CHAPTER 15

Managing Authentication Policies

This chapter describes how network access is granted to users who request access to your network resources. Using the Cisco Identity Services Engine (ISE) user interface, you can define authentication policies that determine who accesses the resources on your network. This chapter contains the following topics:

Understanding Authentication Policies

Authentication policies define the protocols that Cisco ISE should use to communicate with the network devices, and the identity sources that it should use 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 the policy condition and then applies the result that you have defined based on whether the policy evaluation returns a true or a false value.

Note 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.

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 will be available in Cisco ISE that will be used for authentications. Any updates to the authentication policy will override the default settings.

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)

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

This section contains the following topics:

Authentication Type, Protocols, and Databases

The authentication type is based on the protocols that are chosen. Table 5-1 on page 5-1 lists the authentication type and the protocols that are supported by the various databases.

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
  - 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.

If you choose 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 such as authentication failed, user not found, or process failures:

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

Note 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. When authentication fails, it is possible to continue to process the authorization policy for PAP/ASCII, EAP-TLS, or 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

Table 15-1 lists some of the commonly used terms in the authentication policy pages.

Table 15-1 Authentication Policy Terminology

Term	Description
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.

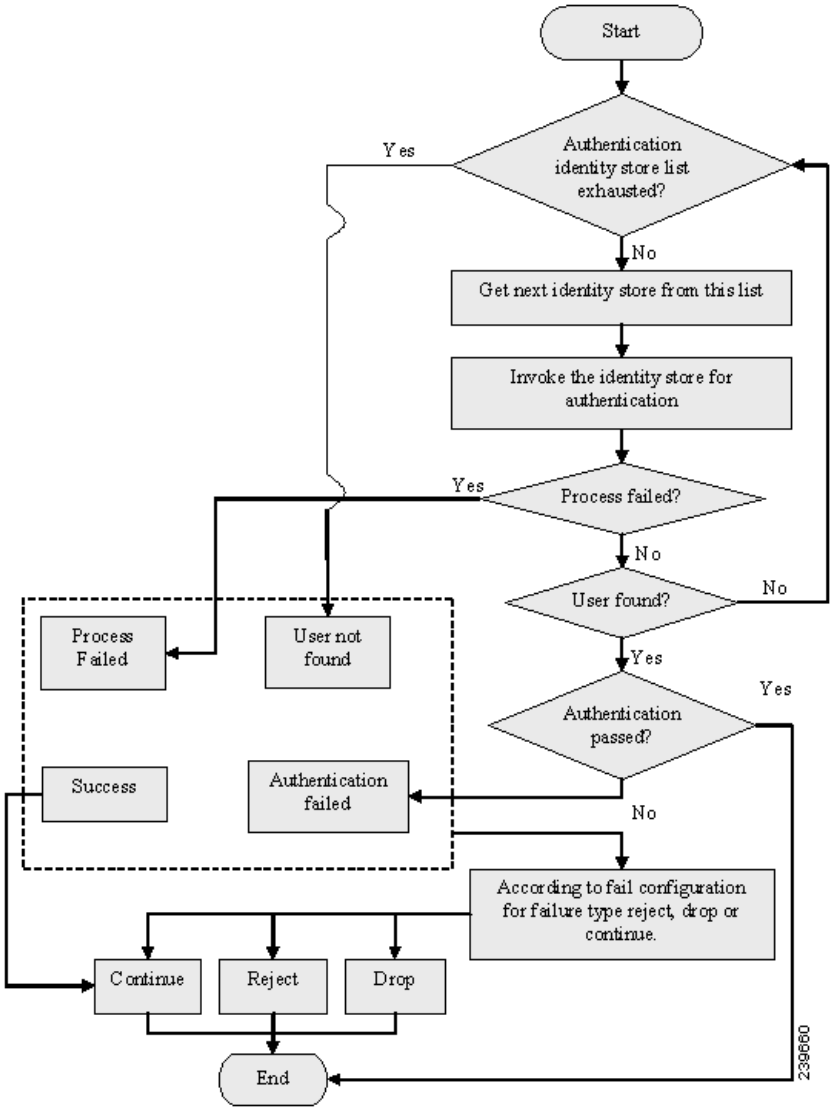
Note Host authentication is performed with the MAC address only (MAB).

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

- Deny access
- Identity database
- Identity sequence

Figure 15-1 shows the simple authentication policy flow.

Figure 15-1 Simple Authentication Policy Flow



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 supports the following dictionaries:

- *Airespace*
- CERTIFICATE

- *Cisco*
- *Cisco-BBSM*
- *Cisco-VPN3000*
- DEVICE
- *Microsoft*
- *Network access*
- RADIUS

where CERTIFICATE, DEVICE, and RADIUS are system-defined dictionaries and *Airespace, Cisco, Cisco-BBSM, Cisco-VPN3000, Microsoft*, and *Network Access* are RADIUS vendor dictionaries.

See the "Dictionaries and Dictionary Attributes" section on page 7-1 for more information on the dictionaries in Cisco ISE.

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. There are two types of conditions:

- Simple condition—A simple condition takes the form *attribute operand value*. These can be saved and reused in other rule-based policies. The simple condition can take the form: A operand B, where A can be any attribute from the ISE dictionary and B can be one of the values that the attribute A can take.

  This is an example of a simple condition: DEVICE:Device Type Equals All Device Types

  See the "Simple Conditions" section on page 15-29 for more information.

- Compound condition—A compound condition is made up of one or more simple conditions with an AND or OR relationship. These are built on top of simple conditions. These can be saved and reused in other rule-based policies. The compound conditions take any one of the following forms:

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

  where X and A are attributes from the ISE dictionary such as username, device type, and so on.

  This is an example of a compound condition: DEVICE:Model Name Matches Catalyst6K AND Network Access:Use Case Equals Host Lookup.

  See the "Compound Conditions" section on page 15-31 for more information.

Table 15-2 lists the fixed attributes that are supported by these dictionaries, which can be used in policy conditions.

Table 15-2 List of Attributes Supported by the Dictionaries

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[1]	ISE Host Name	Yes	Yes
	AuthenticationMethod	No	Yes
	AuthenticationStatus	No	No
	CTSDeviceID	No	No
	Device IP Address	Yes	Yes
	EapAuthentication	No	Yes
	EapTunnel	No	Yes
	Protocol	Yes	Yes
	UseCase	Yes	Yes
	UserName	No	Yes
	WasMachineAuthenticated	No	No

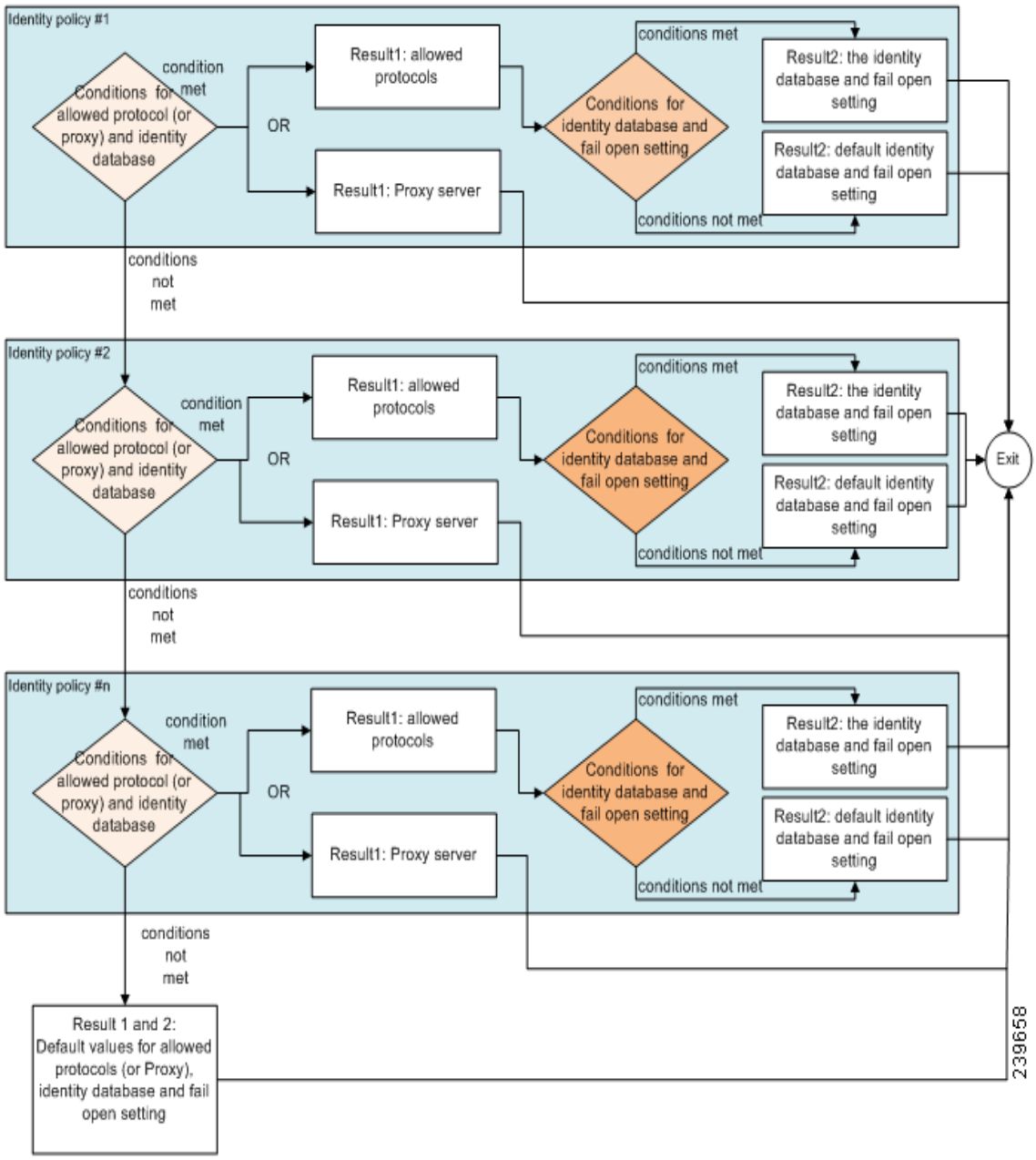
Table 15-2 List of Attributes Supported by the Dictionaries (continued)

Dictionary	Attributes	Allowed Protocol Rules and Proxy	Identity Rules
Certificate	Common Name	No	Yes
	Country		
	Email		
	LocationSubject		
	Organization		
	Organization Unit		
	Serial Number		
	State or Province		
	Subject		
	Subject Alternative Name		
	Subject Alternative Name - DNS		
	Subject Alternative Name - Email		
	Subject Alternative Name - Other Name		
	Subject Serial Number		

1. 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 would only see the following network access attributes: Device IP Address, ISE Host Name, Network Device Name, Protocol, and Use Case.

Figure 15-2 shows the rule-based authentication policy flow.

Figure 15-2 Rule-Based Authentication Policy Flow



In rule-based policies, you can define multiple rules as illustrated in Figure 15-2. 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.

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

Note If you want to switch between the simple and rule-based policies, you must reconfigure the policies because the policy data will no longer be available.

Protocol Settings

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. This section contains the following topics:

Configuring EAP-FAST Settings

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure EAP-FAST settings, complete the following steps:

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

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

Step 3 Choose **EAP-FAST > EAP Fast Settings**.

The EAP-FAST Global Settings page appears.

Step 4 Enter the information as described:

- Authority Identity Info Description—(Required) 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.
- Master Key Generation Period—(Required) Specifies the master 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.

Step 5 Click **Revoke** if you want to revoke all the previously generated master keys and PACs.

Step 6 Click **Save** to save the EAP-FAST settings.

Generating 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.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To generate the PAC for EAP-FAST, complete the following steps:

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.**

The Generate PAC page appears.

Step 4 Enter information as described:

- Tunnel PAC—(Either tunnel PAC or machine PAC is required) Click this radio button to generate a tunnel PAC. This option is the default.
- Machine PAC—Click this radio button to generate a machine PAC.
- Identity—(Required) Specifies the username or machine name presented as the "inner username" by the EAP-FAST protocol. If the identity string does not match that username, authentication will fail.
- PAC Time to Live—(Required) Enter a value in seconds that specifies the expiry 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.
- Password—(Required) Enter a password. The length of the password must be between 8 and 256 characters. The password can contain uppercase or lowercase letters, or numbers, or a combination of alphanumeric characters.

Step 5 Click **Generate PAC** to generate the PAC.

Configuring EAP-TLS Settings

You can configure the runtime characteristics of the EAP-TLS protocol from the Global Options page.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure EAP-TLS settings, complete the following steps:

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

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

Step 3 Choose **EAP-TLS**.

The EAP-TLS settings page appears.

Step 4 Enter the information as described:

- Enable EAP-TLS Session Resume—Check this check box to support an abbreviated reauthentication of a user who has passed full EAP-TLS authentication. This feature provides reauthentication of the user with only a Secure Sockets Layer (SSL) handshake and without applying the certificates. EAP-TLS session resume works only if the EAP-TLS session has not timed out.
- EAP-TLS Session Timeout—Specifies the time in seconds after which the EAP-TLS session times out. The default value is 7200 seconds.

Step 5 Click **Save** to save the EAP-TLS settings.

Configuring PEAP Settings

You can configure the runtime characteristics of the PEAP protocol from the Global Options page.

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure PEAP settings, complete the following steps:

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

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

Step 3 Choose **PEAP**.

The PEAP Settings page appears.

Step 4 Enter the information as described:

- Enable PEAP Session Resume—Check this check box for the Cisco ISE to cache the TLS session that is created during phase one of PEAP authentication, provided the user successfully authenticates in phase two of PEAP. If a user needs to reconnect and the original PEAP session has not timed out, the Cisco ISE uses the cached TLS session, resulting in faster PEAP performance and a reduced AAA server load.

  You must specify a PEAP session timeout value for the PEAP session resume features to work.
- PEAP Session Timeout—Specifies the time in seconds after which the PEAP session times out. The default value is 7200 seconds.
- Enable Fast Reconnect—Check this check box to allow a PEAP session to resume in the Cisco ISE without checking user credentials when the session resume feature is enabled.

Step 5 Click **Save** to save the PEAP 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. These are the two types of network access services that you can use in authentication policies:

- Allowed Protocols Service, page 15-13
- Proxy Service, page 15-20

Allowed Protocols Service

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.

Related Topics

- Defining an Allowed Protocols Service, page 15-14
- Deleting an Allowed Protocol Service, page 15-20
- Configuring the Simple Authentication Policy, page 15-25
- Configuring the Rule-Based Authentication Policy, page 15-28

Defining an Allowed Protocols Service

Prerequisites:

Before you begin this procedure, you should have a basic understanding of the protocol services that are used for authentication. Review the information and the sections noted in the following:

- The Note in Understanding Authentication Policies to understand authentication type and the protocols that are supported by various databases.
- The Allowed Protocols Service and PAC Options sections, 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. See the "Protocol Settings" section on page 15-10 for more information.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To define an allowed protocols service, complete the following steps:

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

Step 2 Click the greater-than sign (>) next to Authentication in the Results navigation pane on the left.

Step 3 Click **Allowed Protocols Services** from the Authentication navigation pane on the left pane.

The Allowed Protocols Services page appears.

Step 4 Click **Add**.

Step 5 Enter the following information:

- Name—(Required) Enter the name of the allowed protocols service.
- Description—Enter an optional description for the allowed protocol service.

Step 6 Select the appropriate Authentication Protocols and options for your network, as described in Table 15-3.

Figure 15-3 shows an example of an allowed protocol selection.

Step 7 If you choose to use PACs, make the appropriate selections, as described in Table 15-4.

Note 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 8 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.

Step 9 You can now create a simple or rule-based authentication policy.

Allowed Protocols Service

Table 15-3 explains the protocol options you specify when Defining an Allowed Protocols Service.

Table 15-3 Allowed Protocols Service

Option	Description
Allowed Protocols	
Process Host Lookup	Check this check box to configure Cisco ISE to process the Host Lookup field (for example, when the RADIUS Service-Type equals 10) and use the System UserName attribute from the RADIUS Calling-Station-ID attribute. 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). **Note** When you want to use the Microsoft Active Directory for MAB authentication, you must uncheck the Process Host Lookup check box from the allowed protocol service that is associated to an authentication policy. You can find the allowed protocol services that you have created in the following location: **Policy > Policy Elements > Results > Authentication > Allowed Protocols > Allowed Protocols Services.**
Authentication Protocols	
Allow PAP/ASCII	This option enables PAP/ASCII. PAP uses cleartext passwords (that is, unencrypted passwords) and is the least secure authentication protocol. When you check the Allow PAP/ASCII check box, you can check the Detect PAP as Host Lookup check box to configure Cisco ISE to detect this type of request as a Host Lookup (instead of PAP) request.
Allow CHAP	This option enables CHAP authentication. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with Microsoft Active Directory.
Allow MS-CHAPv1	This option enables MS-CHAPv1.
Allow MS-CHAPv2	This option enables MS-CHAPv2.
Allow EAP-MD5	This option enables EAP-based MD5 hashed authentication. When you check the Allow EAP-MD5 check box, you can check the Detect EAP-MD5 as Host Lookup check box to configure Cisco ISE to detect this type of request as a Host Lookup (instead of EAP-MD5) request.
Allow EAP-TLS	This option enables the 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. **Note** EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps to configure certificates. Refer to Chapter 12, "Managing Certificates" for more information on certificates.

Table 15-3 Allowed Protocols Service (continued)

Option	Description
Allow LEAP	This option enables Lightweight Extensible Authentication Protocol (LEAP) authentication.
Allow PEAP	This option enables the PEAP authentication protocol and PEAP settings. The default inner method is MS-CHAPv2. When you check the Allow PEAP check box, you can configure the following PEAP inner methods: • Allow EAP-MS-CHAPv2—Check this check box to use EAP-MS-CHAPv2 as the inner method. – Allow Password Change—Check this check box for Cisco ISE to support password changes. – Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1 to 3. • Allow EAP-GTC—Check this check box to use EAP-GTC as the inner method. – Allow Password Change—Check this check box for Cisco ISE to support password changes. – Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1 to 3. • Allow EAP-TLS—Check this check box to use EAP-TLS as the inner method.
Allow EAP-FAST	This option enables the 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. When you check the Allow EAP-FAST check box, you can configure EAP-FAST as the inner method: • Allow EAP-MS-CHAPv2 – Allow Password Change—Check this check box for Cisco ISE to support password changes in phase zero and phase two of EAP-FAST. – Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1-3. • Allow EAP-GTC • Allow Password Change—Check this check box for Cisco ISE to support password changes in phase zero and phase two of EAP-FAST. • Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 1-3. • Use PACs—Choose this option to configure Cisco ISE to provision authorization PACs[1] for EAP-FAST clients. Additional PAC options appear. • Don't use PACs—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. When you choose this option, you can configure Cisco ISE to perform machine authentication.

1. PACs = Protected Access Credentials.

PAC Options

The following table describes the PAC options you can choose from when Defining an Allowed Protocols Service.

Table 15-4 PAC Options

Option	Description
Use PAC	• Tunnel PAC Time to Live—The TTL[1] 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. • Proactive PAC Update When: <n%> 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%. • 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. **Note** To enable anonymous PAC provisioning, you must choose both of the inner methods, EAP-MSCHAPv2 and EAP-GTC. • 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. – 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. • Allow Machine Authentication—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 details are extracted from the PAC and verified in the Cisco ISE external identity source. After these details are correctly verified, no further authentication is performed. **Note** Cisco ISE only supports Active Directory as an external identity source for machine authentication. 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).

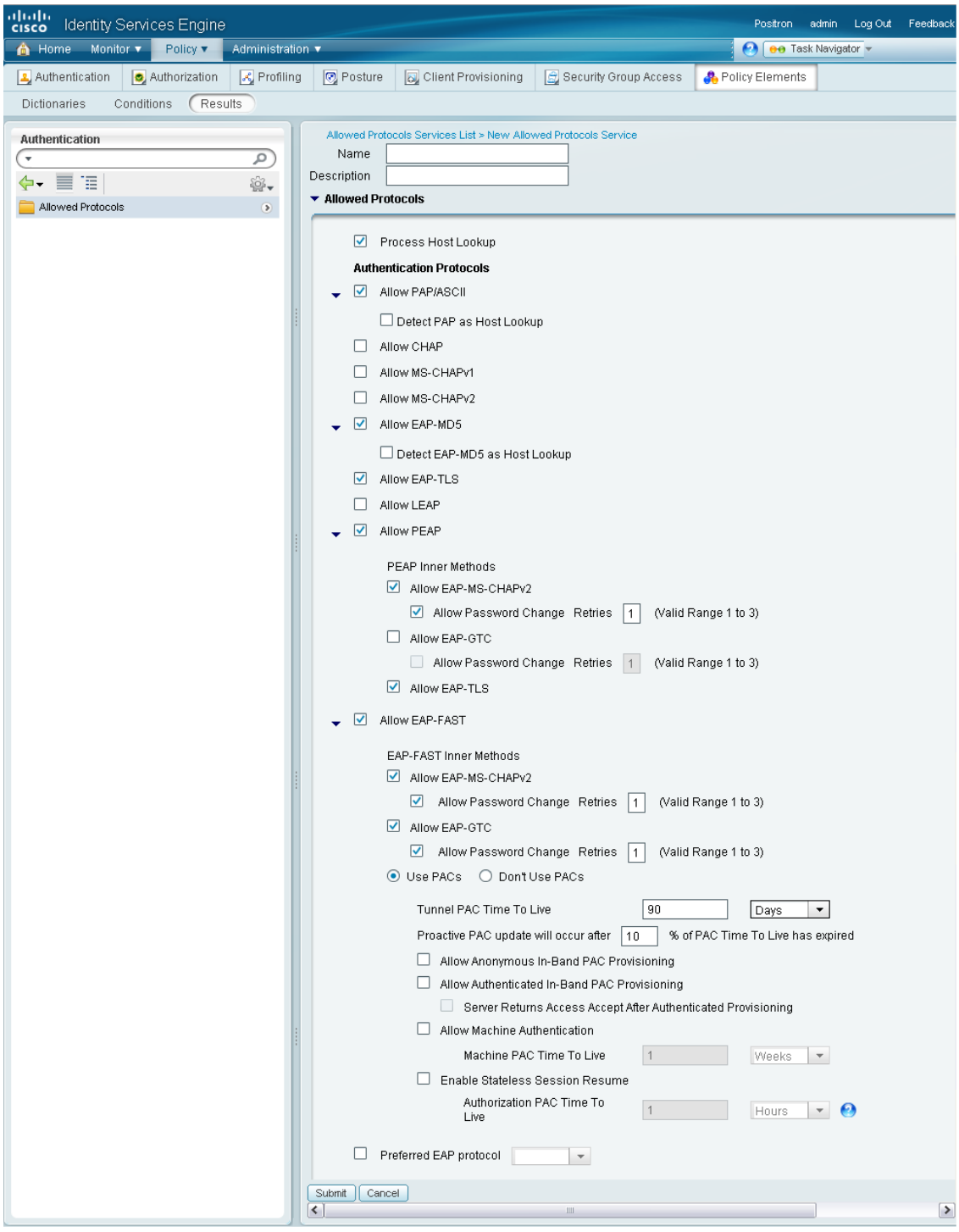
Table 15-4 PAC Options (continued)

Option	Description
	• Enable Stateless Session Resume—Check this check box for Cisco ISE to provision authorization PACs for EAP-FAST clients and always perform phase two of EAP-FAST (default = enabled). Uncheck this check box in the following cases: – If you do not want Cisco ISE to provision authorization PACs for EAP-FAST clients – To always perform phase two of EAP-FAST 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. • Preferred EAP Protocol—Check this check box to choose your preferred EAP protocols from any of the following options: EAP-FAST, PEAP, LEAP, EAP-TLS, and EAP-MD5. By default, LEAP is the preferred protocol to use if you do not enable this field.

1. TTL = Time To Live

Figure 15-3 shows an example of selections made for an allowed protocols service.

Figure 15-3 Allowed Protocols Service



Deleting an Allowed Protocol Service

Prerequisites:

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.
- Ensure that the allowed protocol service that you are about to delete is not referenced in any authentication policies.

To delete an allowed protocol service, complete the following steps:

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

Step 2 Click the greater-than sign (>) next to Authentication in the Results navigation pane on the left.

Step 3 Click **Allowed Protocols Services** from the Authentication navigation pane on the left pane.

The Allowed Protocols Services page appears with a list of allowed protocol services that you have defined.

Step 4 Check the check box next to the allowed protocol service or services that you want to delete, then click **Delete**. Alternatively, you can choose the allowed protocol service from the navigation pane on the left and click **Delete service** from the action icon.

Note If you have chosen more than one allowed protocol service to delete and if one of them is referenced in an authentication policy, then the entire delete operation will fail. Ensure that the allowed protocol services that you want to delete are not referenced in any authentication policies.

Cisco ISE prompts you with the following message:

Are you sure you want to delete?

Step 5 Click **OK** to delete the allowed protocol service or services that you have selected.

Proxy Service

Cisco ISE acts as a RADIUS proxy server by proxying the requests from a network access device (NAD) to a RADIUS server. The RADIUS server processes the request and returns the result to Cisco ISE. Cisco ISE then sends the response to the NAD. In both simple and rule-based authentication policies, you can use the RADIUS server sequences to proxy the requests to a RADIUS server.

Note 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.

To use the RADIUS server sequence for authentication, you should successfully complete the following tasks:

- Defining an External RADIUS Server, page 15-21
- Defining a RADIUS Server Sequence, page 15-24

Defining an External RADIUS Server

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

The 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. This 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.

Note Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To search for RADIUS servers, complete the following steps:

Step 1 Choose **Administration > Network Resources > External RADIUS Servers**.

The External RADIUS Servers page appears.

Step 2 Click **Filter > Advanced Filter** to perform your search. The Filter page appears.

Step 3 You must define whether the search should match any or all of the rules that you define on this page.

Step 4 Enter your search criteria based on the name or description of the RADIUS server, choose an operator, and enter the value.

Step 5 You can do the following:

- To add a filter condition, click the plus sign (+).
- To remove a filter condition, click the minus sign (-).
- To clear all filter conditions, click **Clear Filter**.

Step 6 Click **Go** to perform your search.

You can also save the filter criteria so that it can be used again. Click the **Save** icon to save the filter condition.

Results:

A list of external RADIUS servers that match your search criteria are displayed.

Related Topics

- Creating RADIUS Servers, page 15-22
- Editing RADIUS Servers, page 15-23
- Deleting RADIUS Servers, page 15-23

Creating RADIUS Servers

Prerequisites:

- 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 create the RADIUS server sequence, see the "Defining a RADIUS Server Sequence" section on page 15-24.

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create an external RADIUS server, complete the following steps:

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 described:

- Name—(Required) Enter the name of the external RADIUS server.
- Description—Enter a description of the external RADIUS server.
- Host IP—(Required) Enter the IP address of the external RADIUS server.
- Shared Secret— (Required) Enter the shared secret between Cisco ISE and the external RADIUS server that is used for authenticating the external RADIUS server. A shared secret is an expected string of text that a user must provide to enable the network device to authenticate a username and password. The connection is rejected until the user supplies the shared secret. The shared secret can be up to 128 characters in length.
- Authentication Port—(Required) Enter the RADIUS authentication port number. The valid range is from 1 to 65535. The default is 1812.
- Accounting Port—(Required) Enter the RADIUS accounting port number. The valid range is from 1 to 65535. The default is 1813.
- Server Timeout—(Required) Enter the number of seconds that the Cisco ISE waits for a response from the external RADIUS server. The default is 5 seconds. Valid values are from 5 to 120.
- Connection Attempts—(Required) Enter the number of times that the Cisco ISE attempts to connect to the external RADIUS server. The default is 3 attempts. Valid values are from 1 to 9.

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

Related Topics

- Defining an External RADIUS Server, page 15-21
- Editing RADIUS Servers, page 15-23
- Deleting RADIUS Servers, page 15-23

Editing RADIUS Servers

Prerequisite:

Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To edit an external RADIUS server, complete the following steps:

Step 1 Choose **Administration > Network Resources > External RADIUS Servers**.

The RADIUS Servers page appears with a list of external RADIUS servers.

Step 2 Check the check box next to the RADIUS server that you want to edit and click **Edit**.

Step 3 Modify the values as described in Step 3 of Creating RADIUS Servers.

Step 4 Click **Submit** to save your changes.

Related Topics

- Defining an External RADIUS Server, page 15-21
- Creating RADIUS Servers, page 15-22
- Deleting RADIUS Servers, page 15-23

Deleting RADIUS Servers

Prerequisites:

- You cannot use a RADIUS server by itself. You have to create a RADIUS server sequence and configure it to use the RADIUS server. Before you delete an external RADIUS server, ensure that no RADIUS server sequence uses it.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To delete an external RADIUS server, complete the following steps:

Step 1 Choose **Administration > Network Resources > External RADIUS Servers**.

The RADIUS Servers page appears with a list of external RADIUS servers.

Step 2 Check the check box next to the RADIUS server that you want to delete and click **Delete**.

A dialog box appears with the following message:

Are you sure you want to delete?

Step 3 Click **OK** to delete the RADIUS server.

Defining a RADIUS Server Sequence

RADIUS server sequences in Cisco ISE allow you to proxy requests from a NAD to an external RADIUS server that would process the request and return the result to Cisco ISE, which forwards the response to the NAD. This 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. See "Creating, Editing, and Duplicating RADIUS Server Sequences" procedure on page 15-24 for more information.

Related Topics

- Proxy Service, page 15-20
- Defining an External RADIUS Server, page 15-21

Creating, Editing, and Duplicating RADIUS Server Sequences

Prerequisites:

- Before you begin this procedure, you should have a basic understanding of the Proxy Service and must have successfully completed the task for Defining an External RADIUS Server.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Network Device Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create, edit, or duplicate a RADIUS server sequence, complete the following steps:

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

The RADIUS Server Sequences page appears.

Step 2 Click **Add** to add a RADIUS server sequence, or choose an existing RADIUS server sequence and click **Edit** or **Duplicate** to edit or duplicate an existing sequence.

Step 3 Enter the name of the RADIUS server sequence.

Step 4 Enter an optional description.

Step 5 In the User Selected Service Type area, choose the external RADIUS servers that you want to use as policy servers from the Available list box and move them to the Selected list box.

Step 6 Expand **Advanced Settings**.

Step 7 Enter the following information in the Advanced Settings area:

a. Remote Accounting—Check this check box to enable accounting in the remote policy server.

b. Local Accounting—Check this check box to enable accounting in Cisco ISE.

c. Strip Start of Subject Name up to the First Occurrence of the Separator—Check this check box to strip the username from the prefix. For example, if the subject name is acme\smith and the separator is \, the username becomes smith.

d. Strip End of Subject Name from the Last Occurrence of the Separator—Check this check box 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.

Note You must enable the strip options to extract the username from NetBIOS or User Principle Name (UPN) format usernames (user@domain.com or /domain/user) because only usernames are passed to the RADIUS server for authenticating the user.

Step 8 Click **Submit** to save the RADIUS server sequence to be used in policies.

Next Steps:

1. See the "Configuring a Simple Policy Using RADIUS Server Sequence" section on page 15-27 for information on how to configure a simple authentication policy using the RADIUS server sequence that you created.
2. See the "Configuring the Rule-Based Authentication Policy" section on page 15-28 for information on how to configure a rule-based authentication policy using the RADIUS server sequence that you created.

Configuring the Simple Authentication Policy

The procedure for configuring a simple authentication policy includes defining an allowed protocols service and configuring a simple authentication policy. See the "Defining an Allowed Protocols Service" section on page 15-14 for information on how to create an allowed protocols service.

Note

- If you wish to use the RADIUS server sequence, then you must define this access service before you define the policy. See the "Proxy Service" section on page 15-20 for more information.
- 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. See the "Managing External Identity Sources" section on page 5-1 for information on how to configure the external identity sources.
- 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. See the "Creating Identity Source Sequences" section on page 5-49 for more information.
- 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.

Prerequisites:

- Before you begin this procedure, you should have successfully completed the task for Defining an Allowed Protocols Service.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To define a simple authentication policy, complete the following steps:

Step 1 Choose **Policy > Authentication**.

Step 2 Click the **Simple** radio button.

The following message appears:

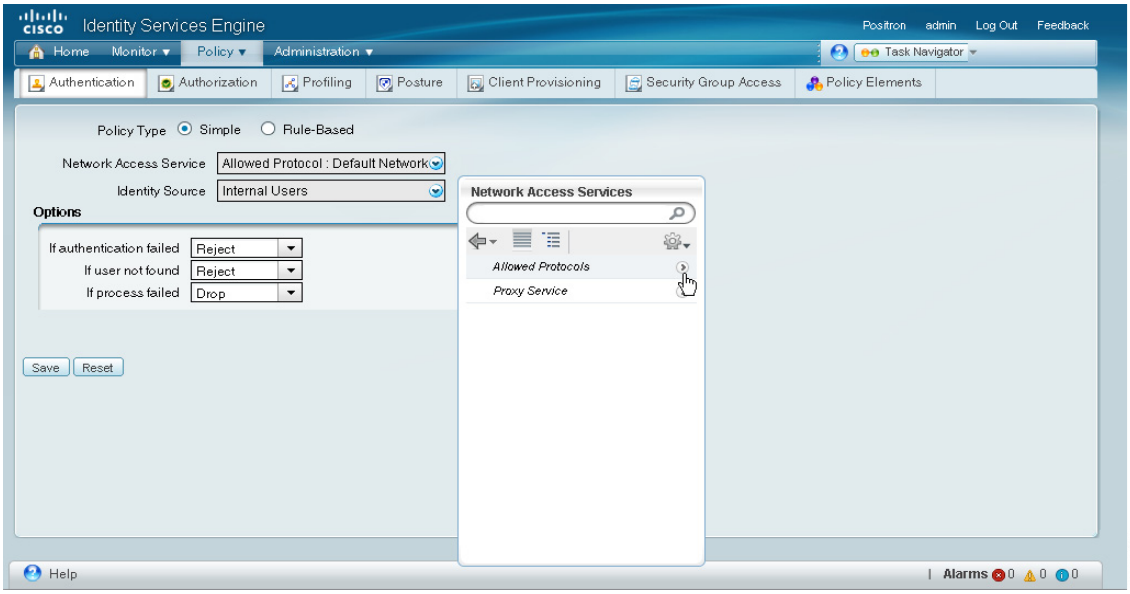
You switched from single to rule-based result selection. Any settings saved in the single mode will be lost when you submit. Click OK to continue.

Step 3 Click **OK** to continue.

Step 4 Choose an allowed protocols service that you have already created from the Network Access Service drop-down menu.

To choose your allowed protocols service, expand the Allowed Protocols service list by clicking the icon as shown in Figure 15-4.

Figure 15-4 Choosing Network Access Service



Step 5 Choose the identity source that you want to use for authentication from the Identity Source drop-down menu.

Note You can also choose an identity source sequence if you have configured it. See the "Creating Identity Source Sequences" section on page 5-49 for information on how to configure identity source sequences.

Step 6 In the Options area, you can define a further course of action for authentication failure, user not found, or process failure events. You can choose one of the following options:

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

Step 7 Click **Save** to save your simple authentication policy.

Related Topics

- Understanding Authentication Policies, page 15-1
- Proxy Service, page 15-20
- Configuring a Simple Policy Using RADIUS Server Sequence, page 15-27

Configuring a Simple Policy Using RADIUS Server Sequence

Prerequisites:

- To configure a simple authentication policy using the RADIUS server sequence, you should have a basic understanding of the Proxy Service and have successfully completed the task for Defining a RADIUS Server Sequence.
- The Note in Understanding Authentication Policies to understand authentication type and the protocols that are supported by various databases.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To configure a simple authentication policy using the RADIUS server sequence, complete the following steps:

Step 1 Choose **Policy > Authentication**.

The Authentication Policy page appears.

Step 2 For the Authentication Method, click the **Simple** radio button.

Step 3 From the Network Access Service drop-down list box, choose the proxy service that you want to use.

Step 4 From the Identity Source drop-down list box, choose the identity database or the identity source sequence that Cisco ISE should use for authentication.

Step 5 In the Options area, you can define a further course of action that Cisco ISE should take if authentication fails, if the user is not found, or if there was a process failure. You can choose any one of the following options:

- Reject—A reject response is sent.
- Drop—No response is sent.
- Continue—Cisco ISE proceeds to evaluate the authorization policy.

Step 6 Click **Save** to save the simple authentication policy.

Result:

You should have a simple authentication policy that is configured using the RADIUS server sequence.

Configuring the Rule-Based Authentication Policy

This section contains:

Understanding the Authentication Policy User Interface Elements

Figure 15-5 shows the rule-based authentication policy page and Table 15-5 describes the rows in this page.

Figure 15-5 Rule-Based Authentication Policy User Interface Elements

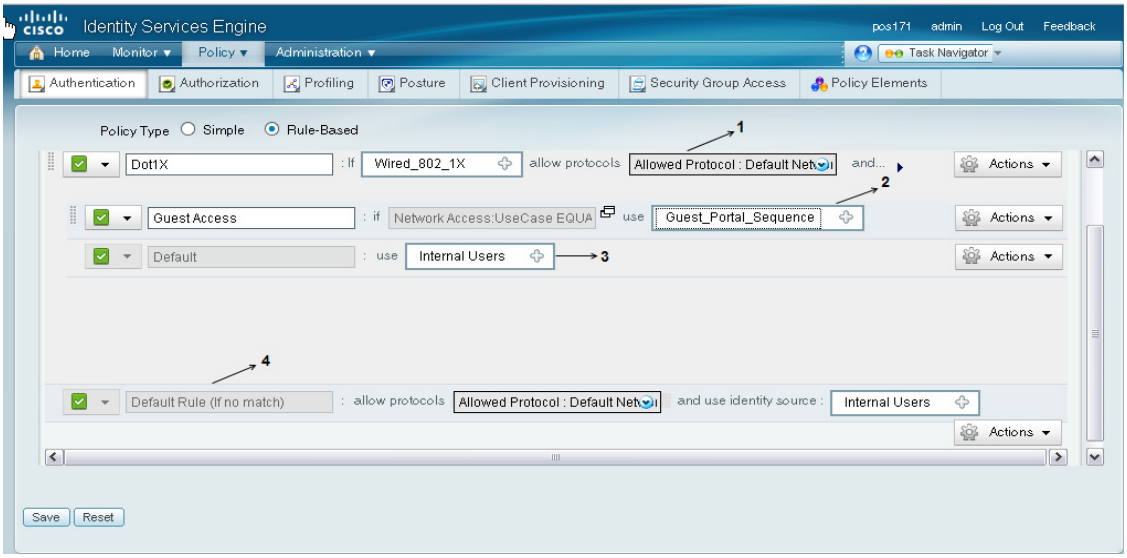


Table 15-5 Rule-Based Authentication Policy User Interface Elements

Callout No.	Description
1	This element is the first rule-based policy. This outer row contains conditions for determining the allowed protocols. You can create more than one outer row, each of which contains conditions for selecting the allowed protocols and identity sources. Each outer row must have one or more inner rows.
2	This element is the inner row, which defines the conditions for identity source selection. This row can contain simple or compound conditions. You can create any number of inner rows, each of which should be based on conditions for selecting identity sources.

Table 15-5 Rule-Based Authentication Policy User Interface Elements (continued)

Callout No.	Description
3	This element is the default identity source that will be used for this policy when the conditions defined for the allowed protocols match those in the request, but the conditions defined for the identity source selection do not match. This row does not have any condition. It contains only the default identity source that Cisco ISE should use if the allowed protocols conditions match, but the identity source selection conditions do not match.
4	This element is the default allowed protocols and identity sources that will be used if none of the policies match the request. This row does not have any condition. It contains only the default allowed protocols and identity source selection that Cisco ISE should use.

This page contains the following fields:

- Status—The status can be one of the following:
  - Enabled—This policy condition is active.
  - Disabled—This policy condition is inactive and will not be evaluated.
  - Monitor Only—This policy condition will be evaluated, but the result will not be enforced. You can use this option for testing purposes. You can view the results of this policy condition in the monitoring and report viewer. 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.
- Name—Name of the condition.
- Conditions—Conditions include the Condition Name or an Expression of type *attribute operand value*. You can create compound conditions using the AND or OR operators at the end of this row. You can create simple and compound conditions under the Policy Elements tab and refer to those conditions in these policies.

For more information:

See Understanding Authentication Policies and Configuring the Rule-Based Authentication Policy for more information.

Simple Conditions

Simple conditions consist of an attribute, an operator, and a value. You can create simple conditions from within the policy pages and also as separate policy elements that can be reused in policies. Cisco ISE allows you to create, edit, and delete simple authentication conditions. This page lists all the simple authentication policy conditions that you have defined in Cisco ISE. See the "Creating Simple Conditions" section on page 15-30 and the "Deleting Simple Conditions" section on page 15-31 for information on how to define simple conditions and delete them, respectively.

Related Topics

- Rule-Based Authentication Policies
- Understanding the Authentication Policy User Interface Elements

Creating Simple Conditions

Prerequisites:

- Before you begin this procedure, you should have a basic understanding of the Rule-Based Authentication Policies, the basic building blocks such as conditions and results, and how they are represented in the GUI. See the "Understanding the Authentication Policy User Interface Elements" section on page 15-28 for more information.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create simple conditions as separate policy elements, complete the following steps:

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

Step 2 From the left navigation pane, click the greater-than sign (>) next to **Authentication**.

Step 3 From the left navigation pane, click **Simple Conditions**.

The Conditions page appears.

Step 4 Click **Add** to add a new condition.

Step 5 Enter the following information:

- Name—Enter the name of the reusable condition.
- Description—Enter an optional description for the condition.
- Attribute—Choose the attribute on which you want to build the condition. Click the drop-down arrow to choose the attribute from the dictionary.
- Operator—Choose the operator from the drop-down list box. This list box is populated only after you choose the attribute.
- Value—Choose a value from the drop-down list box. This list box is populated only after you choose the attribute.

Note For some attributes, you can enter the value.

Step 6 Click **Submit** to save the condition.

You can now use this condition in rule-based policies.

Next Step:

See the "Creating a Rule-Based Authentication Policy" section on page 15-34 for information on how to define a rule-based authentication policy using the simple conditions that you have created.

Deleting Simple Conditions

Prerequisites:

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.
- Ensure that the simple condition or conditions that you are about to delete are not referenced in any authentication policies.

To delete a simple authentication condition, complete the following steps:

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

Step 2 From the left navigation pane, click the greater-than sign (>) next to **Authentication**.

Step 3 From the left navigation pane, click **Simple Conditions**.

The Conditions page appears with a list of simple conditions that you have defined.

Step 4 Check the check box next to the simple condition or conditions that you want to delete, then click **Delete**. Alternatively, you can choose the simple condition that you want to delete from the navigation pane on the left and click **Delete Simple Condition** from the action icon.

Note If you are trying to delete multiple simple conditions at the same time and if one of them is used in any authentication policy, then the entire delete operation will fail.

Cisco ISE prompts you with the following message:

Are you sure you want to delete?

Step 5 Click **OK** to delete the simple condition or conditions.

Compound Conditions

Compound conditions are made up of two or more simple conditions. You can create compound conditions as reusable objects from within the policy creation page or from the Conditions page. This page lists all the compound conditions that you have defined in Cisco ISE. See the "Creating Compound Conditions" section on page 15-32 and "Deleting Compound Conditions" section on page 15-34 for information on how to create compound conditions and delete them.

Related Topics

- Rule-Based Authentication Policies, page 15-5
- Understanding the Authentication Policy User Interface Elements, page 15-28

Creating Compound Conditions

Prerequisites:

- Before you begin this procedure, you should have a basic understanding of the Rule-Based Authentication Policies, the basic building blocks such as conditions and results, and how they are represented in the GUI. See the "Understanding the Authentication Policy User Interface Elements" section on page 15-28 for more information. You can create simple conditions that you can use in compound conditions.
- Cisco ISE comes with predefined compound conditions for some of the most common use cases. See the "Authentication Policy Built-In Configurations" section on page 15-37 for more information on these predefined conditions. You can edit these predefined conditions to suit your requirements.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To create a compound condition from the Conditions page, complete the following steps:

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

Step 2 From the Authentication navigation pane on the left, click **Compound Conditions**.

The Conditions page appears. This page lists any compound conditions that have been defined.

Step 3 Click **Add** to add a new compound condition.

Step 4 Enter a name for the compound condition. You can enter an optional description.

Step 5 Click **Select Existing Condition from Library** to choose an existing simple condition or click **Create New Condition** to choose an attribute, operator, and value from the expression builder.

a. If you have chosen to create a new condition, from the Select Attribute drop-down list box, choose an attribute from the dictionary based on which you want to create a condition.

b. After you have selected an attribute:

- Choose an operator (Equals, Not Equals, Matches, and so on) from the drop-down box.
- Choose the value from the drop-down list box, if available, or enter a value in the text box.
- To save this condition to be reused in other policies, click **Add Condition to Library** from the action icon that appears in the same row.
- Enter a name for this condition in the Condition Name text box and click the ( ) icon.

  The condition is saved as a simple condition and will be available for use in other policies.

Step 6 To add more conditions, click the action icon at the end of this row.

Step 7 Click **Add Attribute/Value** to create a new condition or click **Add Condition from Library** to add an existing simple condition.

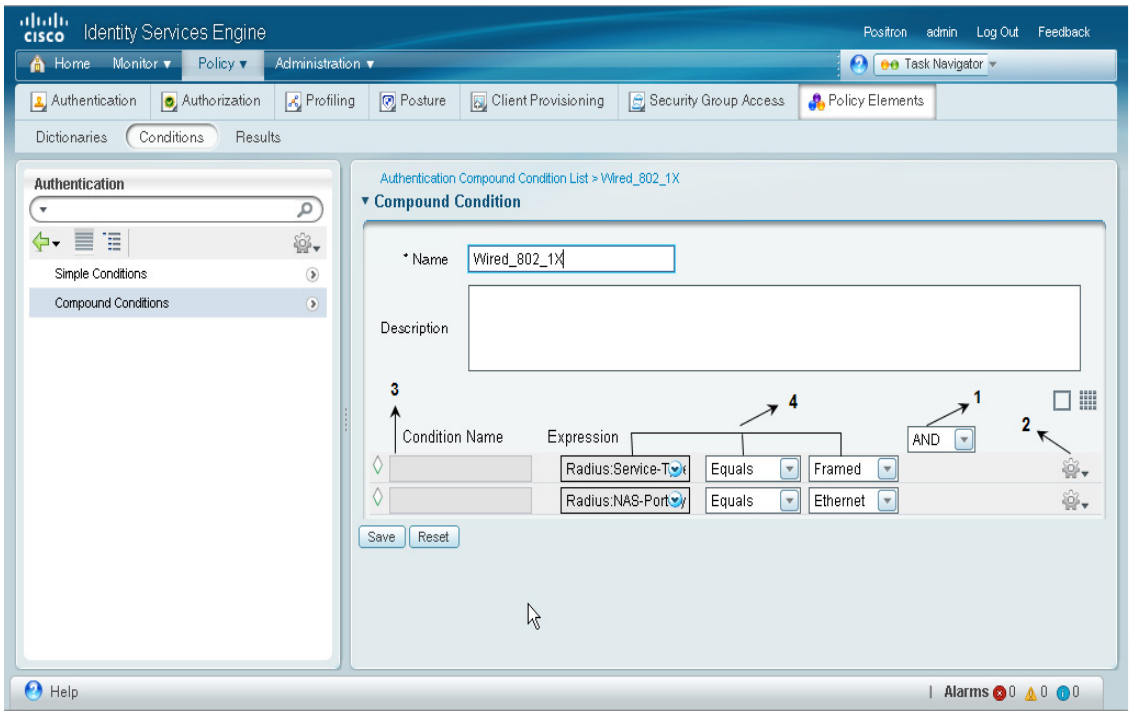
Step 8 Select the operand from the drop-down list box. You can choose either AND or OR and the same operand will be used between all the conditions in this compound condition.

Step 9 Repeat the process from Step 5 to add more conditions.

Step 10 After you have added all the conditions, click **Submit** to create this compound condition.

Figure 15-6 shows a compound conditions page. The table that follows the image provides a description of the user interface elements that appear in this page.

Figure 15-6 Compound Conditions Page



1	This element is the operand to be used between two or more conditions, and can be either AND or OR. For example, compound conditions can be of the following forms: *condition1* AND *condition2* AND *condition3*... or *condition1* OR *condition2* OR *condition3*...
2	You can click the action icon to do the following: • Add new conditions from the library. These are the conditions that you have already created. • Create a condition by adding a new attribute or value. • Duplicate an existing condition. • Add new conditions to the library. • Delete a condition. This option deletes the condition that appears in the same row as the action icon.
3	If you are creating a new condition, you can enter a name here to reuse this condition in other policies. When you provide a name here, this object is created as a separate condition.
4	Choose the attribute based on the reason you want to create the new condition. Choose the operator and the value in the text boxes.

Next Step:

See the "Creating a Rule-Based Authentication Policy" section on page 15-34 for information on how to define a rule-based authentication policy using the compound conditions that you created.

Deleting Compound Conditions

Prerequisites:

- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.
- Ensure that the compound condition or conditions that you are about to delete are not referenced in any authentication policies.

To delete a compound authentication condition, complete the following steps:

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

Step 2 From the left navigation pane, click the greater-than sign (>) next to Authentication.

Step 3 From the left navigation pane, click **Compound Conditions**.

The Conditions page appears with a list of simple conditions that you have defined.

Step 4 Check the check box next to the compound condition or conditions that you want to delete, then click **Delete**. Alternatively, you can choose the compound condition that you want to delete from the navigation pane on the left and click **Delete Compound Condition** from the action icon.

Note If you are trying to delete multiple compound conditions at the same time and if one of them is used in any authentication policy, then the entire delete operation will fail.

Cisco ISE prompts you with the following message:

Are you sure you want to delete?

Step 5 Click **OK** to delete the compound condition or conditions.

Creating a Rule-Based Authentication Policy

Timesaver 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. See the "Proxy Service" section on page 15-20 for more information.

Prerequisites:

- Before you begin this task, you should have a basic understanding of the "Rule-Based Authentication Policies" section on page 15-5, have read the "Understanding the Authentication Policy User Interface Elements" section on page 15-28, and have completed the following tasks successfully:
  - Defining an Allowed Protocols Service
  - Creating Identity Source Sequences if you want to use an identity source sequence
  - Defining a RADIUS Server Sequence if you want to use the RADIUS server sequence in place of the Allowed Protocols access service
- Cisco ISE comes with predefined rule-based authentication policies for the Wired 802.1X, Wireless 802.1X, and Wired MAB use cases. See the "Authentication Policy Built-In Configurations" section on page 15-37 for more information on these predefined policies. You can edit these policies to suit your requirements.
- Every Cisco ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Policy Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

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.

To create a rule-based authentication policy, complete the following steps:

Note If your users are defined in external identity sources, ensure that you have configured these identity sources in Cisco ISE. See Chapter 5, "Managing External Identity Sources" for information on how to configure the external identity sources.

Step 1 Choose **Policy > Authentication**.

The Authentication Policy page appears.

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

The following message appears:

You switched from single to rule-based result selection. Any settings saved in the single mode will be lost when you submit. Click OK to continue.

Step 3 Click **OK** to continue.

This page contains default rule-based policies.

Step 4 To create a new rule-based policy, 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 Click the **Status** drop-down list box to choose the status of this policy. The Status can be any one of the following:

- Enabled
- Disabled
- Monitor Only

Step 6 Enter a name for this policy. By default, it will be named Standard Policy 1, Standard Policy 2, and so on.

Step 7 In the Condition(s) area, click the Expand ( ) button.

Step 8 Click **Select Existing Condition from Library** or **Create New Condition** as described in Creating Compound Conditions.

Step 9 From the Allow Protocols drop-down list box, choose an allowed protocols service or a proxy service.

If you choose a proxy service, Cisco ISE forwards the request to the external policy server that is defined in the proxy service. The external policy server processes the request and returns the result to Cisco ISE. See the "Defining a RADIUS Server Sequence" section on page 15-24 for information on how to create a RADIUS server sequence.

You have created a condition for selecting the allowed protocols. You must then create a condition for selecting the identity source.

Step 10 Click ( ) next to the word "and" to define conditions for the identity source selection.

The default identity source rule appears next to the current row, but is indented.

Step 11 From the action icon in the default identity source row that is indented, click **Insert new row above**.

Step 12 Enter a name for your identity source rule.

Step 13 Click the button to define the conditions based on which you want to choose the identity source.

Step 14 Click **Select Existing Condition from Library** or **Create New Condition** as described in Creating Compound Conditions.

Step 15 Click the **Expand** button to choose the identity source sequence or the identity source.

a. Choose the identity source from the Identity Source List box.

b. Choose the action that you want Cisco ISE to take if authentication fails, if the user is not found, or if the process fails.

c. Click the **Collapse** button to complete your selection.

Step 16 Click the action icon in this inner row to add more conditions for identity source selection.

Step 17 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.

Step 18 Click the action icon in the outer row to add more rule-based policies. Repeat the process from Step 5.

Step 19 The last row in this 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.

Note 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.

Step 20 Click **Save** to save your rule-based authentication policies.

For more information:

See the "Understanding Authentication Policies" section on page 15-1.

Authentication Policy Built-In Configurations

The Cisco ISE software comes with several built-in configurations that are part of common use cases. These built-in configurations are called defaults. Table 15-6 describes the defaults that relate to authentication policies.

Table 15-6 Authentication Policy Configuration Defaults

Name	Path in the UI	Description	Additional Information
Default Network Access Allowed Protocols Access Service	Policy > Policy Elements > Configuration > Allowed Protocol Services	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.

Table 15-6 Authentication Policy Configuration Defaults (continued)

Name	Path in the UI	Description	Additional Information
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. See Configuring the Rule-Based Authentication Policy for more information. You can also define an access service based on your requirements or use the default network access allowed protocols service for this policy. SeeNetwork Access Service for more 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. See Configuring the Rule-Based Authentication Policy for more information. You can also define an access service based on your requirements or use the default network access allowed protocols service for this policy. SeeNetwork Access Service for more information.
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.

Table 15-6 Authentication Policy Configuration Defaults (continued)

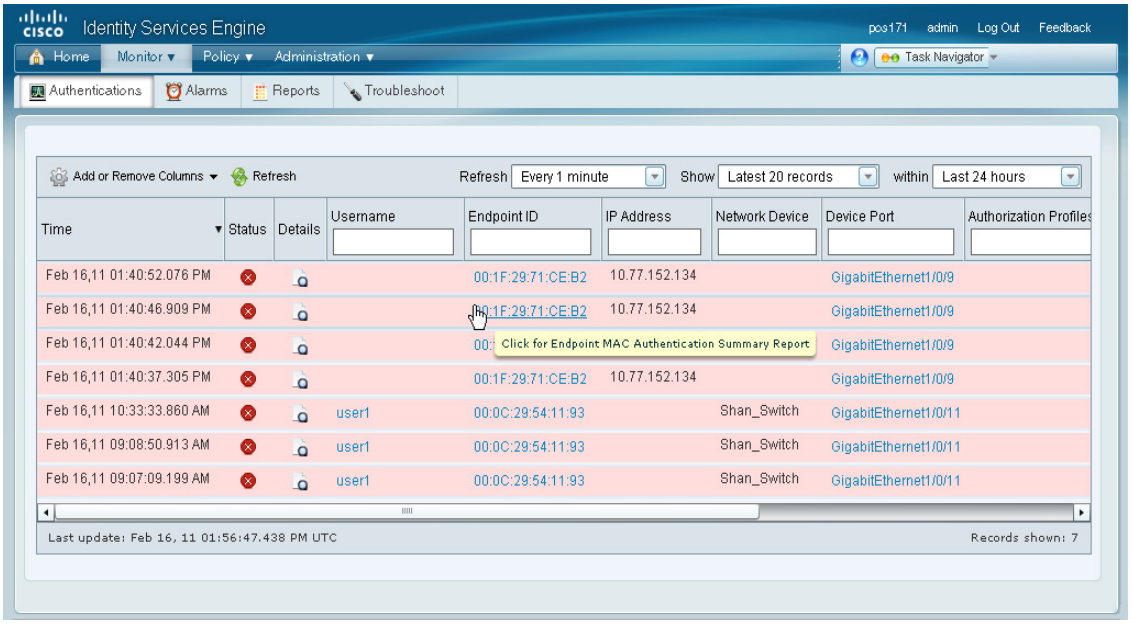
Name	Path in the UI	Description	Additional Information
Wireless 802.1X Authentication Policy	Policy > Authentication > Rule-Based	This policy uses the wireless 802.1X compound condition and the default network access allowed protocols service. This policy will evaluate requests that match the criteria 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.

Viewing Authentication Results

The Cisco ISE dashboard provides a summary of all authentications that take place in your network. To view real-time authentication summary, choose **Monitor > Authentications**. A screen similar to the one shown in Figure 15-7 appears.

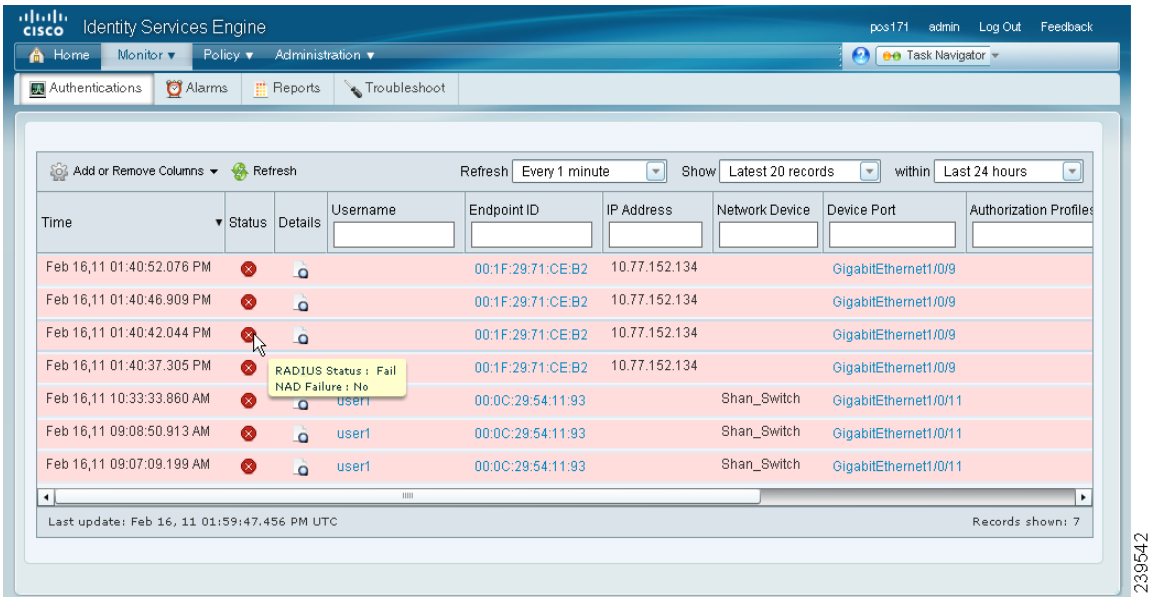
Note Every Cisco ISE administrator account is assigned one or more administrative roles. To view the reports in Cisco ISE, you must have one of the following roles assigned: Super Admin or Helpdesk Admin or Monitoring Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

Figure 15-7 Authentications Screen



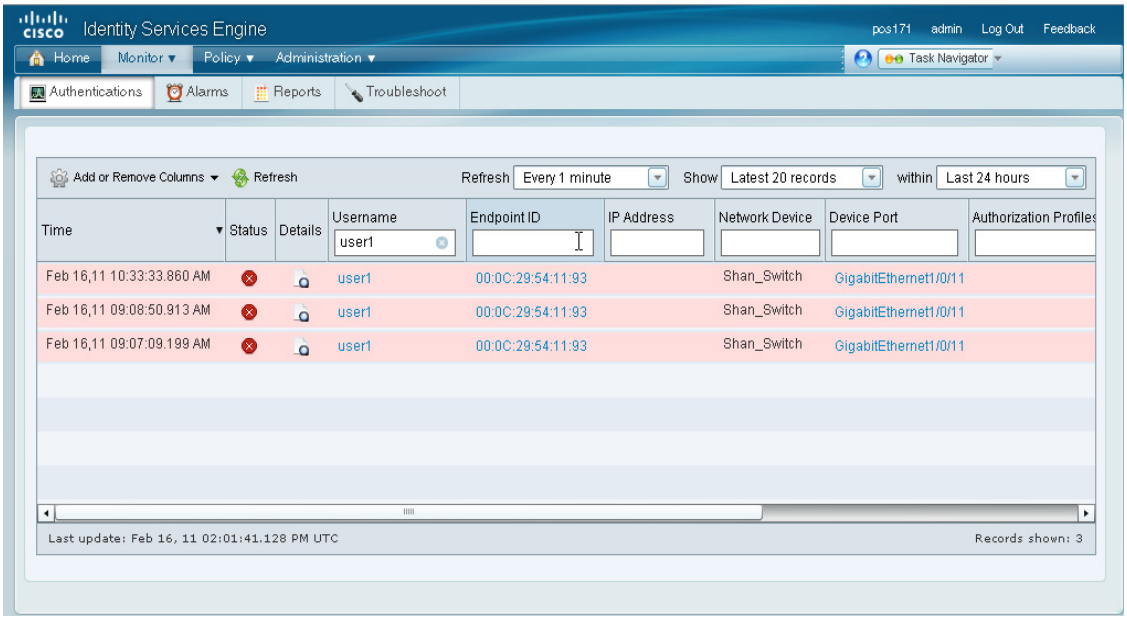
You can move your mouse over the Status icon to view the results of the authentication and a brief summary. A pop-up similar to the one shown in Figure 15-8 appears.

Figure 15-8 Authentication Brief Summary



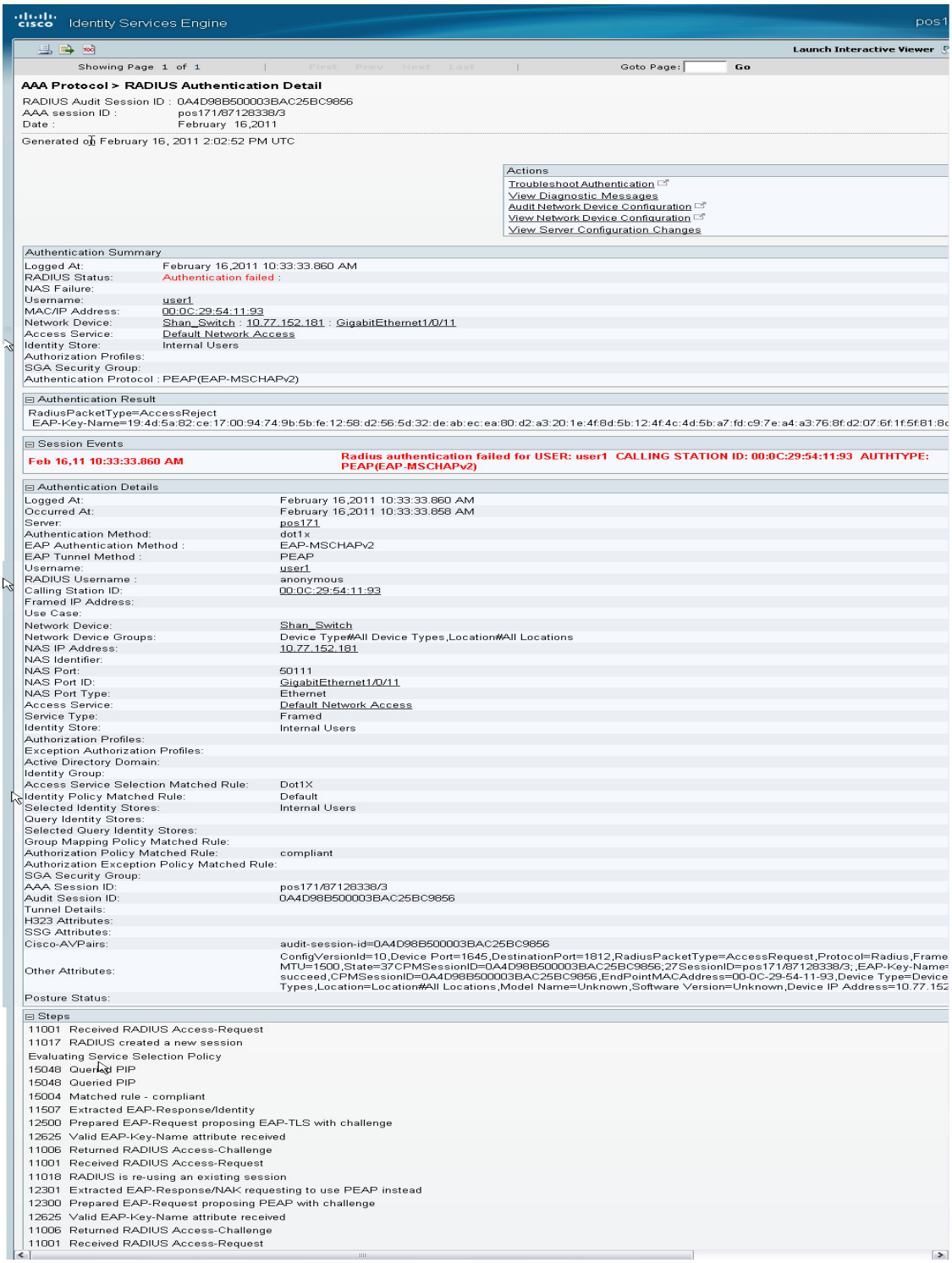
To filter your results, enter your search criteria in any one or more of the text boxes that appear at the top of the list and press **Enter**. A screen similar to the one shown in Figure 15-9 appears.

Figure 15-9 Authentication Screen: Filter View



You can click the magnifier icon under the Details column to view a detailed report as shown in Figure 15-10.

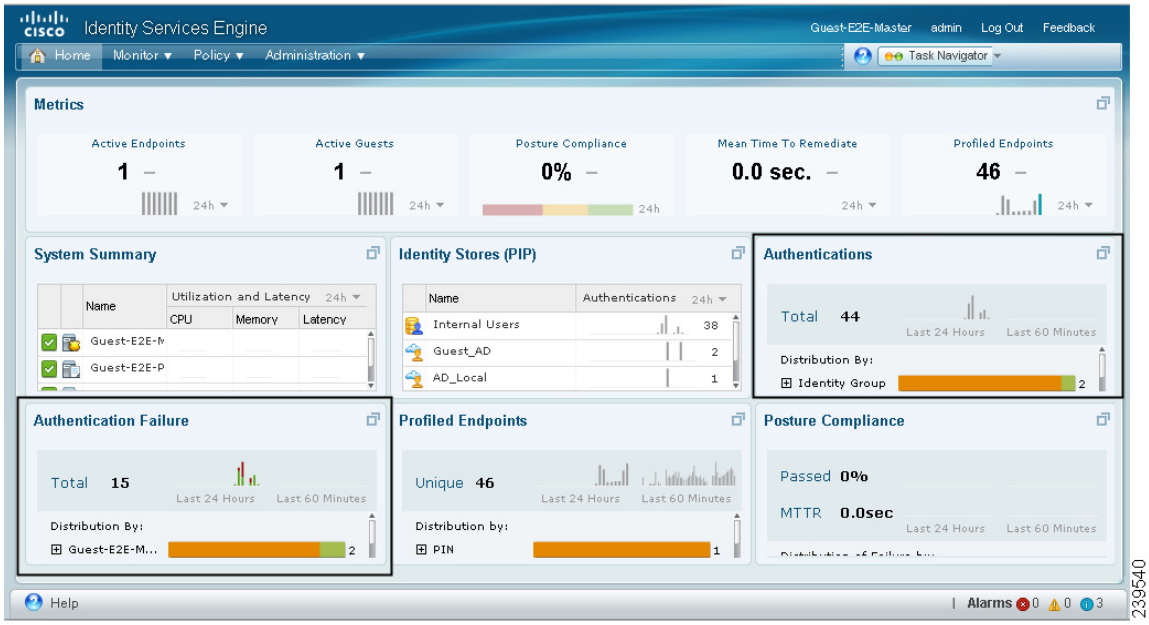
Figure 15-10 Detailed Authentication Summary Report



Cisco ISE also provides at-a-glance information about authentications and authentication failures in the form of dashlets that appear on the Cisco ISE dashboard.

Figure 15-11 shows the Cisco ISE dashboard.

Figure 15-11 Cisco ISE Dashboard



239540

The Authentications and Authentication Failure dashlets provide the following statistical information about the RADIUS authentications that Cisco ISE has handled:

- The total number that appears in the Authentications dashlet is 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 that appears in the Authentication Failure dashlet is the total number of failed RADIUS authentications requests that Cisco ISE has processed.

For information on dashboard and dashlets and how to drill down to look for more information, see Chapter 2, "Introducing the Dashboard" and Chapter 22, "Cisco ISE Dashboard Monitoring."

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

Table 15-7 provides a list of 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.

Table 15-7 List of Reports

Report
AAA Protocol Reports
AAA Diagnostics
Authentication Trend
RADIUS Accounting
RADIUS Authentication

Table 15-7 List of Reports (continued)

Report
Allowed Protocol Reports
Allowed Protocol Authentication Summary
Top *N* Authentications By Allowed Protocol
Server Instance Reports
Server Authentication Summary
Top *N* Authentications By Server
Endpoint Reports
Endpoint MAC Authentication Summary
Top *N* Authentications By Endpoint MAC Address
Top *N* Authentications By Machine
Failure Reason Reports
Authentication Failure Code Lookup
Failure Reason Authentication Summary
Top *N* Authentications By Failure Reason
Network Device Reports
Network Device Authentication Summary
Top *N* Authentications By Network Device
User Reports
Top *N* Authentications By User
User Authentication Summary
Session Directory Reports
RADIUS Active Sessions
RADIUS Session History
RADIUS Terminated Sessions

For more information on how to generate reports and work with the interactive viewer, see Chapter 23, "Reporting."