



## 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 Cisco 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 different vendors. Cisco ISE allows you to create conditions as individual reusable policy elements.

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.



---

**Note** From the **Work Centers > Device Administration**, 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.

---

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



**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. Choose **Work Centers > Network Access > Policy Sets**.

#### ISE Community Resource

For information about using RADIUS results from a WLC, see [WLC Called-Station-ID \(Radius Authentication and Accounting Config\)](#).


- [Policy Set Configuration Settings](#), on page 2
- [Authentication Policies](#), on page 3
- [Authorization Policies](#), on page 11
- [Policy Conditions](#), on page 23
- [Special Network Access Conditions](#), on page 41
- [Policy Set Protocol Settings](#), on page 45
- [Enable MAB from Non-Cisco Devices](#), on page 82
- [Enable MAB from Cisco Devices](#), on page 84

## Policy Set Configuration Settings

The following table describes the fields in the **Policy Sets** window, from which you can configure policy sets, including authentication, exception and authorization policies. Choose **Work Centers > Network Access > Policy Sets** for network access policies. Choose **Work Centers > Device Administration > Device Admin Policy Sets** for device administration policies.

*Table 1: Policy Set Configuration Settings*

Field Name	Usage Guidelines
<b>Status</b>	Choose the status of this policy. It can be one of the following: <ul style="list-style-type: none"> <li>• <b>Enabled</b>: This policy condition is active.</li> <li>• <b>Disabled</b>: This policy condition is inactive and will not be evaluated.</li> <li>• <b>Monitor Only</b>: This policy condition will not be evaluated.</li> </ul>
<b>Policy Set Name</b>	Enter a unique name for this policy set.
<b>Conditions</b>	From a new policy row, click the plus (+) icon or from an existing policy row, click the Edit icon to open the Conditions Studio.
<b>Description</b>	Enter a unique description for the policy.

Field Name	Usage Guidelines
<b>Allowed Protocols or Server Sequence</b>	Choose an allowed protocol that you have already created, or click the (+) sign to <b>Create a New Allowed Protocol</b> , to <b>Create a New Radius Sequence</b> , or to <b>Create a TACACS Sequence</b> .
<b>Conditions</b>	From a new exceptions row, click the plus (+) icon or from an existing exception row, click the Edit icon to open the Conditions Studio.
<b>Hits</b>	Hits are a diagnostic tool indicating the number of times the conditions have matched. Hover over the icon to view when this was last updated, reset to zero and to view the frequency of updates.
<b>Actions</b>	Click the cog icon  from the Actions column to view and select different actions: <ul style="list-style-type: none"> <li>• Insert new row above: Insert a new policy above the policy from which you opened the Actions menu.</li> <li>• Insert new row below: Insert a new policy below the policy from which you opened the Actions menu.</li> <li>• Duplicate above: Insert a duplicate policy above the policy from which you opened the Actions menu, above the original set.</li> <li>• Duplicate below: Insert a duplicate policy below the policy from which you opened the Actions menu, below the original set.</li> <li>• Delete: Delete the policy set.</li> </ul>
<b>View</b>	Click the arrow icon to open the Set view of the specific policy set and view its authentication, exception, and authorization sub-policies.

## 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.

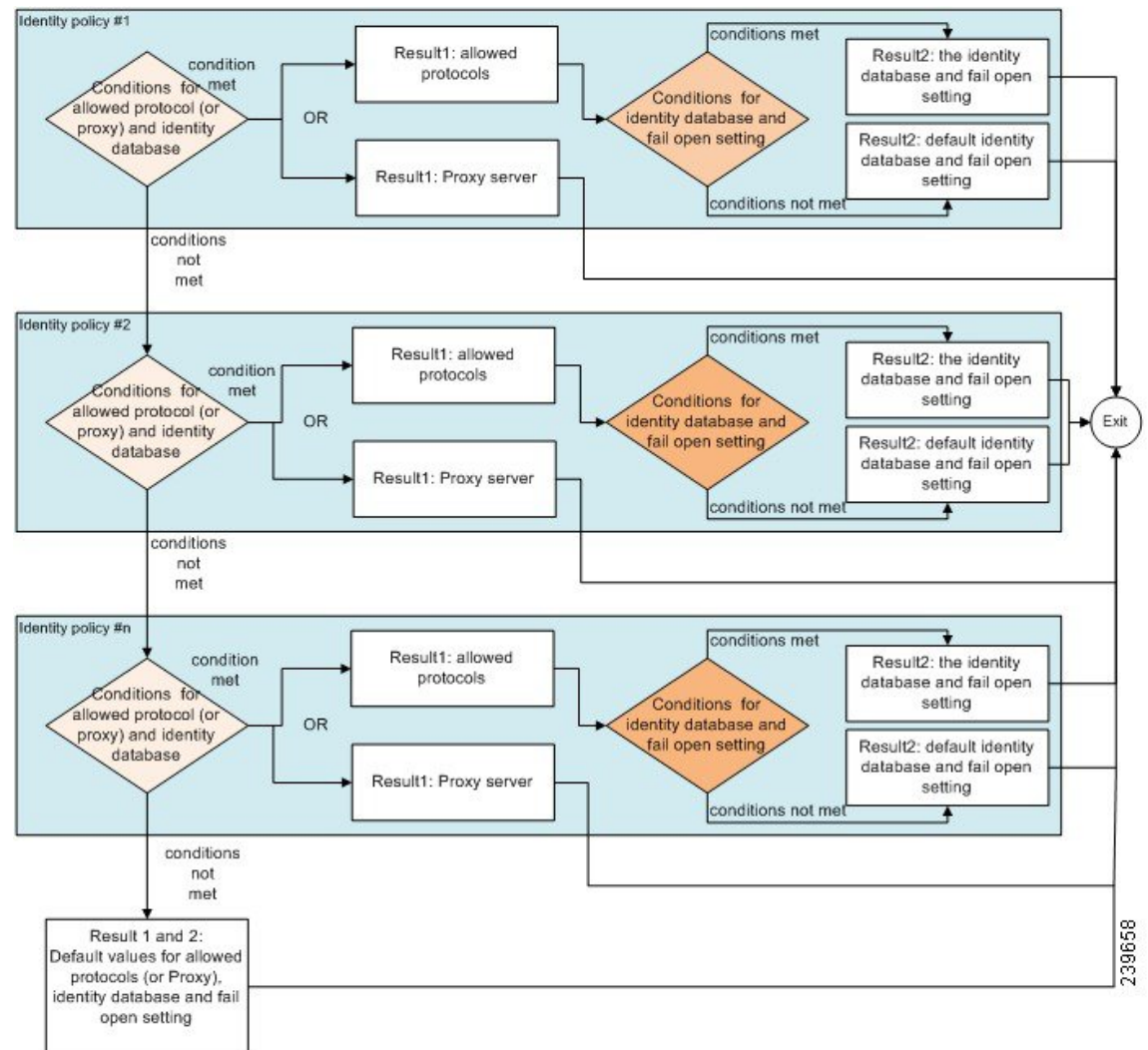
### **Authentication Policy Flow**

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 1: 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.
- Process failed—Unable to access the identity database or databases. The default course of action is drop.

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 the Internal and External Identity Sources section in *Cisco ISE Admin Guide: Asset Visibility*.

- 
- 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, on page 7](#).
- 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 [Special Network Access Conditions](#), on page 41.

Not all attributes you select will include the “Equals”, “Not Equals”, “In”, “Not In”, “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. In case of lists, the “in” operator checks whether a particular value exists in a list. In case of a single string the “in” operator checks whether the strings are same like the “equals” operator.

**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

## Authentication Policy Configuration Settings

The following table describes the fields in the **Authentication Policy** section of the **Policy Sets** window, from which you can configure authentication subpolicies as part of your policy sets. For network access policies, choose **Work Centers > Network Access > Policy Sets**. For device administration policies, choose **Work Centers > Device Administration > Device Admin Policy Sets**. From the Policy Sets page, choose **View > Authentication Policy**

*Table 2: Authentication Policy Configuration Settings*

Field Name	Usage Guidelines
Status	<p>Choose the status of this policy. It can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> This policy condition is active.</li> <li>• <b>Disabled:</b> This policy condition is inactive and will not be evaluated.</li> <li>• <b>Monitor Only:</b> This policy condition will be evaluated, but the result will not be enforced. You can view the results of this policy condition in the Live Log authentication page. In this, see the detailed report which will have the monitored step and attribute. For example, you may want to add a new policy condition, but are not sure if the condition would provide you with the correct results. In this situation, you can create the policy condition in monitored mode to view the results and then enable it if you are satisfied with the results.</li> </ul>

Field Name	Usage Guidelines
Rule Name	Enter a name for this authentication policy.
Conditions	From a new policy row, click the plus (+) icon or from an existing policy row, click the Edit icon to open the <b>Conditions Studio</b> .
Use	Choose the identity source that you want to use for authentication. You can also choose an identity source sequence if you have configured it.  You can edit the default identity source that you want Cisco ISE to use in case none of the identity sources defined in this rule match the request.
Options	Define a further course of action for authentication failure, user not found, or process failure events. You can choose one of the following options: <ul style="list-style-type: none"> <li>• <b>Reject:</b> A reject response is sent.</li> <li>• <b>Drop:</b> No response is sent.</li> <li>• <b>Continue:</b> Cisco ISE proceeds with the authorization policy.</li> </ul>
Hits	Hits are a diagnostic tool indicating the number of times the conditions have matched.
Actions	Click the cog icon  from the Actions column to view and select different actions: <ul style="list-style-type: none"> <li>• Insert new row above: Insert a new authentication policy above the policy from which you opened the Actions menu.</li> <li>• Insert new row below: Insert a new authentication policy below the policy from which you opened the Actions menu.</li> <li>• Duplicate above: Insert a duplicate authentication policy above the policy from which you opened the Actions menu, above the original set.</li> <li>• Duplicate below: Insert a duplicate authentication policy below the policy from which you opened the Actions menu, below the original set.</li> <li>• Delete: Delete the policy set.</li> </ul>



## Password-Based Authentication

Authentication verifies user information to confirm user identity. Traditional authentication uses a name and a fixed password. This is the most popular, simplest, and least-expensive method of authentication. The disadvantage is that this information can be told to someone else, guessed, or captured. An approach that uses simple, unencrypted usernames and passwords is not considered a strong authentication mechanism, but it can be sufficient for low-authorization or low-privilege levels such as Internet access.

## Secure Authentication Using Encrypted Passwords and Cryptographic Techniques

You should use encryption to reduce the risk of password capture on the network. Client and server access control protocols, such as RADIUS, encrypt passwords to prevent them from being captured within a network. However, RADIUS operates only between the authentication, authorization, and accounting (AAA) client and Cisco ISE. Before this point in the authentication process, unauthorized persons can obtain cleartext passwords such as in the following examples:

- In the communication between an end-user client that dials up over a phone line.
- On an ISDN line that terminates at a network access server.
- Over a Telnet session between an end-user client and the hosting device

More-secure methods use cryptographic techniques, such as those used inside the Challenge Authentication Handshake Protocol (CHAP), one-time password (OTP), and advanced EAP-based protocols. Cisco ISE supports a variety of these authentication methods.

## Authentication Methods and Authorization Privileges

A fundamental implicit relationship exists between authentication and authorization. The more authorization privileges that are granted to a user, the stronger the authentication should be. Cisco ISE supports this relationship by providing various methods of authentication.

## 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 the TACACS Live Logs section in *Cisco ISE Admin Guide: Troubleshooting* . For additional information about RADIUS Live Logs settings, see the RADIUS Live Logs section in *Cisco ISE Admin Guide: Troubleshooting* .

[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



**Note** You must enable IPv6 snooping on Cisco Catalyst 4000 Series switches, otherwise IPv6 address will not be mapped to the authentication sessions and will not be displayed in the show output. Use the following commands to enable IPv6 snooping:

```
vlan config <vlan-number>
  ipv6 snooping
  end
ipv6 nd rguard policy router
  device-role router
interface <access-interface>
  ipv6 nd rguard
interface <uplink-interface>
  ipv6 nd rguard attach-policy router
  end
```

## 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 **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 define the location hierarchy (campus/building/floor structure) and configure the secure and non-secure zones using the Cisco Prime Infrastructure application. After defining the location hierarchy, you must synchronize the location hierarchy data with the MSE servers. For more information on Cisco Prime Infrastructure, see: <http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html>.

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.

## Add an 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

Access control lists (ACLs) are lists of access control entries (ACEs), which may be applied by a Policy Enforcement Point (for example, a switch) to a resource. Each ACE identifies the permissions allowed per user for that object, such as read, write, execute and more. For example, an ACL may be configured for use the Sales area of the network, with an ACE allowing Write permissions for the Sales group and a separate

ACE allowing Read permissions for all other employees of the organization. With RADIUS protocol, ACLs grant authorization by filtering source and destination IP addresses, transport protocols, and additional parameters. Static ACLs reside on and are directly configured from the switch and can be applied in your authorization policies from the ISE GUI; downloadable ACLs (DACLS) can be configured, managed and applied in your authorization policies from the ISE GUI. DACLS can also be configured using the custom user attributes and AD attributes.

To implement DACLS in your network authorization policy in ISE:

1. Configure a new or existing DACL from **Policy > Policy Elements > Results > Downloadable ACLs**. For more information see [Configure Permissions for Downloadable ACLs, on page 14](#).
2. Configure a new or existing authorization profile from **Policy > Policy Elements > Results > Authorization Profiles**, using any of the DACLS you already configured.
3. Implement the authorization profiles you have configured when creating and configuring new and existing policy sets from **Policy > Policy Sets**.

### Configure Permissions for Downloadable ACLs

With Cisco ISE, downloadable ACLs (DACLS) can be configured and implemented in your authorization policies for control of how the network is accessed by different users and groups of users. Default authorization DACLS are available with installation of ISE, including the following default profiles:

- DENY\_ALL\_TRAFFIC
- PERMIT\_ALL\_TRAFFIC

When working with DACLS, these defaults cannot be changed, but you can duplicate them in order to create additional, similar, DACLS.

- 
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.
- Step 2** Click **Add** from the top of the **Downloadable ACLs** table or alternatively, choose any of the existing DACLS and click **Duplicate** from the top of the table.
- Step 3** Enter or edit the desired values for the DACL, keeping in mind the following rules:
- Supported characters for the name field are: alphanumeric, hyphen(-), dot( .) and underscore( \_)
  - The keyword **Any** must be the source in all ACEs in the 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.
- Note** The **IP Version** field is noneditable when DACL is mapped to any authorization profile. In this case, remove the DACL reference from **Authorization Profiles**, edit the IP version and remap the DACL in **Authorization Profiles**.
- Step 4** Optionally, when you finish creating the complete list of ACEs, click **Check DACL Syntax** to validate the list. If there are validation errors, the check returns specific instructions identifying the invalid syntax in the window that opens automatically.
- Step 5** 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.
  - Numeric characters: 0-9.
- Identity groups default to “Any” (you can use this global default to apply to all users).
- Conditions allow you to set one or more policy values. However, conditions are optional and are not required to create an authorization policy. These are the two methods for creating conditions:
  - Choose an existing condition or attribute from a corresponding dictionary of choices.
  - Create a custom condition that allows you to select a suggested value or use a text box to enter a custom value.
- Condition names you create must use only the following supported characters:
  - Symbols: hyphen (-), underscore (\_), and period (.).
  - Alphabetic characters: A-Z and a-z.
  - Numeric characters: 0-9.
- Permissions are important when choosing an authorization profile to use for a policy. A permission can grant access to specific resources or allow you to perform specific tasks. For example, if a user belongs

to a specific identity group (such as Device Admins), and the user meets the defined conditions (such as a site in Boston), then this user is granted the permissions associated with that group (such as access to a specific set of network resources or permission to perform a specific operation on a device).

- When you use the **radius** attribute **Tunnel-Private-Group-ID** in an authorization condition, you must mention both the tag and the value in the condition when the **EQUALS** operator is being used, for example:



```
Tunnel-Private-Group-ID EQUALS (tag=0) 77
```

## Configure Authorization Policies

After creating attributes and building blocks for authorization policies from the Policy menu, create authorization policies within policy sets from the Policy Sets menu.

### Before you begin

Before you begin this procedure, you should have a basic understanding of the different building blocks used to create authorization policies such as identify groups and conditions.

- 
- 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. A new row appears in the Authorization Policy table.
- Step 5** 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, on page 17](#).
- Step 6** 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 7** To add or change conditions, hover over the cell in the **Conditions** column and click . The Conditions Studio opens. For more information, see [#unique\\_1036](#).

Not all attributes you select will include the “Equals”, “Not Equals”, “In”, “Not In”, “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. In case of lists, the “in” operator checks whether a particular value exists in a list. In case of a single string the “in” operator checks whether the strings are same like the “equals” operator.



- Step 8** For network access results profiles, select the relevant authorization profile from the **Results Profiles** dropdown list or choose or click **+**, choose **Create a New Authorization Profile** and when the **Add New Standard Profile** screen opens, perform the following steps:
- Enter values as required to configure a new authorization profile. Keep the following in mind:
    - Supported characters for the name field are: space, ! # \$ % & ' ( ) \* + , - . / ; = ? @ \_ {.
    - You can double-check the authorization profile RADIUS syntax from the **Attributes Details** that dynamically appear at the bottom of the screen.
  - Click **Save** to save your changes to the Cisco ISE system database to create an authorization profile.
  - To create, manage, edit, and delete profiles outside of the Policy Sets area, choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.
- Step 9** For network access results security groups, select the relevant security group from the **Results Security Groups** dropdown list or click **+**, choose **Create a New Security Group** and when the Create New Security Group screen opens, perform the following steps:
- Enter a name and description (optional) for the new security group.
  - Check the **Propagate to ACI** check box if you want to propagate this SGT to Cisco ACI. The SXP mappings that are related to this SGT will be propagated to Cisco ACI only if they belong to a VPN that is selected in the Cisco ACI Settings page.

This option is disabled by default.
  - 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**).
  - 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.
- 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 Settings

The following table describes the fields in the **Authorization Policy** section of the **Policy Sets** window, from which you can configure authorization policies as part of your policy sets. For network access policies, choose **Work Centers > Network Access > Policy Sets**. For device administration policies, choose **Work Centers > Device Administration > Device Admin Policy Sets**. From the Policy Sets page, choose **View > Authorization Policy**.

Table 3: Authorization Policy Configuration Settings

Field Name	Usage Guidelines
<p><b>Status</b></p>	<p>Choose the status of this policy. It can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> This policy condition is active.</li> <li>• <b>Disabled:</b> This policy condition is inactive and will not be evaluated.</li> <li>• <b>Monitor Only:</b> This policy condition will be evaluated, but the result will not be enforced. You can view the results of this policy condition in the Live Log authentication page. In this, see the detailed report which will have the monitored step and attribute. For example, you may want to add a new policy condition, but are not sure if the condition would provide you with the correct results. In this situation, you can create the policy condition in monitored mode to view the results and then enable it if you are satisfied with the results.</li> </ul>
<p><b>Rule Name</b></p>	<p>Enter a unique name for this policy.</p>
<p><b>Conditions</b></p>	<p>From a new policy row, click the plus (+) icon or from an existing policy row, click the Edit icon to open the Conditions Studio.</p>
<p><b>Results or Profiles</b></p>	<p>Select the relevant authorization profile, which determines the different levels of permissions offered to the configured security group. If you have not yet configured the relevant authorization profile, you can do so inline.</p>
<p><b>Results or Security Groups</b></p>	<p>Select the relevant security group, which determines the groups of users relevant to the specific rule. If you have not yet configured the relevant security group, you can do so inline.</p>
<p><b>Results or Command Sets</b></p>	<p>Command sets enforce the specified list of commands that can be executed by a device administrator. When a device administrator issues operational commands on a network device, ISE is queried to determine whether the administrator is authorized to issue these commands. This is also referred to as command authorization.</p>
<p><b>Results or Shell Profiles</b></p>	<p>TACACS+ shell profiles control the initial login session of the device administrator.</p>

Field Name	Usage Guidelines
Hits	Hits are a diagnostic tool indicating the number of times the conditions have matched.
Actions	<p>Click the cog icon  from the Actions column to view and select different actions:</p> <ul style="list-style-type: none"> <li>• <b>Insert new row above:</b> Insert a new authorization rule above the rule from which you opened the Actions menu.</li> <li>• <b>Insert new row below:</b> Insert a new authorization rule below the rule from which you opened the Actions menu.</li> <li>• <b>Duplicate above:</b> Insert a duplicate authorization rule above the rule from which you opened the Actions menu, above the original set.</li> <li>• <b>Duplicate below:</b> Insert a duplicate authorization rule below the rule from which you opened the Actions menu, below the original set.</li> <li>• <b>Delete:</b> Delete the rule.</li> </ul>

## Authorization Profile Settings

The following fields in the **Authorization Profiles** window define attributes for network access. The navigation path for this window is **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

### Authorization Profile Settings

- **Name:** Enter a name for this new authorization profile.
- **Description:** Enter a description for this authorization profile.
- **Access Type:** Choose the access type: **ACCESS\_ACCEPT** or **ACCESS\_REJECT**.
- **Service Template:** Enable this option to support sessions with SAnet-capable devices. Cisco ISE implements service templates in authorization profiles using a special flag that marks them as *Service Template* compatible. Since the service template is also an authorization profile, it acts as a single policy that supports both SAnet and non-SAnet devices.
- **Track Movement:** Enable this option to track user location with Cisco Mobility Services Engine (MSE).




---

**Note** This option may impact Cisco ISE performance, it is only intended for high-security locations.

---

- **Passive Identity Tracking:** Enable this option to use the Easy Connect feature of Passive Identity for policy enforcement and user tracking.

## Common Tasks

Common tasks are specific permissions and actions that apply to network access.

- **DACL Name** : Enable this option to use a downloadable ACL. You can use the default values (**PERMIT\_ALL\_TRAFFIC** or **DENY\_ALL\_TRAFFIC**), or select an attribute from the following dictionaries:
  - External identity store (attributes)
  - Endpoints
  - Internal User
  - Internal Endpoint

For more information about adding DACLs or editing and managing existing DACLs, see [Downloadable ACLs, on page 13](#).

- **Security Group**: Enable this option to assign a security group (SGT) part of authorization.
  - If Cisco ISE is not integrated with Cisco DNA Center, Cisco ISE assigns VLAN ID 1.
  - If Cisco ISE is integrated with Cisco DNA Center, then select the Virtual Network (VN) that Cisco DNA Center shared with Cisco ISE, select the **Data Type**, and the subnet/address pool.

A Security Group task includes a security group and an optional VN. If you configure a security group, then you cannot configure a VLAN separately. An endpoint device can only be assigned to one virtual network.

- **VLAN**: Enable this option to specify a virtual LAN (VLAN) ID. You can enter integer or string values for the VLAN ID. The format for this entry is `Tunnel-Private-Group-ID:VLANnumber`.
- **Voice Domain Permission** : Enable this option to use a downloadable ACL. The vendor-specific attribute (VSA) of `cisco-av-pair` is associated with the value `device-traffic-class=voice`. In multidomain authorization mode, if the network switch receives this VSA, the endpoint connects to a voice domain after authorization.
- **Web Redirection (CWA, DRW, MDM, NSP, CPP)**: Enable this option to enable web redirection after authentication.
  - Select the type of redirection. The type of Web Redirection that you select displays additional options, which are described below.
  - Enter an ACL to support the redirection that Cisco ISE sends to the NAD.
 

The ACL you enter to send to the NAD displays in the **Attributes Details** pane as a `cisco-av` pair. For example, if you enter **acl119**, it is displayed in the **Attributes Details** pane as: `cisco-av-pair = url-redirect-acl = acl119`.
  - Select the other settings for the selected web redirection type.

Select one of the following types web redirection:

- **Centralized Web Auth**: Redirect to the portal you select from the **Value** drop-down.
- **Client Provisioning (Posture)**: Redirect to the client provisioning portal you select from the **Value** drop-down, to enable posture on the client.

- **Hot Spot: Redirect:** Redirect to the hot spot portal you select from the **Value** drop-down.
- **MDM Redirect:** Redirect to the MDM portal on the MDM server that you specify.
- **Native Supplicant Provisioning:** Redirect to the BYOD portal you select from the **Value** drop-down.

After selecting the web redirection type, and entering the required parameters, configure the following options:

- **Display Certificates Renewal Message:** Enable this option to display a certificate renewal message. The URL-redirect attribute value changes and includes the number of days for which the certificate is valid. This option is only for Centralized Web Auth redirection.
- **Static IP/Host Name/FQDN:** Enable this option to redirect a user to a different PSN. Enter the target IP address, hostname, or FQDN. If you do not configure this option, the user is redirected to the FQDN of the policy service node that received this request.
- **Suppress Profiler CoA for endpoints in Logical Profile:** Enable this option to cancel the redirect for a certain type of endpoint device.
- **Auto SmartPort:** Enable this option to use Auto SmartPort functionality. Enter an event name, which creates a VSA `cisco-av-pair` with that value as `auto-smart-port=event_name`. This value is displayed in the **Attributes Details** pane.
- **Access Vulnerabilities:** Enable this option to run the Threat Centric NAC Vulnerability Assessment on this endpoint as part of authorization. Select the adapter, and when to run the scan.
- **Reauthentication:** Enable this option to keep the endpoint connected during reauthentication. You choose to maintain connectivity during reauthentication by choosing to use **RADIUS-Request (1)**. The default RADIUS-Request (0) disconnects the existing session. You can also set an inactivity timer.
- **MACSec Policy:** Enable this option to use the MACSec encryption policy whenever a MACSec enabled client connects to Cisco ISE. Choose one of the following options: **must-secure**, **should-secure**, or **must-not-secure**. Your settings are displayed in the **Attributes Details** pane as: `cisco-av-pair = linksec-policy=must-secure`.
- **NEAT :** Enable this option to use Network Edge Access Topology (NEAT), which extends identity recognition between networks. Checking this check box displays `cisco-av-pair = device-traffic-class=switch` in the **Attributes Details** pane.
- **Web Authentication (Local Web Auth) :** Enable this option to use local web authentication for this authorization profile. This value lets the switch recognize authorization for web authentication by Cisco ISE sending a VSA along with a DACL. The VSA is `cisco-av-pair = priv-lvl=15`, which is displayed in the **Attributes Details** pane.
- **Airespace ACL Name:** Enable this option to send an ACL name to Cisco Airespace wireless controller. The Airespace VSA uses this ACL to authorize a locally defined ACL to a connection on the WLC. For example, if you entered **rsa-1188**, it is displayed as `Airespace-ACL-Name = rsa-1188` in the **Attributes Details** pane.
- **ASA VPN:** Enable this option to assign an Adaptive Security Appliances (ASA) VPN group policy. From the drop-down list, choose a VPN group policy.
- **AVC Profile Name:** Enable this option to run application visibility on this endpoint. Enter the AVC profile to use.

### Advanced Attributes Settings

- **Dictionaries:** Click the down arrow icon to view the available options in the **Dictionaries** window. Select a dictionary and an attribute that should be configured in the first field.
- **Attribute Values:** Click the down-arrow icon to display the available options in the **Attribute Values** window. Select the desired attribute group and the attribute value. This value is matched with the one selected in the first field. The **Advanced Attributes** settings that you configure are displayed in the **Attribute Details** panel.
- **Attributes Details:** This pane displays the configured attribute values that you have set for **Common Tasks** and **Advanced Attributes**.

The values that are displayed in the **Attributes Details** pane are read-only.




---

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

---

### Related Topics

- [Cisco ISE Authorization Profiles](#), on page 11
- [Permissions for Authorization Profiles](#), on page 12
- [Configure an Authorization Profile for Redirecting Nonregistered Devices](#)
- [Create Authorization Profiles](#)

## 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. For information about authorization policies, see [Configure Authorization Policies, on page 16](#).




---

**Note** Cisco ISE does not support the use of % character in the authorization policies to avoid security issues.

---

## Local and Global Exceptions Configuration Settings

For network access policies, choose **Work Centers > Network Access > Policy Sets**. For device administration policies, choose **Work Centers > Device Administration > Device Admin Policy Sets**. From the **Policy Sets** window, choose **View > Local Exceptions Policy** or **Global Exceptions Policy**.

Authorization exception settings are identical to the Authorization policy settings and are as described in [Authorization Policy Settings, on page 17](#).

## 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.

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 41.

## Dictionaries and Dictionary Attributes

Dictionaries are domain-specific catalogs of attributes and allowed values that can be used to define access policies for a domain. An individual dictionary is a homogeneous collection of attribute type. Attributes that are defined in a dictionary have the same attribute type and the type indicates the source or context of a given attribute.

Attribute types can be one of the following:

- MSG\_ATTR
- ENTITY\_ATTR
- PIP\_ATTR

In addition to attributes and allowed values, a dictionary contains information about the attributes such as the name and description, data type, and the default values. An attribute can have one of the following data types: BOOLEAN, FLOAT, INTEGER, IPv4, IPv6, OCTET\_STRING, STRING, UNIT32, and UNIT64.

Cisco ISE creates system dictionaries during installation and allows you to create user dictionaries.

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:

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



---

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

---

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

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

### 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
  - Cisco-BBSM
  - Cisco-VPN3000
  - Microsoft
  - Network access

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.

Dictionary	Attributes	Allowed Protocol Rules and Proxy	Identity Rules
Device	Device Type (predefined network device group)	Yes	Yes
	Device Location (predefined network device group)		
	Other Custom Network Device Group		
	Software Version		
	Model Name		
RADIUS	All attributes	Yes	Yes
Network Access	ISE Host Name	Yes	Yes
	AuthenticationMethod	No	Yes
	AuthenticationStatus	No	No
	CTSDeviceID	No	No
	Device IP Address	Yes	Yes
	EapAuthentication (the EAP method that is used during authentication of a user of a machine)	No	Yes
	EapTunnel (the EAP method that is used for tunnel establishment)	No	Yes
	Protocol	Yes	Yes
	UseCase	Yes	Yes
	UserName	No	Yes
	WasMachineAuthenticated	No	No

Dictionary	Attributes	Allowed Protocol Rules and Proxy	Identity Rules
Certificate	Common Name	No	Yes
	Country		
	E-mail		
	LocationSubject		
	Organization		
	Organization Unit		
	Serial Number		
	State or Province		
	Subject		
	Subject Alternative Name		
	Subject Alternative Name - DNS		
	Subject Alternative Name - E-mail		
	Subject Alternative Name - Other Name		
	Subject Serial Number		
	Issuer		
	Issuer - Common Name		
	Issuer - Organization		
	Issuer - Organization Unit		
	Issuer - Location		
	Issuer - Country		
	Issuer - Email		
	Issuer - Serial Number		
	Issuer - State or Province		
Issuer - Street Address			
Issuer - Domain Component			
Issuer - User ID			

## System Defined Dictionaries and Dictionary Attributes

Cisco ISE creates system dictionaries during installation that you can find in the System Dictionaries page. System-defined dictionary attributes are read-only attributes. Because of their nature, you can only view existing system-defined dictionaries. You cannot create, edit, or delete system-defined values or any attributes in a system dictionary.

A system-defined dictionary attribute is displayed with the descriptive name of the attribute, an internal name as understood by the domain, and allowed values.

Cisco ISE also creates dictionary defaults for the IETF RADIUS set of attributes that are also a part of the system-defined dictionaries, which are defined by the Internet Engineering Task Force (IETF). You can edit all free IETF RADIUS attribute fields except the ID.

## Display System Dictionaries and Dictionary Attributes

You cannot create, edit, or delete any system-defined attribute in a system dictionary. You can only view system-defined attributes. You can perform a quick search that is based on a dictionary name and description or an advanced search that is based on a search rule that you define.

- 
- Step 1** Choose **Policy > Policy Elements > Dictionaries > System**.
  - Step 2** Choose a system dictionary in the System Dictionaries page, and click **View**.
  - Step 3** Click **Dictionary Attributes**.
  - Step 4** Choose a system dictionary attribute from the list, and click **View**.
  - Step 5** Click the **Dictionaries** link to return to the System Dictionaries page.
- 

## User-Defined Dictionaries and Dictionary Attributes

Cisco ISE displays the user-defined dictionaries that you create in the User Dictionaries page. You cannot modify the values for Dictionary Name or Dictionary Type for an existing user dictionary once created and saved in the system.

You can do the following in the User Dictionaries page:

- Edit and delete user dictionaries.
- Search user dictionaries based on name and description.
- Add, edit, and delete user-defined dictionary attributes in the user dictionaries.
- Delete attributes of the NMAP extension dictionary, using the NMAP scan action. When custom ports are added or deleted in the NMAP Scan Actions page, the corresponding custom ports attributes are added, deleted, or updated in the dictionary.
- Add or remove allowed values for dictionary attributes.

## Create User-Defined Dictionaries

You can create, edit, or delete user-defined dictionaries.

- 
- Step 1** Choose **Policy > Policy Elements > Dictionaries > User**.
- Step 2** Click **Add**.
- Step 3** Enter the name for the user dictionary, an optional description, and a version for the user dictionary.
- Step 4** Choose the attribute type from the Dictionary Attribute Type drop-down list.
- Step 5** Click **Submit**.
- 

## Create User-Defined Dictionary Attributes

You can add, edit, and delete user-defined dictionary attributes in user dictionaries as well as add or remove allowed values for the dictionary attributes.

- 
- Step 1** Choose **Policy > Policy Elements > Dictionaries > User**.
- Step 2** Choose a user dictionary from the User Dictionaries page, and click **Edit**.
- Step 3** Click **Dictionary Attributes**.
- Step 4** Click **Add**.
- Step 5** Enter the name for an attribute name, an optional description, and an internal name for the dictionary attribute.
- Step 6** Choose a data type from the Data Type drop-down list.
- Step 7** Click **Add** to configure the name, allowed value, and set the default status in the Allowed Values table.
- Step 8** Click **Submit**.
- 

## RADIUS-Vendor Dictionaries

Cisco ISE allows you to define a set of RADIUS-vendor dictionaries, and define a set of attributes for each one. Each vendor definition in the list contains the vendor name, the vendor ID, and a brief description.

Cisco ISE provides you the following RADIUS-vendor dictionaries by default:

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

The RADIUS protocol supports these vendor dictionaries, and the vendor-specific attributes that can be used in authorization profiles and in policy conditions.

## Create RADIUS-Vendor Dictionaries

You can also create, edit, delete, export, and import RADIUS-vendor dictionaries.

- 
- Step 1** Choose **Policy > Policy Elements > Dictionaries > System > Radius > Radius Vendors**.
  - Step 2** Click **Add**.
  - Step 3** Enter a name for the RADIUS-vendor dictionary, an optional description, and the vendor ID as approved by the Internet Assigned Numbers Authority (IANA) for the RADIUS vendor.
  - Step 4** Choose the number of bytes taken from the attribute value to specify the attribute type from the Vendor Attribute Type Field Length drop-down list. Valid values are 1, 2, and 4. The default value is 1.
  - Step 5** Choose the number of bytes taken from the attribute value to specify the attribute length from the Vendor Attribute Size Field Length drop-down list. Valid values are 0 and 1. The default value is 1.
  - Step 6** Click **Submit**.
- 

## Create RADIUS-Vendor Dictionary Attributes

You can create, edit, and delete RADIUS vendor attributes that Cisco ISE supports. Each RADIUS-vendor attribute has a name, data type, description, and direction, which specifies whether it is relevant to requests only, responses only, or both.

- 
- Step 1** Choose **Policy > Policy Elements > Dictionaries > System > Radius > Radius Vendors**.
  - Step 2** Choose a RADIUS-vendor dictionary from the RADIUS vendor dictionaries list, and click **Edit**.
  - Step 3** Click **Dictionary Attributes**, and then click **Add**.
  - Step 4** Enter the attribute name for the RADIUS vendor attribute and an optional description.
  - Step 5** Choose the data type from the Data Type drop-down list.
  - Step 6** Check the **Enable MAC option** check box.
  - Step 7** Choose the direction that applies to RADIUS requests only, RADIUS responses only, or both from the Direction drop-down list.
  - Step 8** Enter the vendor attribute ID in the ID field.
  - Step 9** Check the **Allow Tagging** check box.
  - Step 10** Check the **Allow multiple instances of this attribute in a profile** check box.
  - Step 11** Click **Add** to add the allowed value for the vendor attribute in the Allowed Values table.
  - Step 12** Click **Submit**.
- 

## HP RADIUS IETF Service Type Attributes

Cisco ISE introduces two new values for the RADIUS IETF Service Type attribute. The RADIUS IETF service type attribute is available in **Policy > Policy Elements > Dictionaries > System > RADIUS > IETF**. You can use these two values in policy conditions. These two values are specifically designed for HP devices to understand permissions of the user.

Enumeration Name	Enumeration Value
HP-Oper	252
HP-User	255

## RADIUS Vendor Dictionary Attribute Settings

This section describes RADIUS vendor dictionaries used in Cisco ISE.

The following table describes the fields in the Dictionary window for RADIUS vendors, which allows you to configure dictionary attributes for the RADIUS vendors. The navigation path for this window is **Policy > Policy Elements > Dictionaries > System > RADIUS > RADIUS Vendors**.

**Table 4: RADIUS Vendor Dictionary Attribute Settings**

Field Name	Usage Guidelines
<b>Attribute Name</b>	Enter the vendor specific attribute name for the selected RADIUS vendor.
<b>Description</b>	Enter an optional description for the vendor specific attribute.
<b>Internal Name</b>	Enter the name for the vendor specific attribute that refers to it internally in the database.
<b>Data Type</b>	Choose one of the following data types for the vendor specific attribute: <ul style="list-style-type: none"> <li>• STRING</li> <li>• OCTET_STRING</li> <li>• UNIT32</li> <li>• UNIT64</li> <li>• IPV4</li> <li>• IPV6</li> </ul>
<b>Enable MAC option</b>	<p>Check this check box to enable the comparison of RADIUS attribute as MAC address. By default, for the RADIUS attribute calling-station-id this option is marked as enabled and you cannot disable it. For other dictionary attributes (of string types) within the RADIUS vendor dictionary, you can enable or disable this option.</p> <p>Once you enable this option, while setting the authentication and authorization conditions, you can define whether the comparison is clear string by selecting the Text option or whether it is MAC address by selecting the MAC address option.</p>
<b>Direction</b>	Choose one of the options that applies to RADIUS messages:
<b>ID</b>	Enter the vendor attribute ID. The valid range is 0 to 255.

Field Name	Usage Guidelines
<b>Allow Tagging</b>	<p>Check this check box to mark the attribute as being permitted to have a tag, as defined in RFC2868. The purpose of the tag is to allow grouping of attributes for tunnelled users. See RFC2868 for more details.</p> <p>The tagged attributes support ensures that all attributes pertaining to a given tunnel contain the same value in their respective tag fields, and that each set includes an appropriately-valued instance of the Tunnel-Preference attribute. This conforms to the tunnel attributes that are to be used in a multi-vendor network environment, thereby eliminating interoperability issues among Network Access Servers (NASs) manufactured by different vendors.</p>
<b>Allow Multiple Instances of this Attribute in a Profile</b>	<p>Check this check box when you want multiple instances of this RADIUS vendor specific attribute in profiles.</p>



**Related Topics**

- [System Defined Dictionaries and Dictionary Attributes](#), on page 28
- [User-Defined Dictionaries and Dictionary Attributes](#), on page 28
- [RADIUS-Vendor Dictionaries](#), on page 29
- [Create RADIUS-Vendor Dictionaries](#), on page 29

## 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.

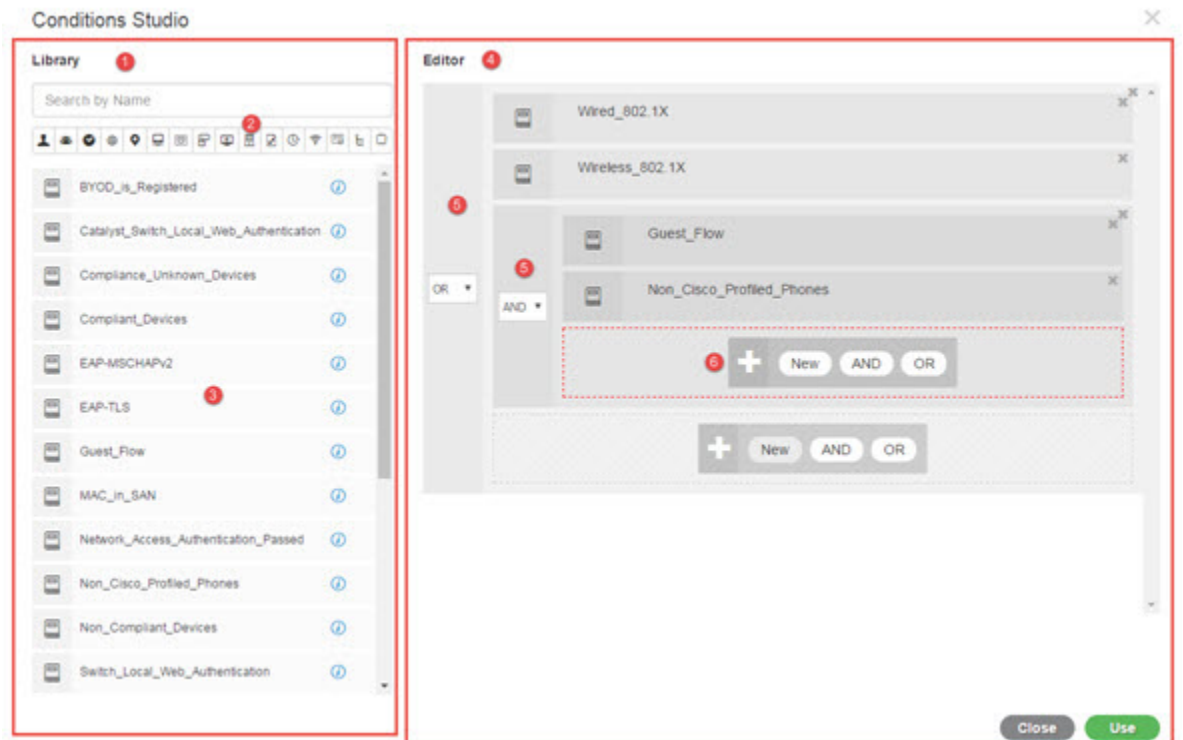
For network access policies, choose **Work Centers > Network Access > Policy Sets**. For device administration policies, choose **Work Centers > Device Administration > Device Admin Policy Sets**.

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 2: 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:

Fields	Usage Guidelines
Library	<p>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.</p> <p>Conditions stored in the Library are all represented by the Library icon , because conditions can be associated with more than one category.</p> <p>Next to each condition in the Library you can also find the i 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.</p> <p>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.</p> <p>There are also predefined conditions upon installation. These conditions can also be changed and deleted.</p>
Search and filter	<p>Search conditions by name or filter them by category. In a similar manner, you can also search and filter attributes from the <b>Click to add an attribute</b> 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.</p>
Conditions List	<p>The complete list of all conditions in the Library, or the list of conditions in the Library based on the search or filter results.</p>

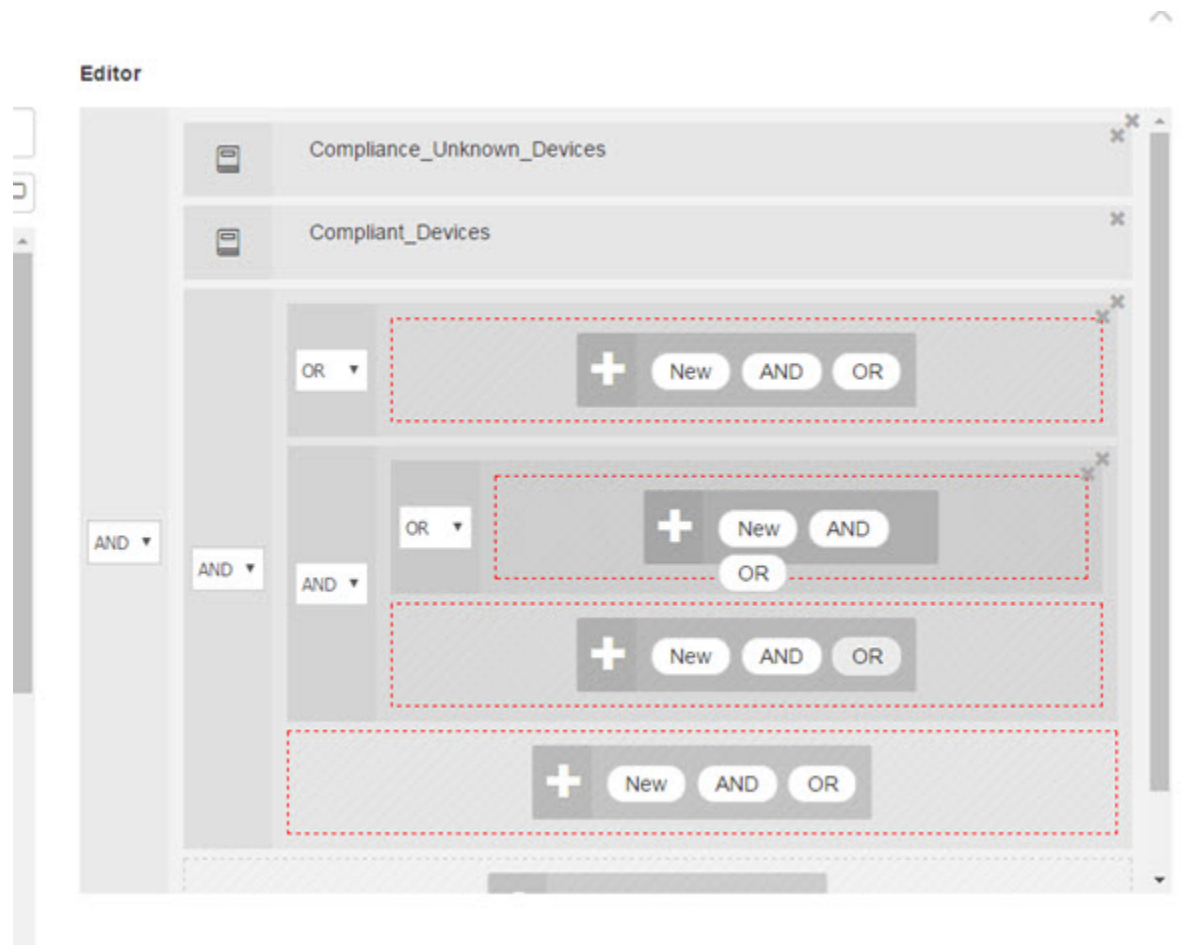
Fields	Usage Guidelines
<p>Editor</p>	<p>Create new conditions to use immediately as well as to save them in the system Library for future use, and edit existing conditions and save those changes in the Library for immediate and future use.</p> <p>When opening the Conditions Studio in order to create 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.</p> <p>When the Editor opens with empty fields, no operator icons appear</p>
	<p>The Editor is divided into different virtual columns and rows.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Once saved to the library, all condition blocks are assigned the Library icon, replacing the category icons that appeared in the Editor.</p> <p>Finally, if a rule is configured to <b>exclude</b> 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.</p>

Fields	Usage Guidelines
	<p>This area displays the options available when working with hierarchical levels as well as multiple rules within a condition.</p> <p>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.</p> <p>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.</p> <p>Additional levels can be added to the condition with the <b>AND</b> and <b>OR</b> operator options. Choose <b>New</b> to create a new rule on the same level from which you clicked the option. The <b>New</b> option only appears once you have configured at least one rule on the top level of the hierarchy.</p>

## 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 3: 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** Access the Policy Sets area. Choose **Policy** > **Policy Sets** .

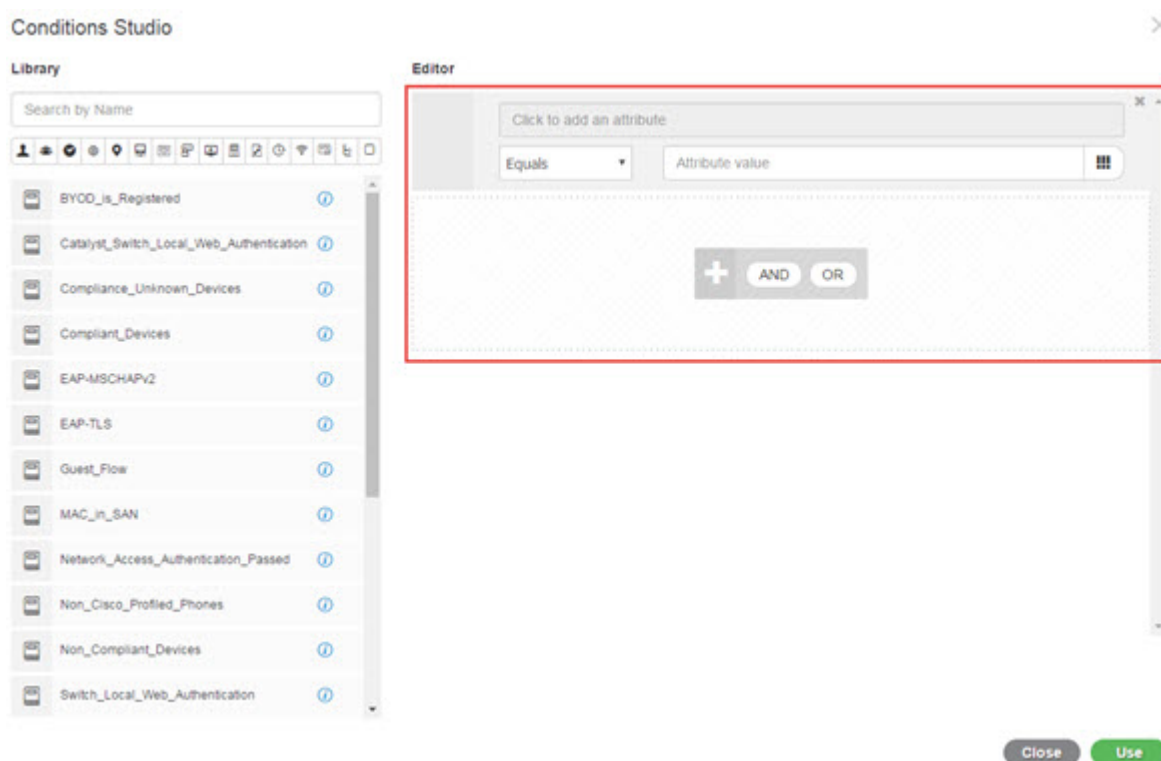
**Step 2** Access the Conditions Studio to create a new condition and to edit existing condition blocks, in order to then use those conditions as part of the rules you configure for the specific policy set (and its associated policies and rules), or in order to save to the Library for future use:

- 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 32](#).

**Figure 4: Conditions Studio—Creating a New Condition**



### Step 3

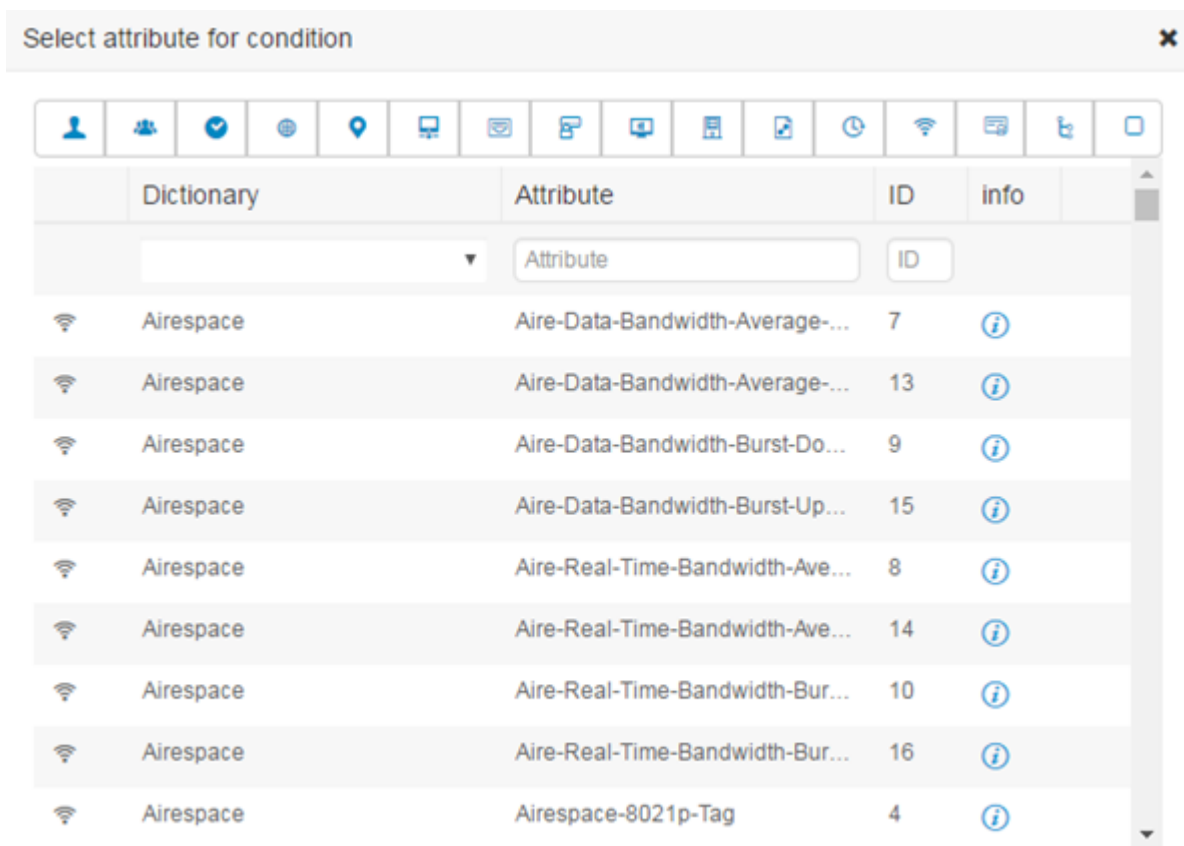
Use an existing condition block from the Library as a rule in the condition that you are creating or editing.

- 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:

Fields	Usage Guidelines
Attribute Category toolbar	<p>Contains a unique icon for each of the different attribute categories. Choose any attribute category icon to filter the view by category.</p> <p>Click a highlighted icon in order to deselect it, thereby removing the filter.</p>

Fields	Usage Guidelines
Dictionary	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.
Attribute	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.
ID	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.
Info	Hover the information icon on the relevant attribute row to view extra details about the attribute.

- 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 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.

**Note** When an AD attribute is needed in any policy set, the corresponding AD condition must be configured.

## 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 Condition 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 the IPv6 attributes in your rule conditions to process such requests from IPv6-enabled endpoints and ensure that the endpoint is compliant.

You can use wildcard characters 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
- 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

The following table lists Supported Cisco Attribute-Value pairs and their equivalent IETF attributes:

Cisco Attribute-Value Pairs	IETF Attributes
ipv6:addrv6=<ipv6 address>	Framed-ipv6-Address
ipv6:stateful-ipv6-address-pool=<name>	Stateful-IPv6-Address-Pool
ipv6:delegated-ipv6-pool=<name>	Delegated-IPv6-Prefix-Pool
ipv6:ipv6-dns-servers-addr=<ipv6 address>	DNS-Server-IPv6-Address

The RADIUS Live Logs page, RADIUS Authentication report, RADIUS Accounting report, Current Active Session report, RADIUS Error report, Misconfigured NAS report, Adaptive Network Control Audit, 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 by 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. See [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.

- 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.
- 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, Mojave, or Catalina 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 these MAC OSX devices.

---

## Configure EAP-FAST Settings

### Before you begin

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

- 
- Step 1** Choose **Administration** > **System** > **Settings** > **Protocols** > **EAP-FAST** > **EAP Fast Settings**.
  - Step 2** Enter the details as required to define the EAP-FAST protocol.
  - Step 3** Click **Revoke** if you want to revoke all the previously generated primary keys and PACs.
  - Step 4** Click **Save** to save the EAP-FAST settings.
- 

## 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**.
-

## EAP-FAST Settings

*Table 5: Configuring EAP-FAST Settings*

Field Name	Usage Guidelines
<b>Authority Identity Info Description</b>	Enter a user-friendly string that describes the Cisco ISE node that sends credentials to a client. The client can discover this string in the Protected Access Credentials (PAC) information for type, length, and value (TLV). The default value is Identity Services Engine.
<b>Master Key Generation Period</b>	Specifies the primary key generation period in seconds, minutes, hours, days, or weeks. The value must be a positive integer in the range 1 to 2147040000 seconds. The default is 604800 seconds, which is equivalent to one week.
<b>Revoke all master keys and PACs</b>	Click Revoke to revoke all primary keys and PACs.
<b>Enable PAC-less Session Resume</b>	Check this check box if you want to use EAP-FAST without the PAC files.
<b>PAC-less Session Timeout</b>	Specifies the time in seconds after which the PAC-less session resume times out. The default is 7200 seconds.

### Related Topics


[Policy Set Protocol Settings](#), on page 45

[Guidelines for Using EAP-FAST as Protocol](#), on page 45

[Benefits of EAP-FAST](#), on page 82

[Configure EAP-FAST Settings](#), on page 46

## PAC Settings

The following table describes the fields on the Generate PAC window, which you can use to configure protected access credentials for EAP-FAST authentication. The navigation path for this page is: To view this window, click the **Menu** icon () and choose **Administration > System > Settings > Protocols > EAP-FAST > Generate PAC**.

*Table 6: Generating PAC for EAP-FAST Settings*

Field Name	Usage Guidelines
<b>Tunnel PAC</b>	Click this radio button to generate a tunnel PAC.
<b>Machine PAC</b>	Click this radio button to generate a machine PAC.
<b>Trustsec PAC</b>	Click this radio button to generate a Trustsec PAC.

Field Name	Usage Guidelines
<b>Identity</b>	<p>(For Tunnel and Machine PAC) Specifies the username or machine name that is presented as the “inner username” by the EAP-FAST protocol. If the identity string does not match that username, authentication fails.</p> <p>This is the hostname as defined on the Adaptive Security Appliance (ASA). The identity string must match the ASA hostname otherwise, ASA cannot import the PAC file that is generated.</p> <p>If you are generating a Trustsec PAC, the Identity field specifies the Device ID of a Trustsec network device and is provided with an initiator ID by the EAP-FAST protocol. If the Identity string entered here does not match that Device ID, authentication fails.</p>
<b>PAC Time to Live</b>	<p>(For Tunnel and Machine PAC) Enter a value in seconds that specifies the expiration time for the PAC. The default is 604800 seconds, which is equivalent to one week. This value must be a positive integer between 1 and 157680000 seconds. For the Trustsec PAC, enter a value in days, weeks, months, or years. By default, the value is one year. The minimum value is one day and the maximum is 10 years.</p>
<b>Encryption Key</b>	<p>Enter an encryption key. The length of the key must be between 8 and 256 characters. The key can contain uppercase or lowercase letters, or numbers, or a combination of alphanumeric characters.</p>
<b>Expiration Data</b>	<p>(For Trustsec PAC only) The expiration date is calculated based on the PAC Time to Live.</p>

#### Related Topics

[Policy Set Protocol Settings](#), on page 45

[Guidelines for Using EAP-FAST as Protocol](#), on page 45

[Generate the PAC for EAP-FAST](#), on page 46

## 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:

- 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.

- Step 1** Choose **Administration > System > Settings > Protocols > EAP-TTLS**.
- Step 2** Enter the required details in the EAP-TTLS Settings page.
- Step 3** Click **Save**.

## EAP-TTLS Settings

*Table 7: EAP-TTLS Settings*

Field Name	Usage Guidelines
<b>Enable EAP-TTLS Session Resume</b>	<p>If you check this check box, Cisco ISE will cache the TLS session that is created during phase one of EAP-TTLS authentication, provided the user successfully authenticates in phase two of EAP-TTLS. If a user needs to reconnect and the original EAP-TTLS session has not timed out, Cisco ISE uses the cached TLS session, resulting in faster EAP-TTLS performance and a reduced AAA server load.</p> <p><b>Note</b> When the EAP-TTLS session is resumed, the inner method is skipped.</p>
<b>EAP-TTLS Session Timeout</b>	<p>Specifies the time in seconds after which the EAP-TTLS session times out. The default value is 7200 seconds.</p>

**Related Topics**

[Policy Set Protocol Settings](#), on page 45

[Using EAP-TTLS as Authentication Protocol](#), on page 48

[Configure EAP-TTLS Settings](#), on page 49

## Configure EAP-TLS Settings

**Before you begin**

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

- 
- Step 1** Choose **Administration** > **System** > **Settings** > **Protocols** > **EAP-TLS**.
  - Step 2** Enter the details as required to define the EAP-TLS protocol.
  - Step 3** Click **Save** to save the EAP-TLS settings.
- 

## EAP-TLS Settings

**Related Topics**

[Policy Set Protocol Settings](#), on page 45

[Configure EAP-TLS Settings](#), on page 50

## Configure PEAP Settings

**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 **PEAP**.
  - Step 4** Enter the details as required to define the PEAP protocol.
  - Step 5** Click **Save** to save the PEAP settings.
- 

## PEAP Settings

**Related Topics**

[Policy Set Protocol Settings](#), on page 45

[Configure PEAP Settings](#), on page 50

[Advantages of Using PEAP](#), on page 80

[Supported Supplicants for the PEAP Protocol](#), on page 80

[PEAP Protocol Flow](#), on page 81

## 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.
- 

## RADIUS Settings

If you enable the **Suppress Repeated Failed Clients** option, clients with repeated authentication failures will be suppressed from the audit logs, and the requests from these clients will be automatically rejected for the specified time period. You can also specify the number of authentication failures after which the requests from these clients should be rejected. For example, if this value is configured as 5, when a client authentication fails five times, all the requests received from that client will be rejected for the configured time period.



- 
- Note**
- If the cause of endpoint authentication failure is the entry of a wrong password and user type is internal user, the endpoint is suppressed and enters rejection mode.
- However, if a wrong password is detected in the case of Active Directory users, the endpoint is suppressed but does not enter rejection mode.
- 



- 
- Note** If you configure suppression of RADIUS failures, you may still receive the error "5440 Endpoint Abandoned EAP Session and started a new one" after you configure RADIUS log suppression. For more information, see the following ISE Community post:

<https://community.cisco.com/t5/network-access-control/authentication-failed-quot-5440-endpoint-abandoned-eap-session/td-p/3191944>

---

**Table 8: RADIUS Settings**

Field Name	Usage Guidelines
<b>Suppress Repeated Failed Clients</b>	

Field Name	Usage Guidelines
<b>Suppress Repeated Failed Clients</b>	<p>Check this check box to suppress the clients for which the authentications fail repeatedly for the same reason. These clients are suppressed from the audit logs and the requests from these clients are rejected for the specified time period if <b>Reject RADIUS Requests from Clients with Repeated Failures</b> option is enabled.</p> <p><b>Note</b> CTS related logs are not suppressed even if this option is enabled and are always included in the Live Logs.</p>
<b>Detect Two Failures Within</b>	<p>Enter the time interval in minutes. If a client fails authentication twice for the same reason within this time period, it will be suppressed from the audit logs, and the requests from this client will be rejected if <b>Reject RADIUS Requests from Clients with Repeated Failures</b> option is enabled.</p>
<b>Report Failures Once Every</b>	<p>Enter the time interval in minutes for the failed authentications to be reported. For example, if this value is set as 15 minutes, clients that repeatedly fail authentication will be reported in the audit logs only once every 15 minutes, thereby preventing over-reporting.</p>
<b>Reject RADIUS Requests from Clients with Repeated Failures</b>	<p>Check this check box to automatically reject the RADIUS requests from the clients for which the authentications fail repeatedly. You can enable this option to avoid unnecessary processing by Cisco ISE and to protect against potential denial of service attacks.</p>
<b>Failures Prior to Automatic Rejection</b>	<p>Enter the number of authentication failures after which requests from clients with repeated failures are automatically rejected. All the requests received from these clients are automatically rejected for the configured time period (specified in <b>Continue Rejecting Requests for</b> field). After the interval expires, the authentication requests from these clients are processed.</p>
<b>Continue Rejecting Requests for</b>	<p>Enter the time interval (in minutes) for which the requests from clients with repeated failures are to be rejected.</p>
<b>Ignore Repeated Accounting Updates Within</b>	<p>Repeated accounting updates that occur within this period will be ignored.</p>
<b>Suppress Successful Reports</b>	

Field Name	Usage Guidelines
<b>Suppress Repeated Successful Authentications</b>	Check this check box to prevent repeated reporting of successful authentication requests in last 24 hours that have no change in identity context, network device, and authorization.
<b>Authentications Details</b>	
<b>Highlight Steps Longer Than</b>	Enter the time interval in milliseconds. If execution of a single step exceeds the specified threshold, it will be marked with a clock icon in the authentication details page.
<b>Disclose Invalid Usernames</b>	Check this checkbox to disclose the usernames labelled as 'USERNAME' or 'INVALID' in the Radius Live Logs. You can then view the logged in username in the Radius Live Logs as well as in the Authentication Summary Report. This option will be disabled automatically after 30 minutes.
<b>RADIUS UDP Ports</b>	
<b>Authentication Ports</b>	Specify the ports to be used for RADIUS UDP authentication flows. You can specify a maximum of 4 port numbers (separated by a comma). By default, port 1812 and port 1645 are used. The valid range is from 1024 to 65535.
<b>Accounting Ports</b>	Specify the ports to be used for RADIUS UDP accounting flows. You can specify a maximum of 4 port numbers (separated by a comma). By default, port 1813 and port 1646 are used. The valid range is from 1024 to 65535.  <b>Note</b> Ensure that these ports are not used by other services.
<b>RADIUS DTLS</b>	
<b>Authentication and Accounting Port</b>	Specify the port to be used for RADIUS DTLS authentication and accounting flows. By default, port 2083 is used. The valid range is from 1024 to 65535.  <b>Note</b> Ensure that this port is not used by other services.
<b>Idle Timeout</b>	Enter the time (in seconds) that you want Cisco ISE to wait before it closes the TLS session if no packets are received from the network device. Default value is 120 seconds. The valid range is from 60 to 600 seconds.

Field Name	Usage Guidelines
<b>Enable RADIUS/DTLS Client Identity Verification</b>	<p>Check this check box if you want Cisco ISE to verify the identity of the RADIUS/DTLS clients during the DTLS handshake. Cisco ISE fails the handshake if the client identity is not valid. Identity check is skipped for the default network device, if configured. Identity check is performed in the following sequence:</p> <ol style="list-style-type: none"> <li>1. If the client certificate contains the subject alternative name (SAN) attribute: <ul style="list-style-type: none"> <li>• If SAN contains the DNS name, the DNS name specified in the certificate is compared with the DNS name that is configured for the network device in Cisco ISE.</li> <li>• If SAN contains the IP address (and does not contain the DNS name), the IP address specified in the certificate is compared with all the device IP addresses configured in Cisco ISE.</li> </ul> </li> <li>2. If the certificate does not contain SAN, subject CN is compared with the DNS name that is configured for the network device in Cisco ISE. Cisco ISE fails the handshake in the case of mismatch.</li> </ol>

#### Related Topics

[Policy Set Protocol Settings](#), on page 45

[RADIUS Protocol Support in Cisco ISE](#), on page 57

[Configure RADIUS Settings](#), on page 51

## Configure Security Settings

Perform the following procedure to configure the security settings.

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

**Step 2** In the **Security Settings** window, choose 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 an EAP server
  - Cisco ISE downloads CRL from HTTPS or a secure LDAP server
  - Cisco ISE is configured as a secure TCP syslog client
  - Cisco ISE is configured as a secure LDAP client
  - Cisco ISE is configured as an ERS server

Also allows TLS 1.0 for communication with the following Cisco ISE components:

- All portals
- Certificate Authority
- MDM Client
- pxGrid
- PassiveID Agent

**Note** We recommend that clients and servers negotiate to use a higher version of TLS for enhanced security.

• **Allow TLS 1.1:** Allows TLS 1.1 for communication with legacy peers for the following workflows:

- Cisco ISE is configured as an EAP server
- Cisco ISE downloads CRL from HTTPS or a secure LDAP server
- Cisco ISE is configured as a secure TCP syslog client
- Cisco ISE is configured as a secure LDAP client
- Cisco ISE is configured as an ERS server

Also allows TLS 1.1 for communication with the following Cisco ISE components:

- All portals
- Certificate Authority
- External RESTful Services (ERS)
- MDM Client
- pxGrid

**Note** We recommend that clients and servers negotiate to use a higher version of TLS for enhanced security.

• **Allow SHA-1 Ciphers:** Allows SHA-1 ciphers for communication with peers for the following workflows:

- Cisco ISE is configured as an EAP server
- Cisco ISE is configured as a RADIUS DTLS server
- Cisco ISE is configured as a RADIUS DTLS client
- Cisco ISE downloads CRL from HTTPS or a secure LDAP server
- Cisco ISE is configured as a secure syslog client
- Cisco ISE is configured as a secure LDAP client

Also allows SHA-1 ciphers for communication with the following Cisco ISE components:

- Admin Access UI
- All portals
- ERS

- pxGrid
- Admin Access: 443
- Cisco ISE Portals: 9002, 8443, 8444, 8445, 8449
- ERS: 9060, 9061, 9063
- pxGrid: 8910

**Note** This option is disabled by default.

You must restart all the nodes in a deployment after enabling or disabling the **Allow SHA-1 Ciphers** option. If restart is not successful, the configuration changes are not applied. In such a scenario, you must restart all the nodes manually using the following commands:

**application stop ise** and **application start ise**.

**Note** We recommend that you use SHA-256 or SHA-384 ciphers for enhanced security.

- **Allow ECDHE-RSA Ciphers:** Allows ECDHE-RSA ciphers for communication with peers for the following workflows:
  - Cisco ISE is configured as an EAP server
  - Cisco ISE is configured as a RADIUS DTLS server
  - Cisco ISE is configured as a RADIUS DTLS client
  - Cisco ISE downloads CRL from HTTPS or a secure LDAP server
  - Cisco ISE is configured as a secure syslog client
  - Cisco ISE is configured as a secure LDAP client
- **Allow 3DES ciphers:** Allows 3DES ciphers for communication with peers for the following workflows:
  - Cisco ISE is configured as an EAP server
  - Cisco ISE is configured as a RADIUS DTLS server
  - Cisco ISE is configured as a RADIUS DTLS client
  - Cisco ISE downloads CRL from HTTPS or a secure LDAP server
  - Cisco ISE is configured as a secure syslog client
  - Cisco ISE is configured as a secure LDAP client
- **Accept Certificates without Validating Purpose:** When Cisco ISE acts as an EAP or RADIUS DTLS server, client certificates are accepted without checking whether:
  - The Key Usage extension contains the keyAgreement bit for ECDHE-ECDSA ciphers or the keyEncipherment bit for other ciphers
  - Extended Key Usage attribute value is ClientAuth

When this option is disabled, Cisco ISE will validate the purpose of all the client certificates. A certificate will be considered valid only if one of the following conditions is met:



- If there is no value for the Extended Key Usage attribute:
  - If the cipherGroup is ECDHE-ECDSA, then the Key Usage extension must contain the KeyAgreement value.
  - If the cipherGroup is not ECDHE-ECDSA, then the Key Usage extension must contain the keyEncipherment and digitalSignature values.
- If the Extended Key Usage attribute value is ClientAuth:
  - If the cipherGroup is ECDHE-ECDSA, then the Key Usage extension must contain the KeyAgreement value.
  - If the cipherGroup is not ECDHE-ECDSA, then the Key Usage extension must contain the keyEncipherment and digitalSignature values.

The certificate validation will fail if none of the above conditions are met.

- **Allow DSS ciphers for ISE as a client:** When Cisco ISE acts as a client, allows DSS ciphers for communication with a server for the following workflows:
  - Cisco ISE is configured as a RADIUS DTLS client
  - Cisco ISE downloads CRL from HTTPS or a secure LDAP server
  - Cisco ISE is configured as a secure syslog client
  - Cisco ISE is configured as a secure LDAP client
- **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 a secure LDAP server
  - Cisco ISE is configured as a secure syslog client
  - Cisco ISE is configured as a secure LDAP client

**Step 3** Click **Save**.

---

## RADIUS Protocol Support in Cisco ISE

RADIUS is a client/server protocol through which remote-access servers communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. You can use RADIUS to maintain user profiles in a central database that all remote servers can share. This protocol provides better security, and you can use it to set up a policy that is applied at a single administered network point.

RADIUS also functions as a RADIUS client in Cisco ISE to proxy requests to a remote RADIUS server, and it provides Change of Authorization (CoA) activities during an active session.

Cisco ISE supports RADIUS protocol flow according to RFC 2865 and generic support for all general RADIUS attributes as described in RFC 2865 and its extension. Cisco ISE supports parsing of vendor-specific attributes only for vendors that are defined in the Cisco ISE dictionary.

RADIUS interface supports the following attribute data types that are defined in RFC 2865:

- Text (Unicode Transformation Format [UTF])
- String (binary)
- Address (IP)
- Integer
- Time

#### [ISE Community Resource](#)

For information about the network access attributes supported by Cisco ISE, see [ISE Network Access Attributes](#).

## Allowed Protocols

The following table describes the fields in the **Allowed Protocols** window, which allows you to configure the protocols to be used during authentication. The navigation path is **Policy > Policy Elements > Results > Authentication > Allowed Protocols**.

**Table 9: Allowed Protocols**

Field Name	Usage Guidelines
<b>Allowed Protocols &gt; Authentication Bypass</b>	
<b>Process Host Lookup</b>	<p>Check this check box if you want Cisco ISE to process the Host Lookup request. The Host Lookup request is processed for PAP/CHAP protocol when the RADIUS Service-Type equals 10 (Call-Check) and the username is equal to Calling-Station-ID. The Host Lookup request is processed for EAP-MD5 protocol when the Service-Type equals 1 (Framed) and the username is equal to Calling-Station-ID. Uncheck this check box if you want Cisco ISE to ignore the Host Lookup request and use the original value of the system username attribute for authentication. When unchecked, message processing is done according to the protocol (for example, PAP).</p> <p><b>Note</b>      Disabling this option could result in the failure of existing MAB authentications.</p>
<b>Allowed Protocols &gt; Authentication Protocols</b>	
<b>Allow PAP/ASCII</b>	This option enables PAP/ASCII. PAP uses cleartext passwords (that is, unencrypted passwords) and is the least secure authentication protocol.

Field Name	Usage Guidelines
<b>Allow CHAP</b>	This option enables CHAP authentication. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with Microsoft Active Directory.
<b>Allow MS-CHAPv1</b>	Check this check box to enable MS-CHAPv1.
<b>Allow MS-CHAPv2</b>	Check this check box to enable MS-CHAPv2.
<b>Allow EAP-MD5</b>	Check this check box to enable EAP-based MD5 password hashed authentication.

Field Name	Usage Guidelines
<p><b>Allow EAP-TLS</b></p>	<p>Check this check box to enable EAP-TLS Authentication protocol and configures EAP-TLS settings. You can specify how Cisco ISE will verify the user identity as presented in the EAP identity response from the end-user client. User identity is verified against information in the certificate that the end-user client presents. This comparison occurs after an EAP-TLS tunnel is established between Cisco ISE and the end-user client.</p> <p><b>Note</b> EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps to configure certificates.</p> <ul style="list-style-type: none"> <li>• <b>Allow authentication of expired certificates to allow certificate renewal in Authorization Policy:</b> Check this check box, if you want to allow users to renew certificates. If you check this check box, ensure that you configure appropriate authorization policy rules to check if the certificate has been renewed before processing the request any further.</li> <li>• <b>Enable Stateless Session Resume:</b> Check this check box to allow EAP-TLS session resumption without requiring the session state to be stored at the server. Cisco ISE supports session ticket extension as described in RFC 5077. Cisco ISE creates a ticket and sends it to an EAP-TLS client. The client presents the ticket to ISE to resume a session.</li> <li>• <b>Proactive Session Ticket update:</b> Enter the value as a percentage to indicate how much of the Time To Live (TTL) must elapse before the session ticket is updated. For example, if you enter the value 60, the session ticket is updated after 60 percent of the TTL has expired.</li> <li>• <b>Session ticket Time to Live:</b> Enter the time after which the session ticket expires. This value determines the duration that a session ticket remains active. You can enter the value in seconds, minutes, hours, days, or weeks.</li> </ul>
<p><b>Allow LEAP</b></p>	<p>Check this check box to enable Lightweight Extensible Authentication Protocol (LEAP) authentication.</p>

Field Name	Usage Guidelines
Allow PEAP	

Field Name	Usage Guidelines
	<p>Check this check box to enable PEAP authentication protocol and PEAP settings. The default inner method is MS-CHAPv2.</p> <p>When you check the Allow PEAP check box, you can configure the following PEAP inner methods:</p> <ul style="list-style-type: none"> <li>• <b>Allow EAP-MS-CHAPv2:</b> Check this check box to use EAP-MS-CHAPv2 as the inner method. <ul style="list-style-type: none"> <li>• <b>Allow Password Change:</b> Check this check box for Cisco ISE to support password changes.</li> <li>• <b>Retry Attempts:</b> Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0 to 3.</li> </ul> </li> <li>• <b>Allow EAP-GTC:</b> Check this check box to use EAP-GTC as the inner method. <ul style="list-style-type: none"> <li>• <b>Allow Password Change:</b> Check this check box for Cisco ISE to support password changes.</li> <li>• <b>Retry Attempts:</b> Specifies how many times Cisco ISE requests user credentials before returning login failure. The valid range is from 0 to 3.</li> </ul> </li> <li>• <b>Allow EAP-TLS:</b> Check this check box to use EAP-TLS as the inner method. <p>Check the <b>Allow authentication of expired certificates to allow certificate renewal in Authorization Policy</b> check box, if you want to allow users to renew certificates. If you check this check box, ensure that you configure appropriate authorization policy rules to check if the certificate has been renewed before processing the request any further.</p> </li> <li>• <b>Require Cryptobinding TLV:</b> Check this check box if you want both the EAP peer and the EAP server to participate in the inner and outer EAP authentications of the PEAP authentication.</li> <li>• <b>Allow PEAPv0 Only for Legacy Clients:</b> Check this check box to allow PEAP supplicants to negotiate using PEAPv0. Some legacy clients do not conform to the PEAPv1 protocol standards.</li> </ul>

Field Name	Usage Guidelines
	To ensure that such PEAP conversations are not dropped, check this check box.

Field Name	Usage Guidelines
Allow EAP-FAST	



Field Name	Usage Guidelines
	<p>Check this check box to enable EAP-FAST authentication protocol and EAP-FAST settings. The EAP-FAST protocol can support multiple internal protocols on the same server. The default inner method is MS-CHAPv2.</p> <p>When you check the Allow EAP-FAST check box, you can configure EAP-FAST as the inner method:</p> <ul style="list-style-type: none"> <li>• <b>Allow EAP-MS-CHAPv2</b> <ul style="list-style-type: none"> <li>• <b>Allow Password Change:</b> Check this check box for Cisco ISE to support password changes.</li> <li>• <b>Retry Attempts:</b> Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0-3.</li> </ul> </li> <li>• <b>Allow EAP-GTC</b> <ul style="list-style-type: none"> <li><b>Allow Password Change:</b> Check this check box for Cisco ISE to support password changes.</li> <li><b>Retry Attempts:</b> Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0-3.</li> </ul> </li> <li>• <b>Use PACs:</b> Choose this option to configure Cisco ISE to provision authorization Protected Access Credentials (PAC) for EAP-FAST clients. Additional PAC options appear.</li> <li>• <b>Don't Use PACs:</b> Choose this option to configure Cisco ISE to use EAP-FAST without issuing or accepting any tunnel or machine PACs. All requests for PACs are ignored and Cisco ISE responds with a Success-TLV without a PAC. <ul style="list-style-type: none"> <li>When you choose this option, you can configure Cisco ISE to perform machine authentication.</li> </ul> </li> <li>• <b>Allow EAP-TLS:</b> Check this check box to use EAP-TLS as the inner method.</li> </ul> <p>Check the <b>Allow authentication of expired certificates to allow certificate renewal in Authorization Policy</b> check box, if you want to allow users to renew certificates. If you check this check box, ensure that you configure appropriate authorization policy rules to check if the certificate has been renewed before processing the request any further.</p>

Field Name	Usage Guidelines
	<ul style="list-style-type: none"> <li>• <b>Enable EAP Chaining:</b> Check this check box to enable EAP chaining.</li> </ul> <p>EAP chaining allows Cisco ISE to correlate the results of user and machine authentication and apply the appropriate authorization policy using the EAPChainingResult attribute.</p> <p>EAP chaining requires a supplicant that supports EAP chaining on the client device. Choose the User and Machine Authentication option in the supplicant.</p> <p>EAP chaining is available when you choose the EAP-FAST protocol (both in PAC based and PAC less mode).</p> <p>For PAC-based authentication, you can use user authorization PAC or machine authorization PAC, or both to skip the inner method.</p> <p>For certificate-based authentication, if you enable the Accept Client Certificate for Provisioning option for the EAP-FAST protocol (in the Allowed Protocol service), and if the endpoint (AnyConnect) is configured to send the user certificate inside the tunnel, then during tunnel establishment, ISE authenticates the user using the certificate (the inner method is skipped), and machine authentication is done through the inner method. If these options are not configured, EAP-TLS is used as the inner method for user authentication.</p> <p>After you enable EAP chaining, update your authorization policy and add a condition using the NetworkAccess:EapChainingResult attribute and assign appropriate permissions.</p>

Field Name	Usage Guidelines
<b>Allow EAP-TTLS</b>	<p>Check this check box to enable EAP-TTLS protocol.</p> <p>You can configure the following inner methods:</p> <ul style="list-style-type: none"> <li>• <b>Allow PAP/ASCII:</b> Check this check box to use PAP/ASCII as the inner method. You can use EAP-TTLS PAP for token and OTP-based authentications.</li> <li>• <b>Allow CHAP:</b> Check this check box to use CHAP as the inner method. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with Microsoft Active Directory.</li> <li>• <b>Allow MS-CHAPv1:</b> Check this check box to use MS-CHAPv1 as the inner method.</li> <li>• <b>Allow MS-CHAPv2:</b> Check this check box to use MS-CHAPv2 as the inner method.</li> <li>• <b>Allow EAP-MD5:</b> Check this check box to use EAP-MD5 as the inner method.</li> <li>• <b>Allow EAP-MS-CHAPv2:</b> Check this check box to use EAP-MS-CHAPv2 as the inner method. <ul style="list-style-type: none"> <li>• <b>Allow Password Change:</b> Check this check box for Cisco ISE to support password changes.</li> <li>• <b>Retry Attempts:</b> Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0 to 3.</li> </ul> </li> </ul>
<b>Preferred EAP Protocol</b>	<p>Check this check box to choose your preferred EAP protocols from any of the following options: EAP-FAST, PEAP, LEAP, EAP-TLS, EAP-TTLS, and EAP-MD5. If you do not specify the preferred protocol, EAP-TLS is used by default.</p>
<b>EAP-TLS L-bit</b>	<p>Check this check box to support legacy EAP supplicants that expect length-included flag (L-bit flag) by default in TLS Change Cipher Spec message and Encrypted Handshake message from ISE.</p>

Field Name	Usage Guidelines
<b>Allow Weak Ciphers for EAP</b>	<p>If this option is enabled, legacy clients are allowed to negotiate using weak ciphers (such as RSA_RC4_128_SHA, RSA_RC4_128_MD5). We recommend that you enable this option only if your legacy clients support only weak ciphers.</p> <p>This option is disabled by default.</p> <p><b>Note</b> Cisco ISE does not support EDH_RSA_DES_64_CBC_SHA and EDH_DSS_DES_64_CBC_SHA.</p>
<b>Require Message Authenticator for all RADIUS Requests</b>	<p>If this option is enabled, Cisco ISE verifies whether the RADIUS Message Authenticator attribute is present in the RADIUS message. If the message authenticator attribute is not present, the RADIUS message is discarded.</p> <p>Enabling this option provides protection from spoofed Access-Request messages and RADIUS message tampering.</p> <p>The RADIUS Message Authenticator attribute is a Message Digest 5 (MD5) hash of the entire RADIUS message.</p> <p><b>Note</b> EAP uses the Message Authenticator attribute by default and does not require that you enable it.</p>
<b>Allow 5G</b>	<p>Check this check box to enable Cisco Private 5G in Cisco ISE.</p> <p><b>Note</b> You must already have Cisco Private 5G deployed in your network, prior to enabling 5G as a Service (5GaaS) in Cisco ISE</p>

**Related Topics**

[Allowed Protocols in FIPS and Non-FIPS Modes for TACACS+ Device Administration](#)

[Define Allowed Protocols for Network Access, on page 76](#)

## PAC Options

The following table describes the fields after you select Use PACs in the **Allowed Protocols Services List** window. The navigation path for this window is **Policy > Policy Elements > Results > Authentication > Allowed Protocols**.

*Table 10: PAC Options*

Field Name	Usage Guidelines
Use PAC	

Field Name	Usage Guidelines
	<ul style="list-style-type: none"> <li>• Tunnel PAC Time To Live: The Time to Live (TTL) value restricts the lifetime of the PAC. Specify the lifetime value and units. The default is 90 days. The range is between 1 and 1825 days.</li> <li>• Proactive PAC Update When: &lt;n%&gt; of PAC TTL is Left: The Update value ensures that the client has a valid PAC. Cisco ISE initiates an update after the first successful authentication but before the expiration time that is set by the TTL. The update value is a percentage of the remaining time in the TTL. The default is 90%.</li> <li>• Allow Anonymous In-band PAC Provisioning: Check this check box for Cisco ISE to establish a secure anonymous TLS handshake with the client and provision it with a PAC by using phase zero of EAP-FAST with EAP-MSCHAPv2. To enable anonymous PAC provisioning, you must choose both of the inner methods, EAP-MSCHAPv2 and EAP-GTC.</li> <li>• Allow Authenticated In-band PAC Provisioning: Cisco ISE uses SSL server-side authentication to provision the client with a PAC during phase zero of EAP-FAST. This option is more secure than anonymous provisioning but requires that a server certificate and a trusted root CA be installed on Cisco ISE.  When you check this option, you can configure Cisco ISE to return an Access-Accept message to the client after successful authenticated PAC provisioning. <ul style="list-style-type: none"> <li>• Server Returns Access Accept After Authenticated Provisioning: Check this check box if you want Cisco ISE to return an access-accept package after authenticated PAC provisioning.</li> </ul> </li> <li>• Allow Machine Authenticatio: Check this check box for Cisco ISE to provision an end-user client with a machine PAC and perform machine authentication (for end-user clients who do not have the machine credentials). The machine PAC can be provisioned to the client by request (in-band) or by the administrator (out-of-band). When Cisco ISE receives a valid machine PAC from the end-user client, the machine identity</li> </ul>

Field Name	Usage Guidelines
	<p>details are extracted from the PAC and verified in the Cisco ISE external identity source. Cisco ISE only supports Active Directory as an external identity source for machine authentication. After these details are correctly verified, no further authentication is performed.</p> <p>When you check this option, you can enter a value for the amount of time that a machine PAC is acceptable for use. When Cisco ISE receives an expired machine PAC, it automatically reprovisions the end-user client with a new machine PAC (without waiting for a new machine PAC request from the end-user client).</p> <ul style="list-style-type: none"> <li>• <b>Enable Stateless Session Resume:</b> Check this check box for Cisco ISE to provision authorization PACs for EAP-FAST clients and skip phase two of EAP-FAST (default = enabled).</li> </ul> <p>Uncheck this check box in the following cases:</p> <ul style="list-style-type: none"> <li>• If you do not want Cisco ISE to provision authorization PACs for EAP-FAST clients</li> <li>• To always perform phase two of EAP-FAST</li> </ul> <p>When you check this option, you can enter the authorization period of the user authorization PAC. After this period, the PAC expires. When Cisco ISE receives an expired authorization PAC, it performs phase two EAP-FAST authentication.</p>

**Related Topics**

- [OOB TrustSec PAC](#)
- [Generate the PAC for EAP-FAST](#), on page 46

## 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.

### 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+ 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 11: TACACS+ External Server Settings*

Fields	Usage Guidelines
Name	Enter the name of the TACACS+ external server.

Fields	Usage Guidelines
Description	Enter a description for the TACACS+ external server setting.
Host IP	Enter the IP address (IPv4 or IPv6 address) of the remote TACACS+ external server.
Connection Port	Enter the port number of the remote TACACS+ external server. The port number is 49.
Timeout	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.
Shared Secret	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.
Use Single Connect	<p>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.</p> <p>You can check the Use Single Connect check box for high-traffic environment and uncheck it for low-traffic environment.</p>

## 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.

## 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 12: TACACS+ Server Sequence Settings*

Fields	Usage Guidelines
Name	Enter the name of the TACACS proxy server sequence.
Description	Enter a description for the TACACS proxy server sequence.
Server List	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.
Logging Control	Check to enable logging control: <ul style="list-style-type: none"> <li>• Local Accounting: Accounting messages are logged by the server that handles requests from devices.</li> <li>• Remote Accounting: Accounting messages are logged by the proxy server that handles requests from devices.</li> </ul>
Username Stripping	Username Prefix/Suffix Stripping: <ul style="list-style-type: none"> <li>• 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 \.</li> <li>• Suffix Strip: Check to strip the username from the suffix. For example, if the subject name is smith@acme.com and the separator is @, the username becomes smith. The default separator is @.</li> </ul>

## 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-Generic 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.

## Network Access for Users

For network access, a host connects to the network device and requests to use network resources. The network device identifies the newly connected host, and, using the RADIUS protocol as a transport mechanism, requests Cisco ISE to authenticate and authorize the user.

Cisco ISE supports network access flows depending on the protocol that is transported over the RADIUS protocol.

### RADIUS-Based Protocols Without EAP

RADIUS-based protocols that do not include EAP include the following:

- Password Authentication Protocol (PAP)
- CHAP
- Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1)
- MS-CHAP version 2 (MS-CHAPv2)

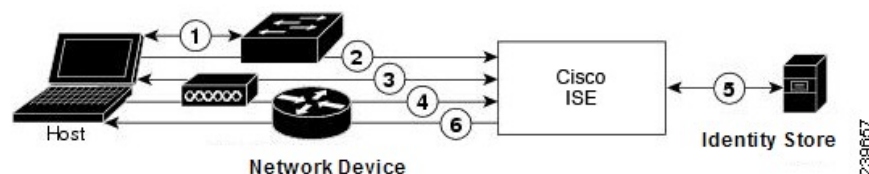
### RADIUS-Based Non-EAP Authentication Flow

This section describes RADIUS-based flow without EAP authentication. RADIUS-based flow with PAP authentication occurs in the following process:

1. A host connects to a network device.
2. The network device sends a RADIUS request (Access-Request) to Cisco ISE that contains RADIUS attributes that are appropriate to the specific protocol that is being used (PAP, CHAP, MS-CHAPv1, or MS-CHAPv2).
3. Cisco ISE uses an identity store to validate user credentials.
4. A RADIUS response (Access-Accept or Access-Reject) is sent to the network device that will apply the decision.

The following figure shows a RADIUS-based authentication without EAP.

**Figure 5: RADIUS-Based Authentication Without EAP**



The non-EAP protocols supported by Cisco ISE are:

### *Password Authentication Protocol*

PAP provides a simple method for users to establish their identity by using a two-way handshake. The PAP password is encrypted with a shared secret and is the least sophisticated authentication protocol. PAP is not a strong authentication method because it offers little protection from repeated trial-and-error attacks.

### *RADIUS-Based PAP Authentication in Cisco ISE*

Cisco ISE checks the username and password pair against the identity stores, until it eventually acknowledges the authentication or terminates the connection.

You can use different levels of security concurrently with Cisco ISE for different requirements. PAP applies a two-way handshaking procedure. If authentication succeeds, Cisco ISE returns an acknowledgment; otherwise, Cisco ISE terminates the connection or gives the originator another chance.

The originator is in total control of the frequency and timing of the attempts. Therefore, any server that can use a stronger authentication method will offer to negotiate that method prior to PAP. RFC 1334 defines PAP.

Cisco ISE supports standard RADIUS PAP authentication that is based on the RADIUS UserPassword attribute. RADIUS PAP authentication is compatible with all identity stores.

The RADIUS-with-PAP-authentication flow includes logging of passed and failed attempts.

### *Challenge Handshake Authentication Protocol*

CHAP uses a challenge-response mechanism with one-way encryption on the response. CHAP enables Cisco ISE to negotiate downward from the most-secure to the least-secure encryption mechanism, and it protects passwords that are transmitted in the process. CHAP passwords are reusable. If you are using the Cisco ISE internal database for authentication, you can use PAP or CHAP. CHAP does not work with the Microsoft user database. Compared to RADIUS PAP, CHAP allows a higher level of security for encrypting passwords when communicating from an end-user client to the AAA client.

Cisco ISE supports standard RADIUS CHAP authentication that is based on the RADIUS ChapPassword attribute. Cisco ISE supports RADIUS CHAP authentication only with internal identity stores.

### *Microsoft Challenge Handshake Authentication Protocol Version 1*

Cisco ISE supports the RADIUS MS-CHAPv1 authentication and change-password features. RADIUS MS-CHAPv1 contains two versions of the change-password feature: Change-Password-V1 and Change-Password-V2. Cisco ISE does not support Change-Password-V1 based on the RADIUS MS-CHAP-CPW-1 attribute, and supports only Change-Password-V2 based on the MS-CHAP-CPW-2 attribute. The RADIUS MS-CHAPv1 authentication and change-password features are supported with the following identity sources:

- Internal identity stores
- Microsoft Active Directory identity store

### *Microsoft Challenge Handshake Authentication Protocol Version 2*

The RADIUS MS-CHAPv2 authentication and change-password features are supported with the following identity sources:

- Internal identity stores
- Microsoft Active Directory identity store

## RADIUS-Based EAP Protocols

EAP provides an extensible framework that supports various authentication types. This section describes the EAP methods supported by Cisco ISE and contains the following topics:

### Simple EAP Methods

- EAP-Message Digest 5
- Lightweight EAP

### EAP Methods That Use Cisco ISE Server Certificate for Authentication

- PEAP/EAP-MS-CHAPv2
- PEAP/EAP-GTC
- EAP-FAST/EAP-MS-CHAPv2
- EAP-FAST/EAP-GTC

Apart from the methods listed above, there are EAP methods that use certificates for both server and client authentication.

## RADIUS-Based EAP Authentication Flow

Whenever EAP is involved in the authentication process, the process is preceded by an EAP negotiation phase to determine which specific EAP method (and inner method, if applicable) should be used. EAP-based authentication occurs in the following process:

1. A host connects to a network device.
2. The network device sends an EAP Request to the host.
3. The host replies with an EAP Response to the network device.
4. The network device encapsulates the EAP Response that it received from the host into a RADIUS Access-Request (using the EAP-Message RADIUS attribute) and sends the RADIUS Access-Request to Cisco ISE.
5. Cisco ISE extracts the EAP Response from the RADIUS packet and creates a new EAP Request, encapsulates it into a RADIUS Access-Challenge (again, using the EAP-Message RADIUS attribute), and sends it to the network device.
6. The network device extracts the EAP Request and sends it to the host.

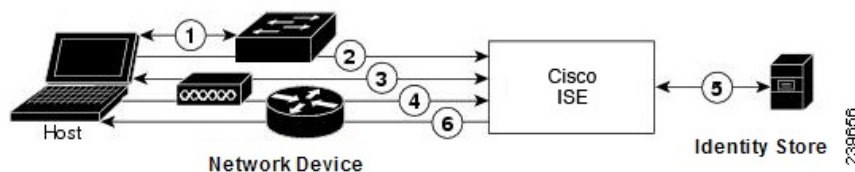
In this way, the host and Cisco ISE indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication.

The EAP messages that are subsequently exchanged are then used to carry the data that is needed to perform the actual authentication. If it is required by the specific EAP authentication method that is negotiated, Cisco ISE uses an identity store to validate user credentials.

After Cisco ISE determines whether the authentication should pass or fail, it sends either an EAP-Success or EAP-Failure message, encapsulated into a RADIUS Access-Accept or Access-Reject message to the network device (and ultimately also to the host).

The following figure shows a RADIUS-based authentication with EAP.

**Figure 6: RADIUS-Based Authentication with EAP**



### Extensible Authentication Protocol-Message Digest 5

Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) provides one-way client authentication. The server sends the client a random challenge. The client proves its identity in a response by encrypting the challenge and its password with MD5. Because a man in the middle could see the challenge and response, EAP-MD5 is vulnerable to dictionary attack when used over an open medium. Because no server authentication occurs, it is also vulnerable to spoofing. Cisco ISE supports EAP-MD5 authentication against the Cisco ISE internal identity store. Host Lookup is also supported when using the EAP-MD5 protocol.

### Lightweight Extensible Authentication Protocol

Cisco ISE currently uses Lightweight Extensible Authentication Protocol (LEAP) only for Cisco Aironet wireless networking. If you do not enable this option, Cisco Aironet end-user clients who are configured to perform LEAP authentication cannot access the network. If all Cisco Aironet end-user clients use a different authentication protocol, such as Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), we recommend that you disable this option.



**Note** If users access your network by using a AAA client that is defined in the *Network Devices* section as a RADIUS (Cisco Aironet) device, then you must enable LEAP, EAP-TLS, or both; otherwise, Cisco Aironet users cannot authenticate.

### Protected Extensible Authentication Protocol

Protected Extensible Authentication Protocol (PEAP) provides mutual authentication, ensures confidentiality and integrity to vulnerable user credentials, protects itself against passive (eavesdropping) and active (man-in-the-middle) attacks, and securely generates cryptographic keying material. PEAP is compatible with the IEEE 802.1X standard and RADIUS protocol. Cisco ISE supports PEAP version 0 (PEAPv0) and PEAP version 1 (PEAPv1) with Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol (EAP-MS-CHAP), Extensible Authentication Protocol-Generic Token Card (EAP-GTC), and EAP-TLS inner methods. The Cisco Secure Services Client (SSC) supplicant supports all of the PEAPv1 inner methods that Cisco ISE supports.

### Advantages of Using PEAP

Using PEAP presents these advantages: PEAP is based on TLS, which is widely implemented and has undergone extensive security review. It establishes a key for methods that do not derive keys. It sends an identity within the tunnel. It protects inner method exchanges and the result message. It supports fragmentation.

### Supported Supplicants for the PEAP Protocol

PEAP supports these supplicants:



- Microsoft Built-In Clients 802.1X XP
- Microsoft Built-In Clients 802.1X Vista
- Cisco Secure Services Client (SSC), Release 4.0
- Cisco SSC, Release 5.1
- Funk Odyssey Access Client, Release 4.72
- Intel, Release 12.4.0.0

### PEAP Protocol Flow

A PEAP conversation can be divided into three parts:

1. Cisco ISE and the peer build a TLS tunnel. Cisco ISE presents its certificate, but the peer does not. The peer and Cisco ISE create a key to encrypt the data inside the tunnel.
2. The inner method determines the flow within the tunnel:
  - EAP-MS-CHAPv2 inner method—EAP-MS-CHAPv2 packets travel inside the tunnel without their headers. The first byte of the header contains the type field. EAP-MS-CHAPv2 inner methods support the change-password feature. You can configure the number of times that the user can attempt to change the password through the Admin portal. User authentication attempts are limited by this number.
  - EAP-GTC inner method—Both PEAPv0 and PEAPv1 support the EAP-GTC inner method. The supported supplicants do not support PEAPv0 with the EAP-GTC inner method. EAP-GTC supports the change-password feature. You can configure the number of times that the user can attempt to change the password through the Admin portal. User authentication attempts are limited by this number.
  - EAP-TLS inner method—The Windows built-in supplicant does not support fragmentation of messages after the tunnel is established, and this affects the EAP-TLS inner method. Cisco ISE does not support fragmentation of the outer PEAP message after the tunnel is established. During tunnel establishment, fragmentation works as specified in PEAP documentation. In PEAPv0, EAP-TLS packet headers are removed, and in PEAPv1, EAP-TLS packets are transmitted unchanged.
  - Extensible Authentication Protocol-type, length, value (EAP-TLV) extension—EAP-TLV packets are transmitted unchanged. EAP-TLV packets travel with their headers inside the tunnel.
3. There is protected acknowledgment of success and failure if the conversation has reached the inner method. The client EAP message is always carried in the RADIUS Access-Request message, and the server EAP message is always carried in the RADIUS Access-Challenge message. The EAP-Success message is always carried in the RADIUS Access-Accept message. The EAP-Failure message is always carried in the RADIUS Access-Reject message. Dropping the client PEAP message results in dropping the RADIUS client message.



---

**Note** Cisco ISE requires acknowledgment of the EAP-Success or EAP-Failure message during PEAPv1 communication. The peer must send back a PEAP packet with empty TLS data field to acknowledge the receipt of success or failure message.

---

### *Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling*

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is an authentication protocol that provides mutual authentication and uses a shared secret to establish a tunnel. The tunnel is used to protect weak authentication methods that are based on passwords. The shared secret, referred to as a Protected Access Credentials (PAC) key, is used to mutually authenticate the client and server while securing the tunnel.

#### *Benefits of EAP-FAST*

EAP-FAST provides the following benefits over other authentication protocols:

- Mutual authentication—The EAP server must be able to verify the identity and authenticity of the peer, and the peer must be able to verify the authenticity of the EAP server.
- Immunity to passive dictionary attacks—Many authentication protocols require a password to be explicitly provided, either as cleartext or hashed, by the peer to the EAP server.
- Immunity to man-in-the-middle attacks—In establishing a mutually authenticated protected tunnel, the protocol must prevent adversaries from successfully interjecting information into the conversation between the peer and the EAP server.
- Flexibility to enable support for many different password authentication interfaces such as MS-CHAPv2, Generic Token Card (GTC), and others—EAP-FAST is an extensible framework that allows support of multiple internal protocols by the same server.
- Efficiency—When using wireless media, peers are limited in computational and power resources. EAP-FAST enables the network access communication to be computationally lightweight.
- Minimization of the per-user authentication state requirements of the authentication server—With large deployments, it is typical to have many servers acting as the authentication servers for many peers. It is also highly desirable for a peer to use the same shared secret to secure a tunnel much the same way that it uses the username and password to gain access to the network. EAP-FAST facilitates the use of a single, strong, shared secret by the peer, while enabling servers to minimize the per-user and device state that it must cache and manage.

#### *EAP-FAST Flow*

The EAP-FAST protocol flow is always a combination of the following phases:

1. Provisioning phase—This is phase zero of EAP-FAST. During this phase, the peer is provisioned with a unique, strong secret that is referred to as the PAC that is shared between the Cisco ISE and the peer.
2. Tunnel establishment phase—The client and server authenticate each other by using the PAC to establish a fresh tunnel key. The tunnel key is then used to protect the rest of the conversation and provides message confidentiality and with authenticity.
3. Authentication phase—The authentication is processed inside the tunnel and includes the generation of session keys and protected termination. Cisco ISE supports EAP-FAST versions 1 and 1a.

## 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).
- Choose **Administration > Network Resources > Network Device Profiles**.
  - Click **Add**.
  - Enter a name and description for the network device profile.
  - Select the vendor name from the **Vendor** drop-down list.
  - 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.
  - Expand the **Authentication/Authorization** section to configure the device's default settings for flow types, attribute aliasing, and host lookup.
  - 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.
  - 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**.



**Note** 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).
- Choose **Administration > Network Resources > Network Device Profiles**.
  - Click **Add**.
  - Enter a name and description for the network device profile.
  - 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.
  - Expand the **Authentication/Authorization** section to configure the device's default settings for flow types, attribute aliasing, and host lookup.
  - 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.
  - 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](#).