default policy set will be selected.

Network Access Work Center

Network Access related options are grouped under the Network Access Work Center menu (Work Centers > Network Access), so that the administrator can easily access all the options related to Network Access at one location.

You can perform the following tasks from the Network Access Work Center:
Configure and Manage Policies

Navigate the Policy Sets Area

Policy sets enable you to logically group authentication and authorization policies within the same set. The Policy Sets area enables you to configure, manage and update your policy sets.

To access the Policy Sets area for network access policies, choose Work Centers > Network Access > Policy Sets. To access the Policy Sets area for device administration policies, choose Work Centers > Device Administration > Device Admin Policy Sets.

The Policy Sets area consists of the main page and the Set view, from which you can manage all of the details for each policy set including configuration for authentication and authorization policies, and exceptions.

Policy Sets

The following figure shows the main elements of the main Policy Sets page.

The following table describes the main elements of the main Policy Sets page.
Table 1: Policy Sets

<table>
<thead>
<tr>
<th></th>
<th>Policy Sets tab</th>
<th>Provides a list of all policy sets currently configured in the system. The order of the enabled policy sets determines the order by which the system searches for the relevant policy set every time an endpoint requests access. The last row in the policy page is the default policy that will be applied if none of the rules match the request. You can edit the allowed protocols and identity source selection for the default policy, but you cannot delete this set. From this table you can:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• Change the order of the policy sets, thereby changing the priority of the sets to be checked by the system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Change the status of the policy set to Enabled, Disabled or Monitored. Enabled is the default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Update the free text policy set name and description of the policy sets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Access the Conditions Studio.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure the policy set protocol.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Create, delete and duplicate policy sets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Access the Set view in order to manage, update and edit the full policy set configuration, including policies and exceptions.</td>
</tr>
<tr>
<td>Status column</td>
<td>To drag rows and change the priority order of the policy sets in the table, click , hold, drag and drop. Enabled (active) policy sets are marked with . For more information about Status, see Policy Set Main Page—Configuration Settings. Rows that have been edited and not yet saved are marked with . The icon disappears when you choose Save.</td>
<td></td>
</tr>
<tr>
<td>Conditions column</td>
<td>Hover over any cell in the Conditions column and click the Edit icon to open the Conditions Studio. From the Conditions Studio, edit any of the Condition Studio conditions in order to use those conditions when configuring policy rules, including those used for the particular policy set from which you accessed the Studio, as well as all other conditions that have been configured and maintained in the system library.</td>
<td></td>
</tr>
</tbody>
</table>
### Actions column

Click the cog icon from the **Actions** column to view and select different actions:

- Insert new row above—insert a new policy set above the set from which you opened the Actions menu.
- Insert new row below—insert a new policy set below the set from which you opened the Actions menu.
- Duplicate above—insert a duplicate policy set of the set from which you opened the Actions menu, above the original set.
- Duplicate below—insert a duplicate policy set of the set from which you opened the Actions menu, below the original set.
- Delete—delete the policy set.

### View column

Click the arrow icon from the **View** column to open the Sets view screen and view, manage, and update the authentication and authorization policies as well as the policy exceptions.

### Action buttons

**Reset**—revert the table to the last saved details, removing any changes not yet saved.

**Save**—save any new changes made directly from the table to any of the policy sets and implement those changes.

---

### Set View

To configure, manage and edit a specific policy set, ensure you have saved or reset any changes made from the Policy Sets table and then choose the arrow icon from the **View** column to open the Set view.

The following figure shows the main elements of the Policy Sets - Set view page. The specific sections for authentication and authorization are described in separate sections.

![Policy Sets - Set view](image.png)

The following table describes the different elements of the Set view.

**Table 2: Set view**

| 1 | Set view | From the Set view you can view, update and manage all of the configurations for the selected policy set. |
Predefined and Default Configurations for Policies and Conditions

Cisco ISE is packaged with several predefined and default configurations that are part of common use cases for network access and device administration policy sets, including policy set, authentication, authorization, exception and condition configurations, as described in the following tables.

**Policy Set Default Configuration**

There is only one predefined policy set when you first install Cisco ISE. This set includes all predefined and default authentication and authorization rule configurations. This policy set is the default policy set. You can make changes to the configuration, but you cannot delete it.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Allowed Protocol / Server Sequence (RADIUS / TACACS+)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Policy Set</td>
<td>You can use this access service for wired and wireless 802.1X and MAB authentication policy rules. For the default policy set in the Network Access work center, this configuration is the network access allowed protocols service to be used in policy sets as the last default. For the default policy set in the Device Admin work center, this configuration uses the TACACS-relevant allowed protocol services to be used in policy sets as the last default. You can change the allowed protocol services for these default sets, but you cannot add conditions or delete the sets.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For the default policy set in the Network Access work center, the Default Allowed Protocol Service is configured to enable process host lookup and allows the following authentication protocols: • PAP/ASCII • EAP-MD5 • EAP-TLS • PEAP • EAP-FAST • EAP-TTLS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information about configuring allowed protocols, see Allowed Protocols. For the default policy set in the Device Admin work center, the Default Device Admin sequence is configured to allow the following authentication protocols: • PAP/ASCII • CHAP • MS-CHAPv1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For more information about configuring allowed protocols for TACACS, see Device Administration - Authorization Policy Results.</td>
<td></td>
</tr>
</tbody>
</table>
Authentication Policy Predefined and Default Rule Configurations

Authentication rules are configured within each policy set. Authentication rules define which identity source database to use for authentication, and what actions to take if authentication fails. The following table describes the information that can be configured for each of the predefined and default authentication rules available in Cisco ISE upon installation:

- Rule name
- Conditions—No conditions are used for any of the system defaults as described in detail below. Conditions can be smart conditions (stored for reuse in the Library) or conditions that you create for a specific rule. The available smart conditions used for the predefined rules are saved with unique names as indicated accordingly for the different predefined rules below, and are as detailed in this table: Predefined Policy Conditions (Smart Conditions), on page 17. You can also customize your own conditions. For more information about configuring customized conditions, see Policy Conditions, on page 32.
- Identity source or source sequence—which user database to use for authentication. For more information about configuring identity source sequences, see Internal and External Identity Sources.
- Failure configurations (Options)—the resulting action if the user cannot be authenticated
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Conditions</th>
<th>Use</th>
<th>Options</th>
</tr>
</thead>
</table>
| Default | For both network access and device administration, this is the default authentication rule that is included in every policy set you create, as well as in the system default policy set. You can edit this policy to configure any identity source sequence or identity source based on your needs, but you cannot add conditions to it or delete it. | There are no conditions for this set. As the default rule, this is the last rule referred to if all rules above it cannot be matched. | If no other authentication rule in the set can be matched, this default policy rule authenticates the All_User_ID_Stores identity sequence, which includes all users in all of the ID stores predefined in the system as follows:.  
  - Internal users database  
  - All AD join points  
  - Guest users  
You can change the identity store configuration, but you cannot change the conditions or delete this rule. | Options are configured as follows:  
  - If authentication fails, then the request is rejected.  
  - If the user cannot be found in the configured identity sources, then the request is rejected.  
  - If the process fails, the system drops the request and sends no response. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Conditions</th>
<th>Use</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dot1X</td>
<td>This authentication rule uses the wired and wireless 802.1X smart conditions as well as the default network access allowed protocols service (as defined in the Policy Set Default Configuration, on page 9 table). This policy evaluates requests that match the criteria specified in both the wireless and wired 802.1X smart conditions. You can make any changes to this configuration necessary based on your organization's needs.</td>
<td>Wired_802.1X</td>
<td>This predefined configuration is available only from the Network Access work center. This default policy uses the internal endpoints database as its identity source. You can edit this policy to configure any identity source sequence or identity source based on your needs.</td>
<td>Options are configured as follows:&lt;br&gt;- If auth fails, then the request is rejected.  &lt;br&gt;- If the user cannot be found in the configured identity sources, then the request is rejected.  &lt;br&gt;- If the process fails, the system drops the request and sends no response.</td>
</tr>
</tbody>
</table>
Options are configured as follows:

- If the request fails, then the request is rejected.
- If the user cannot be found in the configured identity sources, then the request is pushed to another service.
- If the process fails, the system drops the request and sends no response.

Authorization Policy Predefined and Default Rule Configurations

Authorization rules are configured within each policy set.
Authorization rules define permissions within the network for different security groups. The following table describes the information that can be configured for each of the predefined and default authorization rules available in Cisco ISE upon installation:

- Rule name
- Conditions—No conditions are used for any of the system defaults as described in detail below. Conditions can be smart conditions (stored for reuse in the Library) or conditions that you create for a specific rule. The available smart conditions used for the predefined rules are saved with unique names as indicated accordingly for the different predefined rules below, and are as detailed in this table: Predefined Policy Conditions (Smart Conditions), on page 17. You can also customize your own conditions. For more information about configuring customized conditions, see Policy Conditions, on page 32.

- Authorization profiles—defines which permissions are to be provided to the configured security group. For more information about authorization profiles, see Cisco ISE Authorization Profiles, on page 26. You can also configure new authorization profiles inline from the Policy Set pages. For more information, see Configure Authorization Policies, on page 30.

- Security groups—defines different groups of users based on common needs in the network, such as Contractors, Administration, Guests, Engineers, etc. You can configure new authorization profiles inline from the Policy Set pages. For more information, see Configure Authorization Policies, on page 30.

For Device Administration policies, Command Sets and Shell Profiles are configured in place of the authorization profiles and security groups. There is only one default authorization rule, as described in the table below, for Device Administration policy sets, and no additional predefined rules are available at this time. For additional information about command sets and shell profiles, see Control Device Administration Using TACACS+.

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Status</th>
<th>Description</th>
<th>Conditions</th>
<th>Authorization Profiles (Permissions) and Security Groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default (Network Access work center)</td>
<td>Enabled</td>
<td>This is the default authorization rule that is included in every network access policy set you create, as well as in the system default policy set. You can edit this policy to configure any authorization profile or security group based on your needs, but you cannot add conditions to it or delete it.</td>
<td>There are no conditions for this set. As the default rule, this is the last rule referred to if all rules above it cannot be matched.</td>
<td>Access is denied to the network.</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Status</td>
<td>Description</td>
<td>Conditions</td>
<td>Authorization Profiles (Permissions) and Security Groups</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>Default (Device Administration work center)</td>
<td>Enabled</td>
<td>This is the default authorization rule that is included in every device administration policy set you create, as well as in the system default policy set. You can edit this policy to configure any command set or shell group based on your needs, but you cannot add conditions to it or delete it.</td>
<td>There are no conditions for this set. As the default rule, this is the last rule referred to if all rules above it cannot be matched.</td>
<td>Command set—DenyAllCommands Shell Profile—Deny all shell profiles</td>
</tr>
<tr>
<td>Basic_Authenticated_Access</td>
<td>Enabled</td>
<td>To enable access to authenticated users.</td>
<td>Network_Access_Authentication_Passed</td>
<td>PermitAccess</td>
</tr>
<tr>
<td>WiFi_Redirect_to_Guest_Login</td>
<td>Enabled</td>
<td>To redirect users to the CWA Portal.</td>
<td>Wireless_MAB</td>
<td>Cisco_WebAuth</td>
</tr>
<tr>
<td>Wi-Fi_Guest_Access</td>
<td>Disabled</td>
<td>To permit Guest access, after a Guest user is authenticated from the WebAuth.</td>
<td>Wireless_MAB IdentityGroup Name Equals Endpoint Identity Groups:GuestEndpoints</td>
<td>PermitAccess Guest</td>
</tr>
<tr>
<td>Employee_Onboarding</td>
<td>Disabled</td>
<td>Any wireless 802.1X authentication that uses MSCHAPv2 would be redirected to the Native Supplicant Provisioning process.</td>
<td>Wireless _802.1X EAP-MSCHAPv2</td>
<td>NSP_Onboard BYOD</td>
</tr>
<tr>
<td>Employee_EAP-TLS</td>
<td>Disabled</td>
<td></td>
<td>Wireless _802.1X BYOD_is_Registered EAP-TLS MAC_in_SAN</td>
<td>PermitAccess BYOD</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Status</td>
<td>Description</td>
<td>Conditions</td>
<td>Authorization Profiles (Permissions) and Security Groups</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------</td>
<td>--------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>Compliant Devices Access</td>
<td>Disabled</td>
<td>To enable access for compliant devices.</td>
<td>Network Access, Authentication Passed</td>
<td>PermitAccess</td>
</tr>
<tr>
<td>Noncompliant Devices Redirect</td>
<td>Disabled</td>
<td></td>
<td>Network Access, Authentication Passed</td>
<td>AnyConnect Temporal Onboard</td>
</tr>
<tr>
<td>Unknown Compliance Redirect</td>
<td>Disabled</td>
<td></td>
<td>Network Access, Authentication Passed</td>
<td>AnyConnect Temporal Onboard</td>
</tr>
<tr>
<td>Profiled Non Cisco IP Phones</td>
<td>Enabled</td>
<td></td>
<td>Non_Cisco_Profiled_Phones</td>
<td>Non_Cisco_IP_Phones</td>
</tr>
<tr>
<td>Profiled Cisco IP Phones</td>
<td>Enabled</td>
<td></td>
<td>InternalUser IdentityGroup Equals Endpoint Identity Groups:Profiled:Cisco-IP-Phone</td>
<td>Cisco_IP_Phones</td>
</tr>
</tbody>
</table>

**Predefined Policy Conditions (Smart Conditions)**

Policy conditions are created from the Conditions Studio and maintained from the Conditions Studio Library. Upon initial installation, Cisco ISE includes predefined smart conditions that you can easily use when configuring your policy sets and rules, and that are used in the different default and predefined policy sets, and authentication and authorization rules. You can edit, rename and delete these predefined smart conditions based on your organization's needs. For more information about configuring customized conditions and existing predefined conditions, see Policy Conditions, on page 32.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wired 802.1X</td>
<td>• Normalized Radius RadiusFlowType equals Wired802_1x</td>
</tr>
<tr>
<td>Wireless 802.1X</td>
<td>• Normalized Radius RadiusFlowType equals Wireless802_1x</td>
</tr>
<tr>
<td>Wired MAB</td>
<td>• Normalized Radius RadiusFlowType equals WiredMAB</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Wireless_MAB</td>
<td>• Normalized Radius RadiusFlowType equals WirelessMAB</td>
</tr>
</tbody>
</table>
| WLC_Web_Authentication                     | A condition to match requests for web authentication from wireless LAN controllers, according to the corresponding Web Authentication attributes defined in the device profile.                                                                                     • RADIUS:Service-Type equals Login
• Operator: AND
• RADIUS:NAS-Port-Type equals Wireless - IEEE802.11                                                                                                                                                                                                                     |
| Catalyst Switch Local Web Authentication   | • RADIUS:Service-Type equals Outbound
• Operator: AND
• RADIUS:NAS-Port-Type equals Ethernet                                                                                                                                                                                                                                     |
| Wireless Lan Controller (WLC) Local Web Authentication | • Normalized Radius RadiusFlowType equals WirelessWebAuth                                                                                                                                                                                                                                                                                |
| Switch_Web_Authentication                  | • Normalized Radius RadiusFlowType equals WirelessWebAuth                                                                                                                                                                                                                                                                                   |
| Switch_Local_Web_Authentication            | • RADIUS:Service-Type equals Outbound
• Operator: AND
• RADIUS:NAS-Port-Type equals Ethernet                                                                                                                                                                                                                                     |
| Non_Compliant_Devices                     | Session PostureStatus equals Compliant                                                                                                                                                                                                                                                                                                     |
| Non_Cisco_Profiled_Phones                 | EndPoints LogicalProfile equals IP Phones                                                                                                                                                                                                                                                                                                  |
| Network_Access_Authentication_Passed      | Network Access AuthenticationStatus equals AuthenticationPassed                                                                                                                                                                                                                                                                         |
| MAC_in_SAN                                | CERTIFICATE Subject Alternative Name equals Radius Calling-Station-ID                                                                                                                                                                                                                                                                      |
| Guest_Flow                                | Network Access UseCase equals Guest Flow                                                                                                                                                                                                                                                                                                   |
| EAP-TLS                                    | Network Access EapAuthentication equals EAP-TLS                                                                                                                                                                                                                                                                                             |
| EAP-MSCHAPv2                               | Network Access EapAuthentication equals EAP-MSCHAPv2                                                                                                                                                                                                                                                                                         |
| Compliant_Devices                         | Session PostureStatus equals Compliant                                                                                                                                                                                                                                                                                                     |
Configure Policy Sets

Configure policy sets in order to manage your authentication and authorization policy flows.

Following are the guidelines for creating policy sets:

- Rules are configured with names, conditions, and results. You must define authentication and authorization rules in order to implement a policy set. The default pre-configured policy set that is installed automatically with ISE, as well as any new policy sets that you create, are automatically created with the existing default authentication and authorization policy rules which you can then edit or supplement.

- Conditions may be stored in the Library of the Conditions Studio and can be used for multiple policy sets thereafter.

Overview of Steps for Configuring a Policy Set

Following are the steps for configuring a complete policy set including authentication, exception and authorization rules:

1. Upon installing ISE, a default policy set is implemented, including default ISE authentication and authorization rules. The default policy set also includes additional flexible built-in rules (that are not defaults) for authentication and authorization. You can add additional rules to those policies and you can delete and change the built-in rules but you cannot remove the default rules and you cannot remove the default policy set. For more information about the defaults and built-in configurations, see Predefined and Default Configurations for Policies and Conditions, on page 9.

   If you want to customize your sets and rules, you can first create your own conditions, identity sources, security groups and authorization profiles. Alternatively, you can configure your customizations while working with the policy sets that you are creating. For example, while adding rules to your authorization policy, you can select Create a New Authorization Profile in order to customize an authorization profile and to add it to the policy set that you are currently editing.

2. Create and Manage Policy Sets, on page 20

3. Configure Authentication Policies, on page 23

4. Configure Authorization Policies, on page 30
Create and Manage Policy Sets

In order to manage authentication and authorization rules, you must first create a policy set to contain them. This task describes how to create the policy set. Subsequent tasks describe how to update the policy set and manage authentication and authorization rules.

**Step 1**
For network access policies, choose **Work Centers > Network Access > Policy Sets**. For device administration policies, choose **Work Centers > Device Administration > Device Admin Policy Sets**.

**Step 2**
From the **Actions** column on any row, click the cog icon and then from the dropdown menu, insert a new policy set by selecting any of the insert or duplicate options, as necessary. A new row appears in the Policy Sets table.

**Step 3**
From the **Status** column, click the current **Status** icon and from the dropdown list update the status for the policy set as necessary. For more information about policy set status, see **Policy Set Main Page—Configuration Settings**.

**Step 4**
For any policy set in the table, click in the **Policy Set Name** or **Description** cells to make any free-text changes necessary.

**Step 5**
To add or change conditions, hover over the cell in the **Conditions** column and click ![Conditions Studio](image). The Conditions Studio opens. For more information, see **Policy Conditions**, on page 32.

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

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

**Note**
You must use the "equals" operator for straight forward comparison. "Contains" operator can be used for multi-value attributes. "Matches" operator should be used for regular expression comparison. When "Matches" operator is used, regular expression will be interpreted for both static and dynamic values.

**Step 6**
From the **Allowed Protocols** column select the protocol or the server sequence (Radius or TACACS) to be followed for this set or click ![Create New](image) and select **Create a New Allowed Protocol**, **Create a New Radius Sequence** or **Create a TACACS Server Sequence** and follow these steps:

a) From the screen that opens, enter the details for the new protocol or sequence as follows:

- For allowed protocols settings, see **Allowed Protocols**.
- For Radius server sequence settings, see **RADIUS Server Sequences**.
- For TACACS+ server sequence settings, see **TACACS+ Server Sequence Settings**, on page 60.

b) Click **Submit**.

**Step 7**
From the top right-hand side of the table, click **Save**.

**Step 8**
From the **View** column, click ![Access Policy Set Details](image) to access all of the policy set details and to create authentication and authorization rules as well as policy exceptions. To create an authentication rule, see **Configure Authentication Policies**, on page 23. To create authorization and exception rules, see **Configure Authorization Policies**, on page 30.

**What to Do Next**

1. **Configure Authentication Policies**, on page 23
2. **Configure Authorization Policies**, on page 30
Authentication Policies

Each policy set can contain multiple authentication rules that together represent the authentication policy for that set. Priority of the authentication policies is determined based on the order to those policies as they appear within the policy set itself (from the Set view page in the Authentication Policy area).

Cisco ISE dynamically chooses the network access service (either an allowed protocol a server sequence) based on the settings configured on the policy set level, and thereafter checks the identity sources and results from the authentication and authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE dictionary. Cisco ISE allows you to create conditions as individual policy elements that can be stored in the Library and then can be reused for other rule-based policies.

The identity method, which is the result of the authentication policy, can be any one of the following:

- **Deny access**—Access to the user is denied and no authentication is performed.
- **Identity database**—A single identity database that can be any one of the following:
  - Internal users
  - Guest users
  - Internal endpoints
  - Active Directory
  - Lightweight Directory Access Protocol (LDAP) database
  - RADIUS token server (RSA or SafeWord server)
  - Certificate authentication profile
- **Identity source sequences**—A sequence of identity databases that is used for authentication.

The default policy set implemented at initial Cisco ISE installation includes the default ISE authentication and authorization rules. The default policy set also includes additional flexible built-in rules (that are not defaults) for authentication and authorization. You can add additional rules to those policies and you can delete and change the built-in rules but you cannot remove the default rules and you cannot remove the default policy set. For more information about defaults and built-in configurations, see Predefined and Default Configurations for Policies and Conditions, on page 9.

**Authentication Policy Flow**

In authentication policies, you can define multiple rules, which consist of conditions and results. ISE evaluates the conditions that you have specified and based on the result of the evaluation, assigns the corresponding results. The identity database is selected based on the first rule that matches the criteria.

You can also define an identity source sequence consisting of different databases. You can define the order in which you want Cisco ISE to look up these databases. Cisco ISE will access these databases in sequence until the authentication succeeds. If there are multiple instances of the same user in an external database, the authentication fails. There can only be one user record in an identity source.
We recommend that you use only three, or at most four databases in an identity source sequence.

Figure 2: Authentication Policy Flow

**Authentication Failures—Policy Result Options**

If you choose the identity method as deny access, a reject message is sent as a response to the request. If you choose an identity database or an identity source sequence and the authentication succeeds, the processing continues to the authorization policy configured for the same policy set. Some of the authentications fail and these are classified as follows:

- **Authentication failed**—Received explicit response that authentication has failed such as bad credentials, disabled user, and so on. The default course of action is reject.
- **User not found**—No such user was found in any of the identity databases. The default course of action is reject.
Cisco ISE allows you to configure any one of the following courses of action for authentication failures:

- **Reject**—A reject response is sent.
- **Drop**—No response is sent.
- **Continue**—Cisco ISE continues with the authorization policy.

Even when you choose the Continue option, there might be instances where Cisco ISE cannot continue processing the request due to restrictions on the protocol that is being used. For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS, or RADIUS MSCHAP, it is not possible to continue processing the request when authentication fails or user is not found.

When authentication fails, it is possible to continue to process the authorization policy for PAP/ASCII and MAC authentication bypass (MAB or host lookup). For all other authentication protocols, when authentication fails, the following happens:

- **Authentication failed**—A reject response is sent.
- **User or host not found**—A reject response is sent.
- **Process failure**—No response is sent and the request is dropped.

## Configure Authentication Policies

Define an authentication policy per policy set by configuring and maintaining multiple authentication rules, as necessary.

### Before You Begin

To perform the following task, you must be a Super Admin or Policy Admin.

Optionally, if you do not want to use the available system default, ensure you have configured any external identity stores if necessary. For more information, see **Manage Users and External Identity Sources**.

### Step 1

For network access policies, choose **Work Centers > Network Access > Policy Sets**. For device administration policies, choose **Work Centers > Device Administration > Device Admin Policy Sets**.

### Step 2

From the row for the policy set from which you would like to add or update an authentication policy, click ➤ from the View column in the Policy Sets table, in order to access all of the policy set details and to create authentication and authorization policies as well as policy exceptions.

### Step 3

Click the arrow icon next to the Authentication Policy part of the page to expand and view all of the Authentication Policy rules in the table.

### Step 4

From the Actions column on any row, click the cog icon. From the dropdown menu, insert a new authentication policy rule by selecting any of the insert or duplicate options, as necessary.
A new row appears in the Authentication Policy table.

**Step 5**  
From the **Status** column, click the current **Status** icon and from the dropdown list update the status for the policy set as necessary. For more information about status, see Authentication Policy Configuration Settings.

**Step 6**  
For any rule in the table, click in the **Rule Name** or **Description** cells to make any free-text changes necessary.

**Step 7**  
To add or change conditions, hover over the cell in the **Conditions** column and click 📋. The Conditions Studio opens. For more information, see Policy Conditions, on page 32.

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

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

**Note**  
You must use the "equals" operator for straightforward comparison. "Contains" operator can be used for multi-value attributes. "Matches" operator should be used for regular expression comparison. When "Matches" operator is used, regular expression will be interpreted for both static and dynamic values.

**Step 8**  
Organize the policies within the table according to the order by which they are to be checked and matched. To change the order of the rules, drag and drop the rows in to their correct position.

**Step 9**  
Click **Save** to save and implement your changes.

---

**What to Do Next**

1. Configure Authorization Policies, on page 30

---

**Authentication Dashlet**

The Cisco ISE dashboard provides a summary of all authentications that take place in your network and for your devices. It provides at-a-glance information about authentications and authentication failures in the Authentications dashlet.

The RADIUS Authentications dashlet provides the following statistical information about the authentications that Cisco ISE has handled:

- The total number of RADIUS authentication requests that Cisco ISE has handled, including passed authentications, failed authentications, and simultaneous logins by the same user.
- The total number of failed RADIUS authentications requests that Cisco ISE has processed.

You can also view a summary of TACACS+ authentications. The TACACS+ Authentications dashlet provides statistical information for device authentications.

For more information about device administration authentications, see TACACS Live Logs. For additional information about RADIUS Live Logs settings, see RADIUS Live Logs.

---

**ISE Community Resource**

For information on how to troubleshoot failed authentications and authorizations, see How To: Troubleshoot ISE Failed Authentications & Authorizations.
View Authentication Results

Cisco ISE provides various ways to view real-time authentication summary.

Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1

For network authentications (RADIUS), choose Operations > RADIUS > Live Logs or for device authentications (TACACS), choose Operations > TACACS > Live Logs to view the real-time authentication summaries.

Step 2

You can view the authentication summary in the following ways:

• Hover your mouse cursor over the Status icon to view the results of the authentication and a brief summary. A pop-up with status details appears.

• Enter your search criteria in any one or more of the text boxes that appear at the top of the list, and press Enter, to filter your results.

• Click the magnifier icon in the Details column to view a detailed report.

Note  As the Authentication Summary report or dashboard collects and displays the latest data corresponding to failed or passed authentications, the contents of the report appear after a delay of a few minutes.

Authentication Reports and Troubleshooting Tools

Apart from the authentication details, Cisco ISE provides various reports and troubleshooting tools that you can use to efficiently manage your network.

There are various reports that you can run to understand the authentication trend and traffic in your network. You can generate reports for historical as well as current data. The following is a list of authentication reports:

• AAA Diagnostics

• RADIUS Accounting

• RADIUS Authentication

• Authentication Summary

Authorization Policies

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

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.
Authorization profiles are used when creating authorization policies in Cisco ISE. An authorization policy is composed of authorization rules. Authorization rules have three elements: name, attributes, and permissions. The permission element maps to an authorization profile.

**Cisco ISE Authorization Profiles**

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 and network access is authorized accordingly.

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 any of the available vendor dictionaries, and these are returned when the condition for the specific authorization policy matches. Because authorization policies can include condition mapping to a single network service rule, these can also include a list of authorization checks.

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.

**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

To work with Authorization Profiles, choose **Policy > Policy Elements > Results**. From the menu on the left, choose **Authorization > Authorization Profiles**.

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 Results pane initially displays Authentication, Authorization, Profiling, Posture, Client Provisioning, and Trustsec 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.
ISE Community Resource
For an example of how to configure Media Access Control Security (MACsec) encryption between an 802.1x supplicant (Cisco AnyConnect Mobile Security) and an authenticator (switch), see MACsec Switch-host Encryption with Cisco AnyConnect and ISE Configuration Example.

Location Based Authorization

Cisco ISE integrates with Cisco Mobility Services Engine (MSE) to introduce physical location-based authorization. Cisco ISE uses information from MSE to provide differentiated network access based on the actual location of the user, as reported by MSE.

With this feature, you can use the endpoint location information to provide network access when a user is in an appropriate zone. You can also add the endpoint location as an additional attribute for policies to define more granulated policy authorization sets based on device location. You can configure conditions within authorization rules that use location-based attributes, for example:

*MSE.Location Equals LND_Campus1:Building1:Floor2:SecureZone*


You can add one or multiple MSE instances to integrate MSE-based location data to the authorization process. You can retrieve the location hierarchy data from these MSEs and configure location-based authorization rules using this data.

To track the endpoint movement, check the Track Movement check box while creating an authorization profile. Cisco ISE will query the relevant MSE for the endpoint location every 5 minutes to verify if the location was changed.

---

**Note**

Tracking multiple users will impact the performance due to frequent updates. The Track Movement option can be used for high security locations.

The Location Tree is created by using the location data retrieved from the MSE instances. You can select the location entries that are exposed to the authorization policy by using the Location Tree.

---

**Note**

You will need ISE Plus license to use the Location Services.
Add a MSE server

**Before You Begin**
To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1** Choose Administration > Network Resources > Location Services > Location Servers.

**Step 2** Click Add.

**Step 3** Enter the MSE server details, such as server name, hostname/IP address, password, and so on.

**Step 4** Click Test to test MSE connectivity using the server details that you have provided.

**Step 5** (Optional) Enter the MAC address of an endpoint in the Find Location field and click Find to check whether the endpoint is currently connected to this MSE.

If the endpoint location is found, it is displayed in the following format: Campus:Building:Floor:Zone. Sometimes, more than one entry can be displayed depending on the location hierarchy and zone settings. For example, if all the floors of a building (building1) in a campus named Campus1 are defined as non-secure zones, and the Lab Area in the first floor is defined as a secure zone, the following entries will be displayed when the endpoint is located in the Lab Area:

- Found in: Campus1#building1#floor1#LabArea
- Campus1#building1#floor1#NonSecureZone

**Step 6** Click Submit.

After a new MSE is added, go to the Location Tree page and click Get Update to retrieve its location hierarchy and add it to the Location Tree. If there are filters defined on this tree, these filters are applied on the new MSE entries as well.

---

**Location Tree**

The Location Tree is created by using the location data retrieved from the MSE instances. To view the Location Tree, choose Administration > Network Resources > Location Services > Location Tree.

If one building has multiple MSEs, Cisco ISE will collate the location details from all the MSEs and present them as a single tree.

You can select the location entries that are exposed to the authorization policy by using the Location Tree. You can also hide specific locations based on your requirements. It is recommended to update the Location Tree before hiding locations. Hidden locations will remain hidden even when the tree is updated.

If the location entries related to an authorization rule are modified or removed, you must disable the affected rules and set these locations as Unknown or select a replacement location for each affected rule. You must verify the new tree structure before applying the change or canceling the update.

Click Get Update to get the latest location hierarchy structure from all MSEs. After verifying the new tree structure, click Save to apply your changes.
**Downloadable ACLs**

You can define DACLS for the Access-Accept message to return. Use ACLs to prevent unwanted traffic from entering the network. ACLs can filter source and destination IP addresses, transport protocols, and more by using the RADIUS protocol.

After you create DACLS as named permission objects, you can add them to authorization profiles, which you can then specify as the result of an authorization policy.

You can duplicate a DACL if you want to create a new DACL that is the same, or similar to, an existing downloadable ACL.

After duplication is complete, you access each DACL (original and duplicated) separately to edit or delete them.

Note: While creating DACL, the keyword *Any* must be the source in all ACE in DACL. Once the DACL is pushed, the *Any* in the source is replaced with the IP address of the client that is connecting to the switch.

**Configure Permissions for Downloadable ACLs**

**Step 1** Choose Policy > Policy Elements > Results > Authorization > Downloadable ACLs.

**Step 2** Click the action icon and select Create DACL or click Add in the DACL Management page.

**Step 3** Enter the desired values for the DACL. Supported characters for the name field are: space, ! # $ % & ' ( ) * + , - / ; = ? @ _ { }. 

**Step 4** Click Submit.

**Machine Access Restriction for Active Directory User Authorization**

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 is 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 is assigned.

Guidelines for Configuring Authorization Policies and Profiles

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

- Rule names you create must use only the following supported characters:
  - Symbols: plus (+), hyphen (-), underscore (_), period (.), and a space ( ).
  - Alphabetic characters: A-Z and a-z.

- 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. For more information about configuring and managing conditions, see Policy Conditions, on page 32. 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 characters:
  - Symbols: hyphen (-), underscore (_), and period (.).
  - Alphabetic characters: A-Z and a-z.

- 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).

Configure Authorization Policies

The Authorization Policy part of the Policy Sets area enables you to display, create, duplicate, modify, or delete authorization policies. The following authorization policy profile sections reference example actions directed at a standard authorization policy.

Before You Begin

Before you begin this procedure, you should have a basic understanding of conditions, the basic building blocks of identity groups, conditions, and permissions, and how they are used in the Admin portal.
Ensure you have configured security group tags (SGTs) as necessary. For more information, see Security Group Access Control Lists Configuration.

Step 1
For network access policies, choose Work Centers > Network Access > Policy Sets. For device administration policies, choose Work Centers > Device Administration > Device Admin Policy Sets.

Step 2
From the View column, click to access all of the policy set details and to create authentication and authorization policies as well as policy exceptions.

Step 3
Click the arrow icon next to the Authorization Policy part of the page to expand and view the Authorization Policy table.

Step 4
From the Actions column on any row, click the cog icon. From the dropdown menu, insert a new authorization policy rule by selecting any of the insert or duplicate options, as necessary.

Step 5
A new row appears in the Authorization Policy table.

Step 6
To set the status for a policy, click the current Status icon and from the dropdown list select the necessary status from the Status column. For more information about statuses, see Authorization Policy Settings.

Step 7
For any policy in the table, click in the Rule Name cells to make any free-text changes necessary and to create a unique rule name.

Step 8
To add or change conditions, hover over the cell in the Conditions column and click . The Conditions Studio opens.

Step 9
For network access results profiles, select the relevant authorization profile from the Results Profiles dropdown list or choose Create a New Authorization Profile and when the Add New Standard Profile screen opens, perform the following steps:

a) Enter values as required to configure a new authorization profile. Supported characters for the name field are: space, ! # $ % & ' ( ) * + , . / ; = ? @ _ {}.

b) Check the Propagate to ACI check box if you want to propagate this SGT to ACI. The SXP mappings that are related to this SGT will be propagated to ACI only if they belong to a VPN that is selected in the ACI Settings page. This option is disabled by default.

c) Enter a Tag Value. Tag value can be set to be entered manually or autogenerate. You can also reserve a range for the SGT. You can configure it from the General TrustSec Settings page (Work Centers > TrustSec > Settings > General TrustSec Settings).

d) Click Submit.
For more information, see Security Groups Configuration.

**Step 10**
For TACACS+ results, select the relevant Command Sets and Shell Profiles from the Results drop-down lists or click in the Command Sets or Shell Profiles column to open the Add Commands Screen or Add Shell Profile respectively. Choose Create a New Command Set or Create a New Shell Profile and enter the fields. Refer to the Create TACACS+ Command Sets or Create TACACS+ Profiles section for more information.

**Step 11**
Organize the order by which the policies are to be checked and matched within the table.

**Step 12**
Click Save to save your changes to the Cisco ISE system database and create this new authorization policy.

### Authorization Policy Exceptions

Within each policy set, you can define regular authorization policies, as well as local exception rules (defined from the Authorization Policy Local Exceptions part in the Set view for each policy set) and global exception rules (defined from the Authorization Policy Global Exceptions part in the Set view for each policy set).

Global authorization exception policies enable you to define rules that override all authorization rules in all of your policy sets. Once you configure a global authorization exception policy, it is added to all policy sets. Global authorization exception policies can then be updated from within any of the currently configured policy sets. Every time you update a global authorization exception policy, those updates are applied to all policy sets.

The local authorization exception rule overwrites the global exception rule. The authorization rules are processed in the following order: first the local exception rule, then the global exception rule, and finally, the regular rule of the authorization policy.

Authorization exception policy rules are configured identically to Authorization policy rules. To configure exception policies, see the instructions above for configuring regular Authorization policies: Configure Authorization Policies, on page 30.

### Policy Conditions

Cisco ISE uses rule-based policies to provide network access. A policy is a set of rules and results, where the rules are made up of conditions. Cisco ISE allows you to create conditions as individual policy elements that can be stored in the system library and then reused for other rule-based policies from the Conditions Studio.

Conditions can be as simple or complex as necessary using an operator (equal to, not equal to, greater than, and so on), and a value, or by including multiple attributes, operators and complex hierarchies. At runtime, Cisco ISE evaluates a policy condition and then applies the result that you have defined based on whether the policy evaluation returns a true or a false value.

After you create a condition and assign it a unique name, you can reuse this condition multiple times across various rules and policies by selecting it from the Conditions Studio Library, for example:

**Network Conditions.MyNetworkCondition** **EQUALS** **true**

You cannot delete conditions from the Condition Studio that are used in a policy or are part of another condition.

Each condition defines a list of objects that can be included in policy conditions, resulting in a set of definitions that are matched against those presented in the request.
You can use the operator, **EQUALS true**, to check if the network condition evaluates to true (whether the value presented in the request matches at least one entry within the network condition) or **EQUALS false** to test whether the network condition evaluates to false (does not match any entry in the network condition).

Cisco ISE also offers predefined smart conditions that you can use in your policies separately or as building blocks in your own customized conditions, and which you can update and change based on your needs. These smart conditions are as described in **Predefined and Default Configurations for Policies and Conditions**, on page 9.

You can create the following unique network conditions to restrict access to the network:

- **Endstation Network Conditions**—Based on endstations that initiate and terminate the connection.
  
  Cisco ISE evaluates the remote address TO field (which is obtained based on whether it is a TACACS+ or RADIUS request) to identify whether it is the IP address, MAC address, calling line identification (CLI), or dialed number identification service (DNIS) of the endpoint.

  In a RADIUS request, this identifier is available in Attribute 31 (Calling-Station-Id).

  In a TACACS+ request, if the remote address includes a slash (/), the part before the slash is taken as the FROM value and the part after the slash is taken as the TO value. For example, if a request has CLI/DNIS, CLI is taken as the FROM value and DNIS is taken as the TO value. If a slash is not included, the entire remote address is taken as the FROM value (whether IP address, MAC address, or CLI).

- **Device Network Conditions**—Based on the AAA client that processes the request.
  
  A network device can be identified by its IP address, device name that is defined in the network device repository, or Network Device Group.

  In a RADIUS request, if Attribute 4 (NAS-IP-Address) is present, Cisco ISE obtains the IP address from this attribute. If Attribute 32 (NAS-Identifier) is present, Cisco ISE obtains the IP address from Attribute 32. If these attributes are not found, it obtains the IP address from the packet that it receives.

  The device dictionary (NDG dictionary) contains network device group attributes such as Location, Device Type, or other dynamically created attributes that represent NDGs. These attributes contain the groups that the current device is related to.

- **Device Port Network Conditions**—Based on the device's IP address, name, NDG, and port (physical port of the device that the endstation is connected to).

  In a RADIUS request, if Attribute 5 (NAS-Port) is present in the request, Cisco ISE obtains the value from this attribute. If Attribute 87 (NAS-Port-Id) is present in the request, Cisco ISE obtains the request from Attribute 87.

  In a TACACS+ request, Cisco ISE obtains this identifier from the port field of the start request (of every phase).

For more information about these unique conditions, see **Special Network Access Conditions**, on page 47.

**Attributes and Dictionaries—Tools for Configuring Conditions**

Attributes are stored in different system dictionaries. Attributes are used to configure conditions. Attributes can be reused in multiple conditions.

To reuse a valid attribute when creating 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 in which the authentication succeeded.

When an identity source sequence is used 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 a condition where a user authenticated using an LDAP directory (LDAP13) in the authorization policy, you can define the following reusable condition:

\[
\text{If } \text{NetworkAccess.AuthenticationStatus} \text{ EQUALS AuthenticationPassed AND} \\
\text{NetworkAccess.AuthenticationIdentityStore} \text{ EQUALS LDAP13}
\]

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 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.

Calling-Station-ID is accepted only in AA:BB:CC:DD:EE:FF format in Cisco ISE 2.3 and above. Hence, authorization condition might fail if the Calling-Station-ID is provided in AA-BB-CC-DD-EE-FF format.

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".

**Supported Dictionaries for Network Access Policies**

Cisco ISE supports the following system-stored dictionaries that contain the different attributes necessary when building conditions and rules for your authentication and authorization policies:

- System-defined dictionaries
  - CERTIFICATE
  - DEVICE
  - RADIUS

- RADIUS vendor dictionaries
  - Airespace
  - Cisco
For authorization policy types, the verification configured in the condition must comply with the authorization profiles to be returned.

Verifications typically include one or more conditions that include a user-defined name that can then be added to a library and reused by other policies.

The following sections describe the supported attributes and dictionaries available for configuring conditions.

**Attributes Supported by Dictionaries**

The table lists the fixed attributes that are supported by dictionaries, which can be used in policy conditions. Not all of these attributes are available for creating all types of conditions.

For example, while creating a condition to choose the access service in authentication policies, you will only see the following network access attributes: Device IP Address, ISE Host Name, Network Device Name, Protocol, and Use Case.

You can use the attributes listed in the following table in policy conditions.

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Attributes</th>
<th>Allowed Protocol Rules and Proxy</th>
<th>Identity Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Device Type (predefined network device group)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Device Location (predefined network device group)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other Custom Network Device Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Model Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RADIUS</td>
<td>All attributes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Cisco-BBSM
*Cisco-VPN3000
*Microsoft
*Network access
<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Attributes</th>
<th>Allowed Protocol Rules and Proxy</th>
<th>Identity Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Access</td>
<td>ISE Host Name</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>AuthenticationMethod</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>AuthenticationStatus</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>CTSDeviceID</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Device IP Address</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>EapAuthentication (the EAP method that is used during authentication of a user of a machine)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>EapTunnel (the EAP method that is used for tunnel establishment)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Protocol</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>UseCase</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>UserName</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>WasMachineAuthenticated</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Dictionary</td>
<td>Attributes</td>
<td>Allowed Protocol Rules and Proxy</td>
<td>Identity Rules</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------</td>
<td>----------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Certificate</td>
<td>Common Name</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Country</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E-mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LocationSubject</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Organization</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Organization Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Serial Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>State or Province</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject Alternative Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject Alternative Name - DNS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject Alternative Name - E-mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject Alternative Name - Other Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject Serial Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Common Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Organization</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Organization Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Location</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Country</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Email</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Serial Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - State or Province</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Street Address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Navigate the Conditions Studio

Use the Conditions Studio to create, manage and re-use conditions. Conditions can include more than one rule, and can be built with any complexity including only one level, or multiple hierarchical levels. When using the Conditions Studio to create new conditions, you can use the condition blocks that you have already stored in the Library and you can also update and change those stored condition blocks. While creating and managing conditions later, easily find the blocks and attributes that you need by using quick category filters, and more.

For network access policies, choose Work Centers > Network Access > Policy Sets. For device administration policies, choose Work Centers > Device Administration > Device Admin Policy Sets.

To edit or change conditions that have already been applied to the specific rule in any of your policy sets, hover over the cell in the Conditions column and click , or click the plus sign + from the Conditions column in the Policy Set table in order to create a new condition, which you can then immediately apply to the same policy set or alternatively you can also save in the Library for future use.
The following figure shows the main elements of the Conditions Studio.

**Figure 3: Conditions Studio**

The Condition Studio is divided into two main parts: the Library and the Editor. The Library stores condition blocks for reuse while the Editor enables you to edit those saved blocks and create new ones.

The following table describes the different parts of the Conditions Studio:
<table>
<thead>
<tr>
<th></th>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Library</td>
<td>Displays the list of all condition blocks that were created and saved in the ISE database for reuse. To use these condition blocks as part of your currently edited condition, drag and drop them from the Library to the relevant level in the Editor and update the operators as necessary. Conditions stored in the Library are all represented by the Library icon, because conditions can be associated with more than one category. Next to each condition in the Library you can also find the icon. Hover over this icon to view a full description of the condition, view the categories to which it is associated, and to delete the condition from the library entirely. You cannot delete conditions if they are used by policies. Drag and drop any of the Library conditions into the Editor in order to use it for the currently edited policy on its own or as a building block for a more complex condition to be used in the current policy or saved as a new condition in the Library. You can also drag and drop the condition in the Editor in order to make changes to that condition and then save it under the same or a new name in the Library. There are also predefined conditions upon installation. These conditions can also be changed and deleted.</td>
</tr>
<tr>
<td>2</td>
<td>Search and filter</td>
<td>Search conditions by name or filter them by category. In a similar manner, you can also search and filter attributes from the <strong>Click to add an attribute</strong> field in the Editor. The icons on the toolbar represent different attribute categories such as subject, address and so forth. Click an icon to view attributes related to the specific category and click a highlighted icon from the category toolbar in order to deselect it, thereby removing the filter.</td>
</tr>
<tr>
<td>3</td>
<td>Conditions List</td>
<td>The complete list of all conditions in the Library, or the list of conditions in the Library based on the search or filter results.</td>
</tr>
<tr>
<td>4</td>
<td>Editor</td>
<td>Create new conditions to use immediately as well as to save them in the system Library for future use, and edit existing conditions and save those changes in the Library for immediate and future use. When opening the Conditions Studio in order to create a new condition (click the plus sign from any of the policy set tables), the Editor appears with only a single, empty, line to which you can add your first rule. When the Editor opens with empty fields, no operator icons appear</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>The Editor is divided into different virtual columns and rows. Columns represent different hierarchical levels, and each column is indented based on its position in the hierarchy; rows represent individual rules. You can create single or multiple rules per level, and you can include multiple levels. The example in the image above displays a condition that is in the process of being built or edited and includes a hierarchy of rules, where both the first and second levels in the figure are marked with the number 5. The rules on the top parent level use the operator OR. In order to change the operator once you have selected it and created the hierarchical level, simply select the relevant option from the dropdown list that appears in this column. In addition to the operator dropdown list, each rule has a relevant icon in this column, indicating what category it belongs to. If you hover over the icon, a tooltip indicates the name of the category. Once saved to the library, all condition blocks are assigned the Library icon, replacing the category icons that appeared in the Editor. Finally, if a rule is configured to exclude all relevant matched items, then the Is-Not indicator also appears in this column. For example, if a location attribute with the value London is set to Is-Not then all devices from London will be denied access.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>This area displays the options available when working with hierarchical levels as well as multiple rules within a condition. When you hover over any column or row the relevant actions appear. When you select an action, it is applied to that section and all of the children sections. For example, with five levels in Hierarchy A, if you choose AND from any rule in the third level, then a new hierarchy, Hierarchy B, is created under the original rule so that the original rule becomes the parent rule for Hierarchy B, which is embedded in Hierarchy A. When you first open the Condition Studio in order to create a new condition from scratch, the Editor area includes only one line for a single rule that you can configure, as well as the option to select relevant operators or to drag and drop relevant conditions from the Library. Additional levels can be added to the condition with the AND and OR operator options. Choose New to create a new rule on the same level from which you clicked the option. The New option only appears once you have configured at least one rule on the top level of the hierarchy.</td>
<td></td>
</tr>
</tbody>
</table>
Configure, Edit and Manage Policy Conditions

Use the Conditions Studio to create, manage and re-use conditions. Conditions can include more than one rule, and can be built with any complexity including only one level, or multiple hierarchical levels. Manage the condition hierarchy from the Editor side of the Conditions Studio as in the following image:

*Figure 4: Editor—Conditions Hierarchy*

When creating new conditions, you can use the condition blocks that you have already stored in the Library and you can also update and change those stored condition blocks. While creating and managing conditions, easily find the blocks and attributes that you need by using quick category filters, and more.

When creating and managing condition rules, use attributes, operators and values.

Cisco ISE also includes predefined condition blocks for some of the most common use cases. You can edit these predefined conditions to suit your requirements. Conditions saved for re-use, including the out-of-the-box blocks, are stored in the Library of the Condition Studio, as described in this task.
To perform the following task, you must be a Super Admin or Policy Admin.

**Step 1**  

**Step 2**  
Access the Conditions Studio to create a new condition and to edit existing condition blocks, in order to then use those conditions as part of the rules you configure for the specific policy set (and its associated policies and rules), or in order to save to the Library for future use:

a) Click + from the Conditions column in the Policy Set table on the main Policy Set page in order to create conditions that are relevant for the entire policy set (conditions that are checked prior to matching authentication policy rules).

b) Alternatively, click + from a specific policy set row in order to view the Set view, including all rules for authentication and authorization. From the Set view, hover over the cell in the Conditions column from any of the rule tables and click + to open the Conditions Studio.

c) If you are editing conditions that have already been applied to the policy set, then click to access the Conditions Studio.

The Conditions Studio opens. If you have opened it in order to create new conditions, then it appears as in the following image. For a description of the fields and to see an example of the Conditions Studio when you have opened it to edit conditions that were already applied to the policy set, see Navigate the Conditions Studio, on page 38.

**Figure 5: Conditions Studio—Creating a New Condition**

![Conditions Studio](image)

**Step 3**  
Use an existing condition block from the Library as a rule in the condition that you are creating or editing.
a) Filter by selecting the relevant category from the category toolbar—in the Library, all blocks that contain an attribute from the selected category are displayed. Condition blocks that contain more than one rule but that use an attribute from the selected category for at least one of those rules, are also displayed. If there are additional filters added, then the results displayed include only condition blocks from the specific filter that also match the other filters that were included. For example, if you select the Ports category from the toolbar and you also enter "auth" as free text in the Search by Name field, then all blocks related to ports with "auth" in their names are displayed. Click the highlighted icon again from the category toolbar in order to deselect it, thereby removing that filter.

b) Search for condition blocks with free text—in the Search by Name free text field, enter any term, or part of a term, that appears in the name of the block for which you are searching. As you type, the system dynamically searches for relevant results in real time. If no category is selected (none of the icons are highlighted) then the results include condition blocks from all categories. If a category icon is already selected (the displayed list is already filtered), then the results displayed include only blocks in the specific category that use the specific text.

c) Once you find the condition block, drag it to the Editor and drop it in the correct level of the block that you are building. If you drop it in the incorrect location, you can drag and drop it again from within the Editor, until it is placed correctly.

d) Hover over the block from the Editor and click **Edit** to change the rule, in order make changes relevant for the condition you are working on, to overwrite the rule in the Library with those changes or alternatively to save the rule as a new block in the Library.

The block, which is read-only when dropped into the Editor can now be edited and has the same fields, structures, lists and actions as all other customized rules in the Editor. Continue to the next steps for more information in editing this rule.

**Step 4**  
Add an operator to the current level in order to then add additional rules on the same level—choose **AND**, **OR** or **Set to 'Is not'**. **Set to 'Is not'** can also be applied to individual rules.

**Step 5**  
Create and edit rules using the attribute dictionaries—click in the **Click to add an attribute** field. The Attribute Selector opens as in the following image:
The parts of the Attribute Selector are as described in the following table:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Category toolbar</td>
<td>Contains a unique icon for each of the different attribute categories. Choose any attribute category icon to filter the view by category. Click a highlighted icon in order to deselect it, thereby removing the filter.</td>
</tr>
<tr>
<td>Dictionary</td>
<td>Indicates the name of the dictionary in which the attribute is stored. Select a specific dictionary from the dropdown in order to filter attributes by vendor dictionary.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Indicates the name of the attribute. Filter attributes by typing free text for the attribute name in the available field. As you type, the system dynamically searches for relevant results in real time.</td>
</tr>
<tr>
<td>ID</td>
<td>Indicates the unique attribute identification number. Filter attributes by typing the ID number in the available field. As you type, the system dynamically searches for relevant results in real time.</td>
</tr>
</tbody>
</table>
a) From the Attribute Selector search, filter and search for the attribute you need. When you filter or enter free text in any part of the Attribute Selector, if there are no other filters activated, then the results include all attributes relevant for the selected filter only. If more than one filter is used, then the search results that are displayed match all filters. For example, if you click the Port icon from the toolbar and type "auth" in the Attribute column, then only attributes from the Port category that have "auth" in their name are displayed. When you choose a category, the icon in the toolbar is highlighted in blue and the filtered list is displayed. Click the highlighted icon again from the category toolbar in order to deselect it, thereby removing the filter.

b) Choose the relevant attribute in order to add it to the rule. The Attribute Selector closes and the attribute you selected is added to the Click to add an attribute field.

c) From the Equals dropdown list, select the relevant operator. Not all attributes you select will include the "Equals," "Not Equals," "Matches," "Starts With," or "Not Starts With" operator options.

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

You must use the "equals" operator for straight forward comparison. "Contains" operator can be used for multi-value attributes. "Matches" operator should be used for regular expression comparison. When "Matches" operator is used, regular expression will be interpreted for both static and dynamic values.

d) From the Attribute value field do one of the following:

- Type a free text value in the field
- Select a value from the list that dynamically loads (when relevant—depending on the attribute selected in the previous step)
- Use another attribute as the value for the condition rule—choose the table icon next to the field in order to open the Attribute Selector and then search, filter and select the relevant attribute. The Attribute Selector closes and the attribute you selected is added to the Attribute value field.

### Step 6

Save rules in the Library as a condition block.

a) Hover over the rule or hierarchy of rules that you would like to save as a block in the Library. The Duplicate and Save buttons appear for any rule or group of rules that can be saved as a single condition block. If you would like to save a group of rules as a block, choose the action button from the bottom of the entire hierarchy in the blocked area for the entire hierarchy.

b) Click Save. The Save condition screen pops up.

c) Choose:

- Save to Existing Library Condition—choose this option to overwrite an existing condition block in the Library with the new rule you have created and then select the condition block that you want to overwrite from the Select from list dropdown list.
- Save as a new Library Condition—type a unique name in the Condition Name field for the block.
d) Optionally, enter a description in the Description field. This description appears when you hover over the info icon for any condition block from within the Library, enabling you to quickly identify the different condition blocks and their uses.

e) Click Save to save the condition block in the Library.

**Step 7** To create a new rule on a new child level—click AND or OR to apply the correct operator between the existing parent hierarchy and the child hierarchy that you are creating. A new section is added to the Editor hierarchy with the selected operator, as a child of the rule or hierarchy from which you chose the operator.

**Step 8** To create a new rule on a a current existing level—click New from the relevant level. A new empty row appears for a new rule in the same level as the level from which you began.

**Step 9** Click X to remove any condition from the Editor and all of its children.

**Step 10** Click Duplicate to automatically copy and paste the specific condition within the hierarchy, thereby creating additional identical children at the same level. You can duplicate individual rules with or without their children, depending on the level from which you click the Duplicate button.

**Step 11** Click Use from the bottom of the page to save the condition you created in the Editor and to implement that condition in your policy set.

---

**Special Network Access Conditions**

This section describes unique conditions that can be useful when creating your policy sets. These conditions cannot be created from the Conditions Studio and so have their own unique processes.

**Configure Device Network Conditions**

**Step 1** Choose Policy > Policy Elements > Conditions > Network Conditions > Device Network Conditions.

**Step 2** Click Add.

**Step 3** Enter a name and description for the network condition.

**Step 4** Enter the following details:

- IP Addresses—You can add a list of IP addresses or subnets, one per line. The IP address/subnet can be in IPv4 or IPv6 format.
- Device Name—You can add a list of device names, one per line. You must enter the same device name that is configured in the Network Device object.
- Device Groups—You can add a list of tuples in the following order: Root NDG, comma, and an NDG (that it under the root NDG). There must be one tuple per line.

**Step 5** Click Submit.
Configure Device Port Network Condition

Step 1  Choose Policy > Policy Elements > Conditions > Network Conditions > Device Port Network Conditions.
Step 2  Click Add.
Step 3  Enter a name and description for the network condition.
Step 4  Enter the following details:
  • IP Addresses—Enter the details in the following order: IP address or subnet, comma, and a port (that is used by the device). There must be one tuple per line.
  • Devices—Enter the details in the following order: device name, comma, and a port. There must be one tuple per line. You must enter the same device name that is configured in the Network Device object.
  • Device Groups—Enter the details in the following order: Root NDG, comma, NDG (that it under the root), and a port. There must be one tuple per line.

Step 5  Click Submit.

Configure Endstation Network Conditions

Step 1  Choose Policy > Policy Elements > Conditions > Network Conditions > Endstation Network Conditions.
Step 2  Click Add.
Step 3  Enter a name and description for the network condition.
Step 4  Enter the following details:
  • IP Addresses—You can add a list of IP addresses or subnets, one per line. The IP address/subnet can be in IPv4 or IPv6 format.
  • MAC Addresses—You can enter a list of Endstation MAC addresses and Destination MAC addresses, separated by a comma. Each MAC address must include 12 hexadecimal digits and must be in one of the following formats: nn:nn:nn:nn:nn:nn, nn-nn-nn-nn-nn-nn, nnnn.nnnn.nnnn, or nnnnnnnnnnnn. If the Endstation MAC or the Destination MAC is not required, use the token '-ANY-' instead.
  • CLI/DNIS—You can add a list of Caller IDs (CLI) and Called IDs (DNIS), separated by a comma. If the Caller ID (CLI) or the Called ID (DNIS) is not required, use the token '-ANY-' instead.

Step 5  Click Submit.
Create 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 directed by the attribute settings you make.

Before You Begin

To perform the following task, you must be a Super Admin or Policy Admin.

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

Step 2
Enter appropriate values in the fields.

- In the Standard Settings area, specify the time and date to provide access.
- In the Exceptions area, specify the time and date range to limit access.

Step 3
Click Submit.

Use IPv6 Attributes in Authorization Policies

Cisco ISE can detect, manage, and secure IPv6 traffic from endpoints.

When an IPv6-enabled endpoint connects to the Cisco ISE network, it communicates with the Network Access Device (NAD) over an IPv6 network. The NAD conveys the accounting and profiling information from the endpoint (including IPv6 values) to Cisco ISE over an IPv4 network. You can configure authorization profiles and policies in Cisco ISE using IPv6 attributes to process such requests from IPv6-enabled endpoints and ensure that the endpoint is compliant.

Wildcard characters are supported in IPv6 prefix and IPv6 interface values. For example: 2001:db8:1234::/48.

Supported IPv6 address formats include:

- Full notation: Eight groups of four hexadecimal digits separated by colons. For example, 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Shortened notation: Exclude leading zeros in a group; replace groups of zeros with two consecutive colons. For example: 2001:db8:85a3::8a2e:370:7334
- Dotted-quad notation (IPv4-mapped and IPv4 compatible-IPv6 addresses): For example, ::ffff:192.0.2.128

Supported IPv6 attributes include:

- NAS-IPv6-Address
- Framed-Interface-Id
- Framed-IPv6-Prefix
Use IPv6 Attributes in Authorization Policies

- Login-IPv6-Host
- Framed-IPv6-Route
- Framed-IPv6-Pool
- Delegated-IPv6-Prefix
- Framed-IPv6-Address
- DNS-Server-IPv6-Address
- Route-IPv6-Information
- Delegated-IPv6-Prefix-Pool
- Stateful-IPv6-Address-Pool

Supported Cisco Attribute-Value pairs and their equivalent IETF attributes are listed in the table below:

<table>
<thead>
<tr>
<th>Cisco Attribute-Value Pairs</th>
<th>IETF Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6:addrv6=&lt;ipv6 address&gt;</td>
<td>Framed-ipv6-Address</td>
</tr>
<tr>
<td>ipv6:stateful-ipv6-address-pool=&lt;name&gt;</td>
<td>Stateful-IPv6-Address-Pool</td>
</tr>
<tr>
<td>ipv6:delegated-ipv6-pool=&lt;name&gt;</td>
<td>Delegated-IPv6-Prefix-Pool</td>
</tr>
<tr>
<td>ipv6:ipv6-dns-servers-addr=&lt;ipv6 address&gt;</td>
<td>DNS-Server-IPv6-Address</td>
</tr>
</tbody>
</table>

The RADIUS Live Logs page, RADIUS Authentication report, RADIUS Accounting report, Current Active Session report, RADIUS Error report, Misconfigured NAS report, EPS Audit report, and Misconfigured Supplicant report support IPv6 addresses. You can view the details about these sessions from the RADIUS Live Logs page or from any of these reports. You can filter the records based on IPv4, IPv6, or MAC addresses.

Note

If you connect an Android device to an IPv6 enabled DHCPv6 network, it receives only the link-local IPv6 address from the DHCP server. Hence, global IPv6 address is not displayed in the Live Logs and in the Endpoints page (Work Centers > Network Access > Identities > Endpoints).

The following procedure describes how to configure IPv6 attributes in authorization policies.
Before You Begin

Ensure that the NADs in your deployment support AAA with IPv6. Refer to AAA Support for IPv6 for information on how to enable AAA support for IPv6 on your NADs.

---

**Step 1** For network access policies, choose Work Centers > Network Access > Policy Sets. For device administration policies, choose Work Centers > Device Administration > Device Admin Policy Sets.

**Step 2** Create authorization rules. See Configure Authorization Policies, on page 30.

**Step 3** When creating authorization rules, create a condition from the Condition Studio. In the Condition Studio, from the RADIUS dictionary, choose the RADIUS IPv6 attribute, the operator, and the value. See Configure, Edit and Manage Policy Conditions, on page 42.

**Step 4** Click Save to save the authorization rules in the policy set.

---

**Policy Set Protocol Settings**

You must define global protocol settings in Cisco ISE before you can use these protocols to create, save and implement a policy set. You can use the Protocol Settings page to define global options for the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and Protected Extensible Authentication Protocol (PEAP) protocols, which communicate with the other devices in your network.

**Supported Network Access Policy Set Protocols**

The following is a list of protocols that you can choose while defining your Network Access Policy Set policy:

- Password Authentication Protocol (PAP)
- Protected Extensible Authentication Protocol (PEAP)
- Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2)
- Extensible Authentication Protocol-Message Digest 5 (EAP-MD5)
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
- Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS)
- Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)

**Guidelines for Using EAP-FAST as Protocol**

Follow these guidelines when using EAP-FAST as an authentication protocol:

- It is highly recommended to enable EAP-TLS inner method when the EAP-FAST accept client certificate is enabled on authenticated provisioning. EAP-FAST accept client certificate on authenticated provisioning
is not a separate authentication method but a shorter form of client certificate authentication that uses the same certificate credentials type to authenticate a user but does not require to run an inner method.

- Accept client certificate on authenticated provisioning works with PAC-less full handshake and authenticated PAC provisioning. It does not work for PAC-less session resume, anonymous PAC provisioning, and PAC-based authentication.

- EAP attributes are displayed per identity (so in EAP chaining displayed twice) are shown in authentication details in monitoring tool in order user then machine even if authentication happens in different order.

- When EAP-FAST authorization PAC is used then EAP authentication method shown in live logs is equal to the authentication method used for full authentication (as in PEAP) and not as Lookup.

- In EAP chaining mode when tunnel PAC is expired then ISE falls back to provisioning and AC requests User and Machine authorization PACs - Machine Authorization PAC cannot be provisioned. It will be provisioned in the subsequent PAC-based authentication conversation when AC requests it.

- When Cisco ISE is configured for chaining and AC for single mode then AC response with IdentityType TLV to ISE. However, the second identity authentication fails. You can see from this conversation that client is suitable to perform chaining but currently is configured for single mode.

- Cisco ISE supports retrieval attributes and groups for both machine and user in EAP-FAST chaining only for AD. For LDAP and Internal DB ISE uses only the last identity attributes.

---

**Note**

"EAP-FAST cryptobinding verification failed" message might be seen if EAP-FAST authentication protocol is used for High Sierra MAC OSX devices. We recommend that you configure the Preferred EAP Protocol field in the Allowed Protocols page to use PEAP or EAP-TLS instead of EAP-FAST for High Sierra MAC OSX devices.

---

## Configure EAP-FAST Settings

### Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Administration &gt; System &gt; Settings &gt; Protocols &gt; EAP-FAST &gt; EAP Fast Settings.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter the details as required to define the EAP-FAST protocol.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Revoke if you want to revoke all the previously generated master keys and PACs.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Save to save the EAP-FAST settings.</td>
</tr>
</tbody>
</table>

## Generate the PAC for EAP-FAST

You can use the Generate PAC option in the Cisco ISE to generate a tunnel or machine PAC for the EAP-FAST protocol.
Before You Begin

To perform the following task, you must be a Super Admin or System Admin.

**Step 1**  Choose Administration > System > Settings.

**Step 2**  From the Settings navigation pane on the left, click Protocols.

**Step 3**  Choose EAP-FAST > Generate PAC.

**Step 4**  Enter the details as required to generate machine PAC for the EAP-FAST protocol.

**Step 5**  Click Generate PAC.

Using EAP-TTLS as Authentication Protocol

EAP-TTLS is a two-phase protocol that extends the functionality of EAP-TLS protocol. Phase 1 builds the secure tunnel and derives the session keys used in Phase 2 to securely tunnel attributes and inner method data between the server and the client. You can use the attributes tunneled during Phase 2 to perform additional authentications using a number of different mechanisms.

Cisco ISE can process authentications from a variety of TTLS supplicants including:

- AnyConnect Network Access Manager (NAM) on Windows
- Windows 8.1 native supplicant
- Secure W2 (also called as JoinNow on MultiOS)
- MAC OS X native supplicant
- IOS native supplicant
- Android based native supplicant
- Linux WPA supplicant

**Note**

If cryptobinding is required, you must use EAP-FAST as the inner method.
Configure EAP-TTLS Settings

**Before You Begin**

To perform the following task, you must be a Super Admin or System Admin.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Administration &gt; System &gt; Settings &gt; Protocols &gt; EAP-TTLS.</td>
</tr>
<tr>
<td>2</td>
<td>Enter the required details in the EAP-TTLS Settings page.</td>
</tr>
<tr>
<td>3</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

Configure EAP-TLS Settings

**Before You Begin**

To perform the following task, you must be a Super Admin or System Admin.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Administration &gt; System &gt; Settings &gt; Protocols &gt; EAP-TLS.</td>
</tr>
<tr>
<td>2</td>
<td>Enter the details as required to define the EAP-TLS protocol.</td>
</tr>
<tr>
<td>3</td>
<td>Click Save to save the EAP-TLS settings.</td>
</tr>
</tbody>
</table>

Configure PEAP Settings

**Before You Begin**

To perform the following task, you must be a Super Admin or System Admin.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Administration &gt; System &gt; Settings.</td>
</tr>
<tr>
<td>2</td>
<td>From the Settings navigation pane on the left, click Protocols.</td>
</tr>
<tr>
<td>3</td>
<td>Choose PEAP.</td>
</tr>
<tr>
<td>4</td>
<td>Enter the details as required to define the PEAP protocol.</td>
</tr>
<tr>
<td>5</td>
<td>Click Save to save the PEAP settings.</td>
</tr>
</tbody>
</table>
Configure RADIUS Settings

You can configure the RADIUS settings to detect the clients that fail to authenticate and to suppress the repeated reporting of successful authentications.

Step 1
Choose Administration > System > Settings.

Step 2
From the Settings navigation pane, click Protocols.

Step 3
Choose RADIUS.

Step 4
Enter the details as required to define the RADIUS settings.

Step 5
Click Save to save the settings.

Configure Security Settings

To configure the security settings:

Step 1
Choose Administration > System > Settings > Protocols > Security Settings.

Step 2
In the Security Settings page, select the required options:

- Allow TLS 1.0—Allows TLS 1.0 for communication with legacy peers for the following workflows:
  - Cisco ISE is configured as EAP server
  - Cisco ISE downloads CRL from HTTPS or secure LDAP server
  - Cisco ISE is configured as secure syslog client
  - Cisco ISE is configured as secure LDAP client

  **Note**  Allow TLS 1.0 option is disabled by default in ISE 2.3 and above. TLS 1.0 is not supported for TLS based EAP authentication methods (EAP-TLS, EAP-FAST/TLS) and 802.1X supplicants when this option is disabled. If you want to use the TLS based EAP authentication methods in TLS 1.0, check the Allow TLS 1.0 check box in the Security Settings page ( Administration > System > Settings > Protocols > Security Settings).

- Allow TLS 1.1—Allows TLS 1.1 for communication with legacy peers for the following workflows:
  - Cisco ISE is configured as EAP server
  - Cisco ISE downloads CRL from HTTPS or secure LDAP server
  - Cisco ISE is configured as secure syslog client
  - Cisco ISE is configured as secure LDAP client
Note Allow TLS 1.1 option is disabled by default in Cisco ISE 2.3 and above. TLS 1.1 is not supported for TLS based EAP authentication methods (EAP-TLS, EAP-FAST/TLS) and 802.1X supplicants when this option is disabled. If you want to use the TLS based EAP authentication methods in TLS 1.1, check the Allow TLS 1.1 check box in the Security Settings page (Administration > System > Settings > Protocols > Security Settings).

- Allow SHA1 Ciphers—Allows SHA-1 ciphers for communication with peers for the following workflows:
  * Cisco ISE is configured as EAP server
  * Cisco ISE is configured as RADIUS DTLS server
  * Cisco ISE is configured as RADIUS DTLS client
  * Cisco ISE downloads CRL from HTTPS or secure LDAP server
  * Cisco ISE is configured as secure syslog client
  * Cisco ISE is configured as secure LDAP client

  This option is enabled by default.

Note It is recommended to use SHA-256 or SHA-384 ciphers for enhanced security.

- Allow ECDHE-RSA Ciphers—Allow ECDHE-RSA ciphers for communication with peers for the following workflows:
  * Cisco ISE is configured as EAP server
  * Cisco ISE is configured as RADIUS DTLS server
  * Cisco ISE is configured as RADIUS DTLS client
  * Cisco ISE downloads CRL from HTTPS or secure LDAP server
  * Cisco ISE is configured as secure syslog client
  * Cisco ISE is configured as secure LDAP client

  This option is enabled by default.

- Allow 3DES ciphers—Allow 3DES ciphers for communication with peers for the following workflows:
  * Cisco ISE is configured as EAP server
  * Cisco ISE is configured as RADIUS DTLS server
  * Cisco ISE is configured as RADIUS DTLS client
  * Cisco ISE downloads CRL from HTTPS or secure LDAP server
  * Cisco ISE is configured as secure syslog client
  * Cisco ISE is configured as secure LDAP client

  This option is enabled by default.

- Accept Certificates without Validating Purpose—When ISE acts as an EAP or RADIUS DTLS server, client certificates are accepted without checking whether the Key Usage extension contains keyAgreement bit for ECDHE-ECDSA ciphers or keyEncipherment bit for other ciphers. This option is enabled by default.
• Allow DSS ciphers for ISE as a client—When Cisco ISE acts as a client, allow DSS ciphers for communication with server for the following workflows:
  ◦ Cisco ISE is configured as RADIUS DTLS client
  ◦ Cisco ISE downloads CRL from HTTPS or secure LDAP server
  ◦ Cisco ISE is configured as secure syslog client
  ◦ Cisco ISE is configured as secure LDAP client

This option is enabled by default.

• Allow Legacy Unsafe TLS Renegotiation for ISE as a Client—Allows communication with legacy TLS servers that do not support safe TLS renegotiation for the following workflows:
  ◦ Cisco ISE downloads CRL from HTTPS or secure LDAP server
  ◦ Cisco ISE is configured as secure syslog client
  ◦ Cisco ISE is configured as secure LDAP client

This option is enabled by default.

### Step 3
Click Save.

---

**Cisco ISE Acting as a RADIUS Proxy Server**

Cisco ISE can function both as a RADIUS server and as a RADIUS proxy server. When it acts as a proxy server, Cisco ISE receives authentication and accounting requests from the network access server (NAS) and forwards them to the external RADIUS server. Cisco ISE accepts the results of the requests and returns them to the NAS.

Cisco ISE can simultaneously act as a proxy server to multiple external RADIUS servers. You can use the external RADIUS servers that you configure here in RADIUS server sequences. The External RADIUS Server page lists all the external RADIUS servers that you have defined in Cisco ISE. You can use the filter option to search for specific RADIUS servers based on the name or description, or both. In both simple and rule-based authentication policies, you can use the RADIUS server sequences to proxy the requests to a RADIUS server.

The RADIUS server sequence strips the domain name from the RADIUS-Username attribute for RADIUS authentications. This domain stripping is not applicable for EAP authentications, which use the EAP-Identity attribute. The RADIUS proxy server obtains the username from the RADIUS-Username attribute and strips it from the character that you specify when you configure the RADIUS server sequence. For EAP authentications, the RADIUS proxy server obtains the username from the EAP-Identity attribute. EAP authentications that use the RADIUS server sequence will succeed only if the EAP-Identity and RADIUS-Username values are the same.

### Configure External RADIUS Servers

You must configure the external RADIUS servers in the Cisco ISE to enable it to forward requests to the external RADIUS servers. You can define the timeout period and the number of connection attempts.
Before You Begin

- You cannot use the external RADIUS servers that you create in this section by themselves. You must create a RADIUS server sequence and configure it to use the RADIUS server that you create in this section. You can then use the RADIUS server sequence in authentication policies.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1
Choose Administration > Network Resources > External RADIUS Servers.
The RADIUS Servers page appears with a list of external RADIUS servers that are defined in Cisco ISE.

Step 2
Click Add to add an external RADIUS server.

Step 3
Enter the values as required.

Step 4
Click Submit to save the external RADIUS server configuration.

Define RADIUS Server Sequences
RADIUS server sequences in Cisco ISE allow you to proxy requests from a NAD to an external RADIUS server that will process the request and return the result to Cisco ISE, which forwards the response to the NAD.

RADIUS Server Sequences page lists all the RADIUS server sequences that you have defined in Cisco ISE. You can create, edit, or duplicate RADIUS server sequences from this page.

Before You Begin

- Before you begin this procedure, you should have a basic understanding of the Proxy Service and must have successfully completed the task in the first entry of the Related Links.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1
Choose Administration > Network Resources > RADIUS Server Sequences.

Step 2
Click Add.

Step 3
Enter the values as required.

Step 4
Click Submit to save the RADIUS server sequence to be used in policies.

Cisco ISE Acting as a TACACS+ Proxy Client
Cisco ISE can act as proxy client to external TACACS+ servers. When it acts as a proxy client, Cisco ISE receives authentication, authorization, and accounting requests from the Network Access Server (NAS) and forwards them to the external TACACS+ server. Cisco ISE accepts the results of the requests and returns them to the NAS.
The TACACS+ External Servers page lists all the external TACACS+ servers that you have defined in Cisco ISE. You can use the filter option to search for specific TACACS+ servers based on the name or description, or both.

Cisco ISE can simultaneously act as a proxy client to multiple external TACACS+ servers. In order to configure multiple external servers, you can use the TACACS+ server sequence page. Refer to the TACACS+ Server Sequence Settings page for more information.

**TACACS+ External Server Settings**

The following table describes the fields in the TACACS External Servers page. The navigation path is Work Centers > Device Administration > Network Resources > TACACS External Servers page.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the TACACS+ external server.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the TACACS+ external server setting.</td>
</tr>
<tr>
<td>Host IP</td>
<td>Enter the IP address (IPv4 or IPv6 address) of the remote TACACS+ external server.</td>
</tr>
<tr>
<td>Connection Port</td>
<td>Enter the port number of the remote TACACS+ external server. The port number is 49.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Specify the number of seconds that ISE should wait for a response from the external TACACS+ server. The default is 5 seconds. Valid values are from 1 to 120.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>A string of text that is used to secure a connection with the TACACS+ External Server. The connection will be rejected by the TACACS+ External server if this is not configured correctly.</td>
</tr>
<tr>
<td>Use Single Connect</td>
<td>The TACACS protocol supports two modes for associating sessions to connections: Single Connect and Non-Single Connect. Single connect mode reuses a single TCP connection for many TACACS+ sessions that a client may initiate. Non-Single Connect opens a new TCP connection for every TACACS+ session that a client initiates. The TCP connection is closed after each session. You can check the Use Single Connect check box for high-traffic environment and uncheck it for low-traffic environment.</td>
</tr>
</tbody>
</table>

**Configure External TACACS+ Servers**

You must configure the external TACACS servers in the Cisco ISE to enable it to forward requests to the external TACACS servers. You can define the timeout period and the number of connection attempts.
Before You Begin

- You cannot use the external TACACS servers that you create in this section directly in the policy. You must create a TACACS server sequence and configure it to use the TACACS server that you create in this section. You can then use the TACACS server sequence in the policy sets.
- To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose **Work Centers > Device Administration > Network Resources > TACACS External Servers.**
The **TACACS External Servers** page appears with a list of external TACACS servers that are defined in Cisco ISE.

Step 2 Click **Add** to add an external TACACS server.

Step 3 Enter the values as required.

Step 4 Click **Submit** to save the external TACACS server configuration.

**TACACS+ Server Sequence Settings**

The following table describes the fields in the TACACS Server Sequence page. The navigation path is **Work Centers > Device Administration > Network Resources > TACACS Server Sequence** page.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the TACACS proxy server sequence.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the TACACS proxy server sequence.</td>
</tr>
<tr>
<td>Server List</td>
<td>Select the required TACACS proxy servers from the Available list. The available list contains the list of TACACS proxy servers configured in the TACACS External Services Page.</td>
</tr>
<tr>
<td>Logging Control</td>
<td>Check to enable logging control:</td>
</tr>
<tr>
<td></td>
<td>• Local Accounting: Accounting messages are logged by the server that handles requests from devices.</td>
</tr>
<tr>
<td></td>
<td>• Remote Accounting: Accounting messages are logged by the proxy server that handles requests from devices.</td>
</tr>
</tbody>
</table>
### Username Stripping

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username Stripping</td>
<td>Username Prefix/Suffix Stripping:</td>
</tr>
<tr>
<td></td>
<td>• Prefix Strip: Check to strip the username from the prefix. For example, if the subject name is acme\smith and the separator is , the username becomes smith. The default separator is .</td>
</tr>
<tr>
<td></td>
<td>• Suffix Strip: Check to strip the username from the suffix. For example, if the subject name is <a href="mailto:smith@acme.com">smith@acme.com</a> and the separator is @, the username becomes smith. The default separator is @.</td>
</tr>
</tbody>
</table>

#### Define TACACS+ Server Sequences

TACACS+ server sequences in Cisco ISE allow you to proxy requests from a NAD to an external TACACS+ server that will process the request and return the result to Cisco ISE, which forwards the response to the NAD. The TACACS+ Server Sequences page lists all the TACACS+ server sequences that you have defined in Cisco ISE. You can create, edit, or duplicate TACACS+ server sequences from this page.

**Before You Begin**

- You should have a basic understanding of the Proxy Service, Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions.
- To perform the following task, you must be a Super Admin or System Admin.
- Ensure that the external TACACS+ servers that you intend to use in the TACACS+ server sequence are already defined.

**Step 1** Choose **Work Centers > Device Administration > Network Resources > TACACS External Server Sequence**.

**Step 2** Click **Add**.

**Step 3** Enter the required values.

**Step 4** Click **Submit** to save the TACACS+ server sequence to be used in policies.

#### Network Access Service

A network access service contains the authentication policy conditions for requests. You can create separate network access services for different use cases, for example, Wired 802.1X, Wired MAB, and so on. To create a network access service, configure allowed protocols or server sequences. The network access service for network access policies is then configured from the Policy Sets page.
Define Allowed Protocols for Network Access

Allowed protocols define the set of protocols that Cisco ISE can use to communicate with the device that requests access to the network resources. An allowed protocols access service is an independent entity that you should create before you configure authentication policies. Allowed protocols access service is an object that contains your chosen protocols for a particular use case.

The Allowed Protocols Services page lists all the allowed protocols services that you create. There is a default network access service that is predefined in the Cisco ISE.

Before You Begin

Before you begin this procedure, you should have a basic understanding of the protocol services that are used for authentication.

- Review the Cisco ISE Authentication Policies section in this chapter to understand authentication type and the protocols that are supported by various databases.
- Review the PAC Options to understand the functions and options for each protocol service, so you can make the selections that are appropriate for your network.
- Ensure that you have defined the global protocol settings.

To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1** Choose **Policy > Policy Elements > Results > Authentication > Allowed Protocols**.
If Cisco ISE is set to operate in FIPS mode, some protocols are disabled by default and cannot be configured.

**Step 2** Click **Add**.

**Step 3** Enter the required information.

**Step 4** Select the appropriate authentication protocols and options for your network.

**Step 5** If you choose to use PACs, make the appropriate selections.
To enable Anonymous PAC Provisioning, you must choose both the inner methods, EAP-MSCHAPv2 and Extensible Authentication Protocol-General Token Card (EAP-GTC). Also, be aware that Cisco ISE only supports Active Directory as an external identity source for machine authentication.

**Step 6** Click **Submit** to save the allowed protocols service.

The allowed protocols service appears as an independent object in the simple and rule-based authentication policy pages. You can use this object in different rules.

You can now create a simple or rule-based authentication policy.

If you disable EAP-MSCHAP as inner method and enable EAP-GTC and EAP-TLS inner methods for PEAP or EAP-FAST, ISE starts EAP-GTC inner method during inner method negotiation. Before the first EAP-GTC message is sent to the client, ISE executes identity selection policy to obtain GTC password from the identity store. During the execution of this policy, EAP authentication is equal to EAP-GTC. If EAP-GTC inner method is rejected by the client and EAP-TLS is negotiated, identity store policy is not executed again. In case identity store policy is based on EAP authentication attribute, it might have unexpected results since the real EAP authentication is EAP-TLS but was set after identity policy evaluation.
Enable MAB from Non-Cisco Devices

Configure the following settings sequentially to configure MAB from non-Cisco devices.

**Step 1**
Ensure that the MAC address of the endpoints that are to be authenticated are available in the Endpoints database. You can add these endpoints or have them profiled automatically by the Profiler service.

**Step 2**
Create a Network Device Profile based on the type of MAC authentication used by the non-Cisco device (PAP, CHAP, or EAP-MD5).

a) Choose Administration > Network Resources > Network Device Profiles.
b) Click Add.
c) Enter a name and description for the network device profile.
d) Select the vendor name from the Vendor drop-down list.
e) Check the check boxes for the protocols that the device supports. If the device supports RADIUS, select the RADIUS dictionary to use with the network device.
f) Expand the Authentication/Authorization section to configure the device's default settings for flow types, attribute aliasing, and host lookup.
g) In the Host Lookup (MAB) section, do the following:
   - Process Host Lookup—Check this check box to define the protocols for host lookup used by the network device profile.
     Network devices from different vendors perform MAB authentication differently. Depending on the device type, check the Check Password check box and/or Check Calling-Station-Id equals MAC Address check box, for the protocol you are using.
   - Via PAP/ASCII—Check this check box to configure Cisco ISE to detect a PAP request from the network device profile as a Host Lookup request.
   - Via CHAP—Check this check box to configure Cisco ISE to detect this type of request from the network devices as a Host Lookup request.
   - Via EAP-MD5—Check this check box to enable EAP-based MD5 hashed authentication for the network device profile.

h) Enter the required details in the Permissions, Change of Authorization (CoA), and Redirect sections, and then click Submit.
For information on how to create custom NAD profiles, see Network Access Device Profiles with Cisco Identity Services Engine.

**Step 3**
Choose Administration > Network Resources > Network Devices.

**Step 4**
Select the device for which you want to enable MAB, and then click Edit.

**Step 5**
In the Network Device page, select the network device profile that you created in step 2 from the Device Profile drop-down list.

**Step 6**
Click Save.
For Cisco NADs, the Service-Type values used for MAB and web/user authentication are different. This allows ISE to differentiate MAB from web authentication when Cisco NADs are used. Some non-Cisco NADs use the same value for the Service-Type attribute for both MAB and web/user authentication; this may lead to security issues in your access policies. If you are using MAB with non-Cisco devices, we recommend that you configure additional authorization policy rules to ensure that your network security is not compromised. For example, if a printer is using MAB, you could configure an authorization policy rule to restrict it to printer protocol ports in the ACL.

**Enable MAB from Cisco Devices**

Configure the following settings sequentially to configure MAB from Cisco devices.

**Step 1**
Ensure that the MAC address of the endpoints that are to be authenticated are available in the Endpoints database. You can add these endpoints or have them profiled automatically by the Profiler service.

**Step 2**
Create a Network Device Profile based on the type of MAC authentication used by the Cisco device (PAP, CHAP, or EAP-MD5).

a) Choose Administration > Network Resources > Network Device Profiles.
b) Click Add.
c) Enter a name and description for the network device profile.
d) Check the check boxes for the protocols that the device supports. If the device supports RADIUS, select the RADIUS dictionary to use with the network device.
e) Expand the Authentication/Authorization section to configure the device's default settings for flow types, attribute aliasing, and host lookup.
f) In the Host Lookup (MAB) section, do the following:

  • Process Host Lookup—Check this check box to define the protocols for host lookup used by the network device profile.
  
  Depending on the device type, check the Check Password check box and/or Check Calling-Station-Id equals MAC Address check box, for the protocol you are using.

  • Via PAP/ASCII—Check this check box to configure Cisco ISE to detect a PAP request from the network device profile as a Host Lookup request.

  • Via CHAP—Check this check box to configure Cisco ISE to detect this type of request from the network devices as a Host Lookup request.

  • Via EAP-MD5—Check this check box to enable EAP-based MD5 hashed authentication for the network device profile.

g) Enter the required details in the Permissions, Change of Authorization (CoA), and Redirect sections, and then click Submit.

For information on how to create custom NAD profiles, see Network Access Device Profiles with Cisco Identity Services Engine.
Step 3 Choose Administration > Network Resources > Network Devices.
Step 4 Select the device for which you want to enable MAB, and then click Edit.
Step 5 In the Network Device page, select the network device profile that you created in step 2 from the Device Profile drop-down list.
Step 6 Click Save.

ISE Community Resource
For information about IP phone authentication capabilities, see Phone Authentication Capabilities.