Manage Authentication Policies

Cisco ISE Authentication Policies

Authentication policies define the protocols that Cisco ISE uses to communicate with the network devices, and the identity sources that it uses for authentication. A policy is a set of conditions and a result. A policy condition consists of an operand (attribute), an operator (equal to, not equal to, greater than, and so on), and a value. Compound conditions are made up of one or more simple conditions that are connected by the AND or OR operator. 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.

An authentication policy consists of the following:

- Network Access Service—This service can be one of the following:
  - An allowed protocols service to choose the protocols to handle the initial request and protocol negotiation.
  - A proxy service that will proxy requests to an external RADIUS server for processing.

- Identity Source—An identity source or an identity source sequence to be used for authentication.

After installation, a default identity authentication policy is available in Cisco ISE that is used for authentications. Any updates to the authentication policy will override the default settings.

Policy Condition Evaluation

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

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

Supported Authentication Protocols

The following is a list of protocols that you can choose while defining your authentication 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)
- Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)

Supported Authentication Types and Database

The authentication type is based on the protocols that are chosen. The authentication type is password based, where the authentication is performed against a database with the username and password that is presented in the request.

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.

By default, the identity source that Cisco ISE will look up for user information is the internal users database.

Types of Authentication Failures

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. 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.

Authentication Policy Terminology

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

- Allowed Protocols—Allowed protocols define the set of protocols that Cisco ISE can use to communicate with the device that requests access to the network resources.
- Identity Source—Identity source defines which database Cisco ISE should use for user information. The database could be an internal database or an external identity source, such as Active Directory or LDAP.

You can add a sequence of databases to an identity source sequence and list this sequence as the identity source in your policy. Cisco ISE will search for the credentials in the order in which the databases are listed in this sequence.

- Failover Options—You can define what course of action Cisco ISE should take if the authentication fails, the user is not found, or if the process fails.

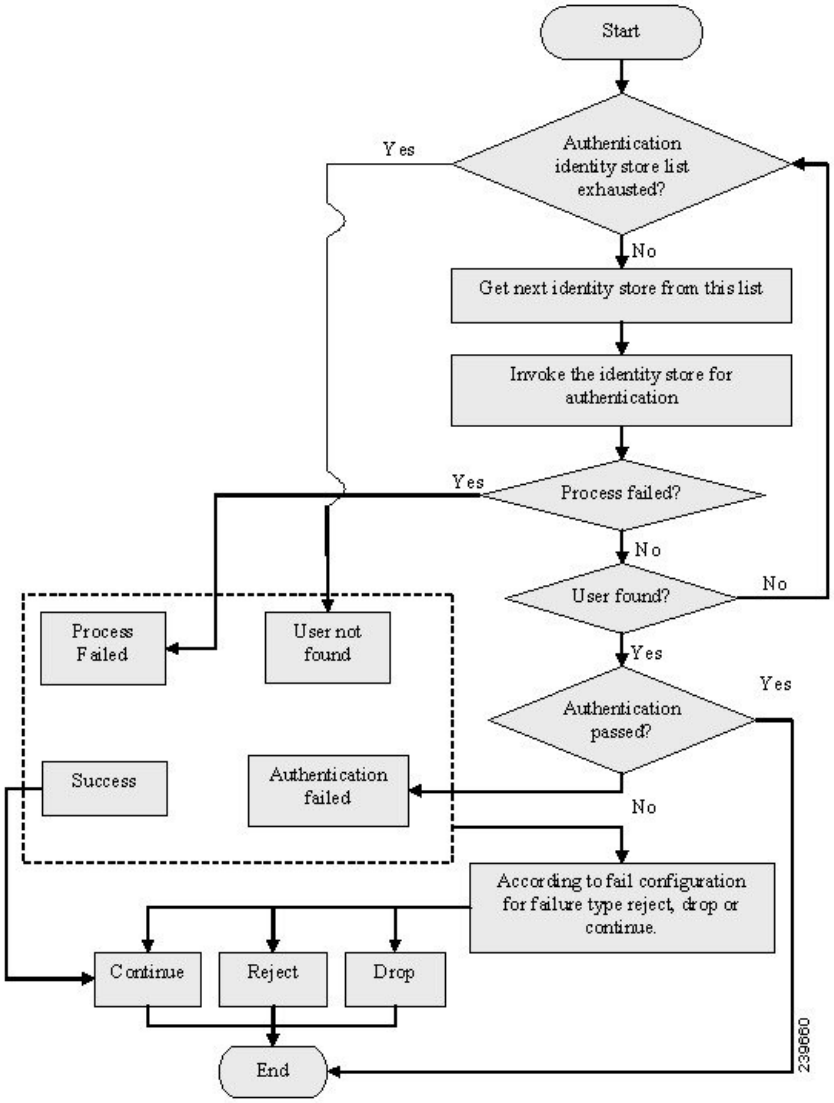
Simple Authentication Policies

A simple authentication policy allows you to statically define the allowed protocols and the identity source or identity source sequence that Cisco ISE should use for communication. You cannot define any condition for simple policies. Cisco ISE assumes that all conditions are met and uses the following definitions to determine the result:

- You can create simple policies in situations where you can statically define the allowed protocols and the identity source that must be used always, and no condition needs to be checked.
- You can also create proxy service-based simple policies. Cisco ISE proxies the request to a policy server to determine which identity source should be used for user authentication. If the request is proxied to a different policy server, the protocol negotiation does not happen. The policy server evaluates which identity source should be used for authentication and returns the response to Cisco ISE.

Simple Authentication Policy Flow

Figure 1: Simple Authentication Policy Flow



The result of a simple policy can be any one of the following:

- Authentication passed
- Authentication failed

An authentication can fail happens due to any of the following reasons:

- Bad credentials or disabled user.
- User not found.
- Authentication process fails.

Guidelines for Configuring Simple Authentication Policies

Follow these guidelines when configuring simple authentication policies:

- If you wish to use the RADIUS server sequence, then you must define this access service before you define the policy.
- If your users are defined in external identity sources, ensure that you have configured these identity sources in Cisco ISE before you define the policy.
- If you want to use an identity source sequence for authenticating users, ensure that you have created the identity source sequence before you define the policy.
- When you switch between simple and rule-based authentication policies, you will lose the policy that you configured earlier. For example, if you configured a simple authentication policy and you want to move to a rule-based authentication policy, you will lose the simple authentication policy. Also, when you move from a rule-based authentication policy to a simple authentication policy, you will lose the rule-based authentication policy.
- Host authentication is performed with the MAC address only (MAB).

Rule-Based Authentication Policies

Rule-based authentication policies consist of attribute-based conditions that determine the allowed protocols and the identity source or identity source sequence to be used for processing the requests. In a simple authentication policy, you can define the allowed protocols and identity source statically. In a rule-based policy, you can define conditions that allows Cisco ISE to dynamically choose the allowed protocols and identity sources. 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, reusable policy elements that can be referred from other rule-based policies. You can also create conditions from within the policy creation page. The two types of conditions are:

- Simple condition
- Compound condition

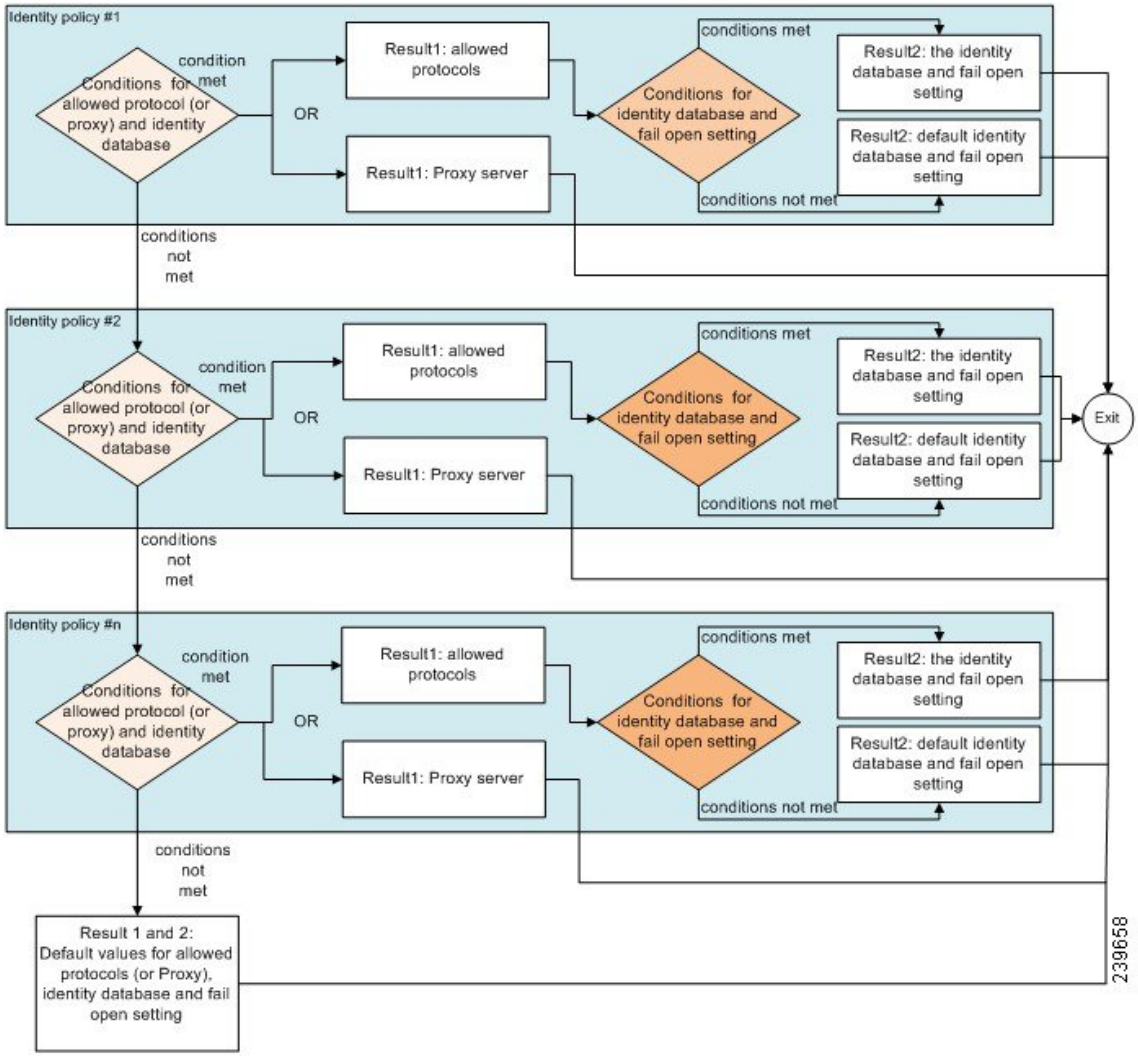
Rule-Based Authentication Policy Flow

In rule-based policies, you can define multiple rules. The identity database is selected based on the first rule that matches the criteria.

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

We recommend that you use only three, or at most four databases in an identity source sequence.

Figure 2: Rule-Based Authentication Policy Flow



Supported Dictionaries for Rule-Based Authentication Policies

Cisco ISE supports the following dictionaries:

- System-defined dictionaries
  - CERTIFICATE
  - DEVICE
  - RADIUS
- RADIUS vendor dictionaries

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft
- Network access

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

Dictionary	Attributes	Allowed Protocol Rules and Proxy	Identity Rules
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		

Dictionary	Attributes	Allowed Protocol Rules and Proxy	Identity Rules
	Issuer - Domain Component		
	Issuer - User ID		

Protocol Settings for Authentication

You must define global protocol settings in Cisco ISE before you can use these protocols to process an authentication request. 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.

Guidelines for Using EAP-FAST as Authentication 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.

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 master 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**.

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.

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.

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.

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.

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.

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 an Allowed Protocol service based on the type of MAC authentication used by the non-Cisco device (PAP, CHAP, or EAP-MD5).

a) Choose **Policy** > **Policy Elements** > **Results** > **Authentication** > **Allowed Protocols**
b) Enter a name for the Allowed Protocol service. For example, MAB for NonCisco Devices.
c) Select the protocol based on the MAC authentication type used by the non-Cisco device:

- PAP—Check the Allow PAP/ASCII check box and check the Detect PAP as Host Lookup check box.
- CHAP—Check the Allow CHAP check box and check the Detect CHAP as Host Lookup check box.
- EAP-MD5—Check the Allow EAP-MD5 check box and check Detect EAP-MD5 as Host Lookup check box.

For each of the protocol listed above, it is recommended to check the following check boxes:

- Check Password—Enable this for checking of the trivial MAB password to authenticate the sending network device.
- Check Calling-Station-Id equals MAC address—Enable this as an extra security check, when Calling-Station-Id is being sent.

Step 3 Configure an authentication policy rule for enabling MAB from non-Cisco devices.

a) Choose **Policy** > **Authentication**.
b) Select the Rule-Based authentication policy.
c) Insert a new rule for MAB.
d) Select the Allowed Protocol service (MAB for NonCisco Devices) that you created in Step 2 in this rule.
e) Select the Internal Endpoints database as the Identity Source in this rule.
f) Save the authentication policy.

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 an Allowed Protocol service based on the type of MAC authentication used by the Cisco device (PAP, CHAP, or EAP-MD5).

a) Choose **Policy** > **Policy Elements** > **Results** > **Authentication** > **Allowed Protocols**

b) Enter a name for the Allowed Protocol service. For example, MAB for Cisco Devices.
c) Check the Process Host Lookup check box.
d) Select the protocol based on the MAC authentication type used by the Cisco device:

- PAP—Check the Allow PAP/ASCII check box and check the Detect PAP as Host Lookup check box.
- CHAP—Check the Allow CHAP check box and check the Detect CHAP as Host Lookup check box.
- EAP-MD5—Check the Allow EAP-MD5 check box and check Detect EAP-MD5 as Host Lookup check box.

For each of the protocol listed above, it is recommended to check the following check boxes:

- Check Password—Enable this for checking of the trivial MAB password to authenticate the sending network device.
- Check Calling-Station-Id equals MAC address—Enable this as an extra security check, when Calling-Station-Id is being sent.

e) Save the Allowed Protocol service.

Step 3 Configure an authentication policy rule for enabling MAB from Cisco devices.

a) Choose **Policy** > **Authentication**.
b) Select the Rule-Based authentication policy.
c) Insert a new rule for MAB.
d) Select the Allowed Protocol service (MAB for Cisco Devices) that you created in Step 2 in this rule.
e) Select the Internal Endpoints database as the Identity Source in this rule.
f) Save the authentication policy.

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.

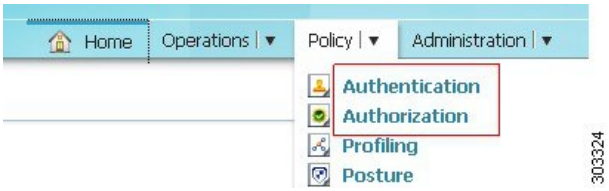
Step 4 Click **Submit** to save the RADIUS server sequence to be used in policies.

Policy Modes

Cisco ISE provides two types of policy modes, the Simple mode and the Policy Set mode. You can select either one of these to configure authentication and authorization policies. When you change the policy mode, you are prompted to login again to the Cisco ISE interface. If you switch from the Policy Set mode to the Simple mode, all the policy set data is deleted except the default policy. The Policy menu options change based on the policy mode selection.

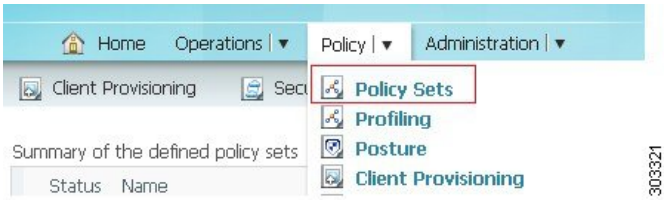
- Simple Mode—If you select Simple mode, you can define authentication and authorization policies separately in the Policy menu.

Figure 3: Simple Mode Policy Menu



- Policy Set Mode—If you select Policy Set mode, you can create policy sets and logically group authentication and authorization within the same group. You can have several groups based on what you need.

Figure 4: Policy Set Mode Policy Menu



Change Policy Modes

The following are the guidelines for changing policy modes:

- After you do a fresh install or upgrade from Cisco ISE, Release 1.1, the Simple Mode policy model is selected by default.
- If you choose to switch to Policy Set Mode from Simple Mode, the authentication and authorization policies are migrated to the default policy set.

- If you choose to switch to Simple Mode from Policy Set Mode, the authentication and authorization of the default policy set are migrated to be the authentication and authorization policies. All other policy set policies are deleted.

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

Step 2 Enable or Disable the Policy Set mode.

Step 3 Click **Save**.
You will be prompted to login again, for the new policy mode to come into effect.

Configure a Simple Authentication Policy

The procedure for configuring a simple authentication policy includes defining an allowed protocols service and configuring a simple authentication policy.

Before You Begin

- To configure a simple authentication policy using the RADIUS server sequence, you should have a basic understanding of the Cisco ISE authentication policies and proxy service to understand authentication types and the protocols that are supported by various databases.
- You should have defined an allowed protocol access service or RADIUS server sequence.
- To perform the following task, you must be a Super Admin or System Admin.

You can also use this process to configure a simple policy using RADIUS server sequence.

Step 1 Choose **Policy** > **Authentication**.

Step 2 Click **OK** on the message that appears.

Step 3 Enter the values as required.

Step 4 Click **Save** to save your simple authentication policy.

Configure a Rule-Based Authentication Policy

In a rule-based policy, you can define conditions that allows Cisco ISE to dynamically choose the allowed protocols and identity sources. You can define one or more conditions using any of the attributes from the Cisco ISE dictionary.

Tip We recommend that you create the allowed protocol access services, conditions, and identity source sequences before you create the rule-based authentication policy. If you want to use the RADIUS server sequence, you can define the RADIUS server sequence before you create the policy.

Before You Begin

- You should have a basic understanding of the rule-based authentication policies, defined allowed protocols for network access, created identity source sequence, and RADIUS server sequence (if you want to use the RADIUS server sequence in place of the allowed protocol access service).
- Cisco ISE comes with predefined rule-based authentication policies for the Wired 802.1X, Wireless 802.1X, and Wired MAB use cases.
- To perform the following task, you must be a Super Admin or System Admin.
- If your users are defined in external identity sources, ensure that you have configured these identity sources in Cisco ISE.

Note When you switch between a simple and a rule-based authentication policy, you will lose the policy that you configured earlier. For example, if you have a simple authentication policy configured and you want to move to a rule-based authentication policy, you will lose the simple authentication policy. Also, when you move from a rule-based authentication policy to a simple authentication policy, you will lose the rule-based authentication policy.

Step 1 Choose **Policy** > **Authentication**.

Step 2 Click the **Rule-Based** radio button.

Step 3 Click OK on the message that appears.

Step 4 Click the action icon and click **Insert new row above** or **Insert new row below** based on where you want the new policy to appear in this list. The policies will be evaluated sequentially.
Each row in this rule-based policy page is equivalent to the simple authentication policy. Each row contains a set of conditions that determine the allowed protocols and identity sources.

Step 5 Enter the values as required to create a new authentication policy.

Step 6 Click **Save** to save your rule-based authentication policies.
You cannot specify the “UserName” attribute when configuring an authentication policy when the EAP-FAST client certificate is sent in the outer TLS negotiation. Cisco recommends using certificate fields like “CN” and “SAN,” for example.

ISE does not restrict a user or machine EAP-TLS authentication against Active Directory when the account in Active Directory is set to deny the user or machine using logon hours, locked-out, or workstations attributes. You should not use these attributes to restrict a user or machine for EAP-TLS authentications.

Default Authentication Policy

The last row in the authentications policy page is the default policy that will be applied if none of the rules match the request. You can edit the allowed protocols and identity source selection for the default policy.

It is a good practice to choose Deny Access as the identity source in the default policy if the request does not match any of the other policies that you have defined.

Policy Sets

Policy 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.

Policy sets are first-match policies. Each policy has a condition that can be a simple or a compound condition, and have the following supported dictionaries:

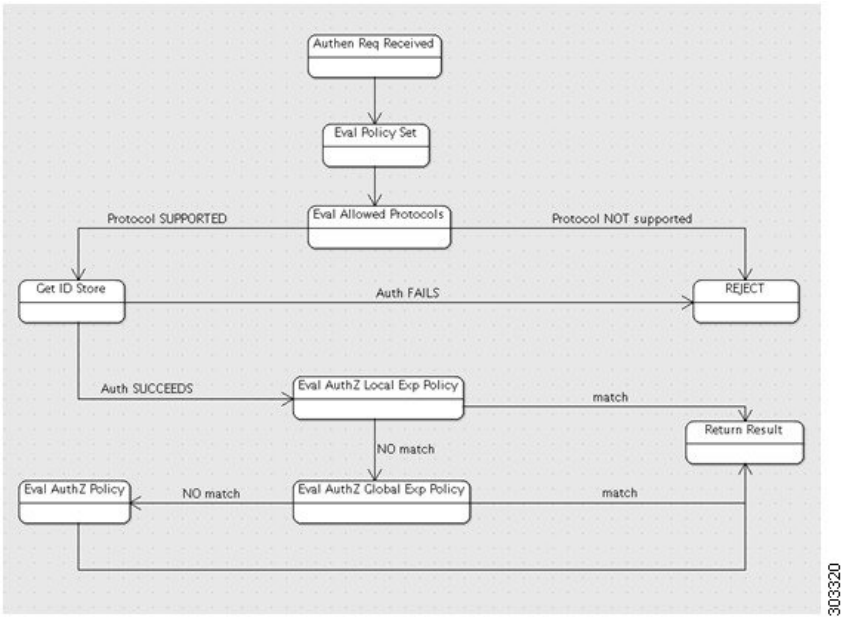
- Airspace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Device, Microsoft
- NetworkAccess
- RADIUS

Once the policy set is matched and selected, its authentication and authorization policies are evaluated. In addition, a global authorization exception policy is available as part of the policy set model.

There is always one policy set defined, which is the default policy set.

Policy Set Evaluation Flow

Figure 5: Policy Set Authentication and Authorization Evaluation Flow



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

1. Evaluate policy set (by evaluating the policy set condition). As a result, one policy set is selected.
2. Evaluate allowed protocols rules of the selected policy set.
3. Evaluate ID store rules of the selected policy set.
4. Evaluate authorization rules of the selected policy set, based on the following paradigm:

   Evaluate the local exception policy in case it is defined

   If no match is found in Step 1 above, evaluate global exception policy if defined

   If no match is found in Step 2 above, evaluate authorization rules

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

Guidelines for Creating Policy Sets

The following are the guidelines for creating policy sets:

- Rules should be specified with names, conditions, and results. You cannot save a policy set as long as all the authentication and authorization rules are not defined.
- You can duplicate rules as long as they are from the same rule type (authentication or authorization) and only from the same policy set.
- Rules cannot be shared by different policy sets; each policy set has its own rule, however conditions can be shared in case you use the condition library.

Global Authorization Exception Policy

The global authorization exception policy allows you to define rules that apply to all policy sets. The global authorization exception policy is added to each authorization policy of all the policy set. Global authorization exception policy can be updated by selecting the Global Exceptions option from the policy set list.

Each authorization policy can have local exception rule, global exception rule, and regular rules. Once you configure the local authorization exception rule, (for some authorization policies) the global exception authorization rules are displayed in read-only mode in conjunction to the local authorization exception rule. The local authorization exception rule can overwrite 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.

Configure Policy Sets

You can use this page to configure Policy sets.

Before You Begin

You should have selected the policy mode as Policy Set to be able to configure Policy sets. To do this, go to **Administration** > **System** > **Settings** > **Policy Sets**.

Step 1 Choose **Policy** > **Policy Sets**.

Step 2 Click the **Default** policy. The default policy is displayed in the right.

Step 3 Click the plus (+) sign on top and choose **Create Above**.

Step 4 Enter the name, description and a condition for this group policy.

Step 5 Define the authentication policy.

Step 6 Define the authorization policy.

Step 7 Click **Submit**. After you configure a policy set, Cisco ISE logs you out. You must log in again to access the Admin portal.

Authentication Policy Built-In Configurations

Cisco ISE is packaged with several default configurations that are part of common use cases.

Table 1: Authentication Policy Configuration Defaults

Name	Path in the User Interface	Description	Additional Information
Default Network Access Allowed Protocols Access Service	Policy > Policy Elements > Configuration > Allowed Protocols	This default is the built-in network access allowed protocols service to be used in authentication policies.	You can use this access service for wired and wireless 802.1X, and wired MAB authentication policies.
Wired 802.1X Compound Condition	Policy > Policy Elements > Conditions > Authentication > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type equals Framed • RADIUS:NAS-Port-Type equals Ethernet	This compound condition is used in the wired 802.1X authentication policy. Any request that matches the criteria specified in this policy would be evaluated based on the wired 802.1X authentication policy.
Wireless 802.1X Compound Condition	Policy > Policy Elements > Conditions > Authentication > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type equals Framed • RADIUS:NAS-Port-Type equals Wireless-IEEE802.11	This compound condition is used in the wireless 802.1X authentication policy. Any request that matches the criteria specified in this policy would be evaluated based on the wireless 802.1X authentication policy.
Wired MAB Compound Condition	Policy > Policy Elements > Conditions > Authentication > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type equals Call-Check • RADIUS:NAS-Port-Type equals Ethernet	This compound condition is used in the wired MAB authentication policy. Any request that matches the criteria specified in this policy would be evaluated based on the wired MAB authentication policy.
Catalyst Switch Local Web Authentication Compound Condition	Policy > Policy Elements > Conditions > Authentication > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type equals Outbound • RADIUS:NAS-Port-Type equals Ethernet	To use this compound condition, you must create an authentication policy that would check for this condition. You can also define an access service based on your requirements or use the default network access allowed protocols service for this policy.

Name	Path in the User Interface	Description	Additional Information
Wireless Lan Controller (WLC) Local Web Authentication Compound Condition	Policy > Policy Elements > Conditions > Authentication > Compound Conditions	This compound condition checks for the following attributes and values: • RADIUS:Service-Type equals Outbound • RADIUS:NAS-Port-Type equals Wireless-IEEE802.11	To use this compound condition, you must create an authentication policy that would check for this condition. You can also define an access service based on your requirements or use the default network access allowed protocols service for this policy.
Wired 802.1X Authentication Policy	Policy > Authentication > Rule-Based	This policy uses the wired 802.1X compound condition and the default network access allowed protocols service. This policy will evaluate requests that match the criteria specified in the wired 802.1X compound condition.	This default policy uses the internal endpoints database as its identity source. You can edit this policy to configure any identity source sequence or identity source based on your needs.
Wireless 802.1X Authentication Policy	Policy > Authentication > Rule-Based	This policy uses the wireless 802.1X compound condition and the default network access allowed protocols service. This policy will evaluate requests that match the criteria specified in the wireless 802.1X compound condition.	This default policy uses the internal endpoints database as its identity source. You can edit this policy to configure any identity source sequence or identity source based on your needs.
Wired MAB Authentication Policy	Policy > Authentication > Rule-Based	This policy uses the wired MAB compound condition and the default network access allowed protocols service. This policy will evaluate requests that match the criteria specified in the wired MAB compound condition.	This default policy uses the internal endpoints database as its identity source.

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 Choose **Operations** > **Authentications** to view real-time authentication summary.

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 that is similar to the one shown in the figure 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 Dashlet

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

The Authentications dashlet provide the following statistical information about the RADIUS 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.

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