



System Configuration: Authentication and Certificates

This chapter addresses authentication and certification features found in the System Configuration section of Cisco Secure ACS Solution Engine.

This chapter contains the following topics:

- [About Certification and EAP Protocols, page 10-1](#)
- [Global Authentication Setup, page 10-26](#)
- [Cisco Secure ACS Certificate Setup, page 10-34](#)

About Certification and EAP Protocols

Cisco Secure ACS uses EAP-TLS and PEAP authentication protocols in combination with digital certification to ensure the protection and validity of authentication information. Digital certification, EAP-TLS, PEAP, and machine authentication are described in the topics that follow.

This section contains the following topics:

- [Digital Certificates, page 10-2](#)
- [EAP-TLS Authentication, page 10-2](#)
- [PEAP Authentication, page 10-8](#)
- [EAP-FAST Authentication, page 10-13](#)

Digital Certificates

The ACS Certificate Setup pages enable you to install digital certificates to support EAP-TLS and PEAP authentication, as well as to support HTTPS protocol for secure access to the Cisco Secure ACS HTML interface. Cisco Secure ACS uses the X.509 v3 digital certificate standard. Certificate files must be in either Base64-encoded X.509 format or DER-encoded binary X.509 format. Also, Cisco Secure ACS supports manual certificate enrollment and provides the means for managing a certificate trust list (CTL) and certificate revocation lists (CRL).

Digital certificates do not require the sharing of secrets or stored database credentials. They can be scaled and trusted over large deployments. If managed properly, they can serve as a method of authentication that is stronger and more secure than shared secret systems. Mutual trust requires that Cisco Secure ACS have an installed certificate that can be verified by end-user clients. This server certificate may be issued from a certification authority (CA) or, if you choose, may be a self-signed certificate. For more information see [Installing a Cisco Secure ACS Server Certificate, page 10-35](#), and [Using Self-Signed Certificates, page 10-47](#).

**Note**

Depending on the end-user client involved, the CA certificate for the CA that issued the Cisco Secure ACS server certificate is likely to be required in local storage for trusted root CAs on the end-user client computer.

EAP-TLS Authentication

This section contains the following topics:

- [About the EAP-TLS Protocol, page 10-3](#)
- [EAP-TLS and Cisco Secure ACS, page 10-4](#)
- [EAP-TLS Limitations, page 10-6](#)
- [Enabling EAP-TLS Authentication, page 10-7](#)

About the EAP-TLS Protocol

EAP and TLS are both IETF RFC standards. The EAP protocol carries initial authentication information, specifically EAPOL (the encapsulation of EAP over LANs as established by IEEE 802.1X). TLS uses certificates both for user authentication and for dynamic ephemeral session key generation. The EAP-TLS authentication protocol uses the certificates of Cisco Secure ACS and of the end-user client, enforcing mutual authentication of the client and of Cisco Secure ACS. For more detailed information on EAP, TLS, and EAP-TLS, refer to the following IETF RFCs: [PPP Extensible Authentication Protocol \(EAP\) RFC 2284](#), [The TLS Protocol RFC 2246](#), and [PPP EAP TLS Authentication Protocol RFC 2716](#).

EAP-TLS authentication involves two elements of trust. The first element of trust is when the EAP-TLS negotiation establishes end-user trust by validating, through RSA signature verifications, that the user possesses a keypair signed by a certificate. This verifies that the end user is the legitimate keyholder for a given digital certificate and the corresponding user identification contained in the certificate. However, trusting that a user possesses a certificate only provides a username/keypair binding. The second element of trust is to use a third-party signature, usually from a certification authority (CA), that verifies the information in a certificate. This third-party binding is similar to the real world equivalent of the seal on a passport. You trust the passport because you trust the preparation and identity checking that the particular country's passport office made when creating that passport. You trust digital certificates by installing the root certificate CA signature.

Some situations do not require this “second element of trust” that is provided by installing the root certificate CA signature. When such external validation of certificate legitimacy is not required, you can use the Cisco Secure ACS self-signed certificate capability. Depending on the end-user client involved, the CA certificate for the CA that issued the Cisco Secure ACS server certificate is likely to be required in local storage for trusted root CAs on the end-user client computer. For more information, see [About Self-Signed Certificates, page 10-47](#).

EAP-TLS requires support from both the end client and the AAA client. An example of an EAP-TLS client includes the Microsoft Windows XP operating system; EAP-TLS-compliant AAA clients include Cisco 802.1x-enabled switch platforms (such as the Catalyst 6500 product line) and Cisco Aironet Wireless solutions. To accomplish secure Cisco Aironet connectivity, EAP-TLS generates a dynamic, per-user, per-connection, unique session key.

EAP-TLS and Cisco Secure ACS

Cisco Secure ACS supports EAP-TLS with any end-user client that supports EAP-TLS, such as Windows XP. To learn which user databases support EAP-TLS, see [Authentication Protocol-Database Compatibility, page 1-10](#). For more information about deploying EAP-TLS authentication, see *Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks* at http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/acstl_wp.htm.

Cisco Secure ACS can use EAP-TLS to support machine authentication to Microsoft Windows Active Directory. The end-user client may limit the protocol used for user authentication to the same protocol used for machine authentication; that is, use of EAP-TLS for machine authentication may require the use of EAP-TLS for user authentication. For more information about machine authentication, see [Machine Authentication, page 13-16](#).

Cisco Secure ACS supports domain stripping for EAP-TLS authentication using Windows Active Directory. For more information, see [EAP-TLS Domain Stripping, page 13-16](#).

Cisco Secure ACS also supports three methods of certificate comparison and a session resume feature. This topic discusses these features.

To permit access to the network by a user or computer authenticating with EAP-TLS, Cisco Secure ACS must verify that the claimed identity (presented in the EAP Identity response) corresponds to the certificate presented by the user. Cisco Secure ACS can accomplish this verification in three ways:

- **Certificate SAN Comparison**—Based on the name in the Subject Alternative Name field in the user certificate.
- **Certificate CN Comparison**—Based on the name in the Subject Common Name field in the user certificate.
- **Certificate Binary Comparison**—Based on a binary comparison between the user certificate stored in the user object in the LDAP server or Active Directory and the certificate presented by the user during EAP-TLS authentication. This comparison method cannot be used to authenticate users stored in an ODBC external user database.



Note If you use certificate binary comparison, the user certificate must be stored in a binary format. Also, for generic LDAP and Active Directory, the attribute storing the certificate must be the standard LDAP attribute named “usercertificate”.

When you set up EAP-TLS, you can select the criterion (one, two, or all) that Cisco Secure ACS uses. For more information, see [Configuring Authentication Options, page 10-33](#).

Cisco Secure ACS supports a session resume feature for EAP-TLS-authenticated user sessions, a particularly useful feature for WLANs, wherein a user may move the client computer so that a different wireless access point is in use. When this feature is enabled, Cisco Secure ACS caches the TLS session created during EAP-TLS authentication, provided that the user successfully authenticates. If a user needs to reconnect and the original EAP-TLS session has not timed out, Cisco Secure ACS uses the cached TLS session, resulting in faster EAP-TLS performance and lessened AAA server load. When Cisco Secure ACS resumes an EAP-TLS session, the user reauthenticates by SSL handshake only, without a certificate comparison.

In effect, enabling EAP-TLS session resume allows Cisco Secure ACS to trust a user based on the cached TLS session from the original EAP-TLS authentication. Because Cisco Secure ACS only caches a TLS session when a new EAP-TLS authentication succeeds, the existence of a cached TLS session is proof that the user has successfully authenticated within the number of minutes defined by the EAP-TLS session timeout option.



Note Session timeout is based on the time of the initial, full authentication of the session. It is not dependent upon an accounting start message.

Changes to group assignment in an external user database are not enforced by the session resume feature. This is because group mapping does not occur when a user session is resumed. Instead, the user is mapped to the same Cisco Secure ACS group that the user was mapped to upon the beginning of the session. Upon the start of a new session, group mapping enforces the new group assignment.

To force an EAP-TLS session to end before the session timeout is reached, either restart the CSAuth service or delete the user from the CiscoSecure user database CiscoSecure user database. Disabling or deleting the user in an external user database has no effect because the session resume feature does not involve the use of external user databases.

You can enable the EAP-TLS session resume feature and configure the timeout interval on the Global Authentication Setup page. For more information about enabling this feature, see [Global Authentication Setup, page 10-26](#).

EAP-TLS Limitations

The Cisco Secure ACS implementation of EAP-TLS has the following limitations:

- **Server and CA certificate file format**—If you install the Cisco Secure ACS server and CA certificates from files rather than from certificate storage, server and CA certificate files must be in either Base64-encoded X.509 format or DER-encoded binary X.509 format.
- **LDAP attribute for binary comparison**—If you configure Cisco Secure ACS to perform binary comparison of user certificates, the user certificate must be stored in Active Directory or an LDAP server, using a binary format. Also, the attribute storing the certificate must be named “usercertificate”.
- **Windows server type**—If you want to use Active Directory to authenticate users with EAP-TLS when Cisco Secure ACS runs on a member server, additional configuration is required. For more information, including steps for the additional configuration, see *Installation Guide for Cisco Secure ACS for Windows Server*.

Additionally, if Cisco Secure ACS receives traffic from a wireless access point that has the wrong shared secret, the error message logged in the failed attempts log reads “EAP request has invalid signature”. Three conditions that might cause this to occur are the following:

- The wrong signature is being used.
- A RADIUS packet was corrupted in transit.
- Cisco Secure ACS is being attacked.

Enabling EAP-TLS Authentication

This procedure provides an overview of the detailed procedures required to configure Cisco Secure ACS to support EAP-TLS authentication.

**Note**

End-user client computers must be configured to support EAP-TLS. This procedure is specific to configuration of Cisco Secure ACS only. For more information about deploying EAP-TLS authentication, see *Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks* at http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/acstl_wp.htm.

Before You Begin

For EAP-TLS machine authentication, if you have a Microsoft certification authority server configured on the domain controller, you can configure a policy in Active Directory to produce a client certificate automatically when a computer is added to the domain. For more information, see [Microsoft Knowledge Base Article 313407, HOW TO: Create Automatic Certificate Requests with Group Policy in Windows](#).

To enable EAP-TLS authentication, follow these steps:

-
- Step 1** Install a server certificate in Cisco Secure ACS. EAP-TLS requires a server certificate. For detailed steps, see [Installing a Cisco Secure ACS Server Certificate, page 10-35](#).

**Note**

If you have previously installed a certificate to support EAP-TLS or PEAP user authentication or to support HTTPS protection of remote Cisco Secure ACS administration, you do not need to perform this step. A single server certificate is sufficient to support all certificate-based Cisco Secure ACS services and remote administration; however, EAP-TLS and PEAP require that the certificate be suitable for server authentication purposes.

- Step 2** Edit the certification trust list so that the certification authority (CA) issuing end-user client certificates is trusted. If you do not perform this step, Cisco Secure ACS only trusts user certificates issued by the same CA that issued the certificate installed in Cisco Secure ACS. For detailed steps, see [Editing the Certificate Trust List, page 10-38](#).
- Step 3** Establish a certificate revocation list (CRL) for each CA and certificate type listed in the certificate trust list (CTL). As part of EAP-TLS authentication, Cisco Secure ACS validates the status of the certificate presented by the user against the cached CRL to ensure that it has not been revoked. For detailed steps, see [Adding a Certificate Revocation List Issuer, page 10-42](#).
- Step 4** Enable EAP-TLS on the Global Authentication Setup page. Cisco Secure ACS allows you to complete this step only after you have successfully completed Step 1. For detailed steps, see [Configuring Authentication Options, page 10-33](#).
- Step 5** Configure a user database. To determine which user databases support EAP-TLS authentication, see [Authentication Protocol-Database Compatibility, page 1-10](#). Cisco Secure ACS is ready to perform EAP-TLS authentication.
-

PEAP Authentication

This section contains the following topics:

- [About the PEAP Protocol, page 10-8](#)
- [PEAP and Cisco Secure ACS, page 10-9](#)
- [PEAP and the Unknown User Policy, page 10-11](#)
- [Enabling PEAP Authentication, page 10-12](#)

About the PEAP Protocol

The PEAP (Protected EAP) protocol is a client-server security architecture that provides a means of encrypting EAP transactions, thereby protecting the contents of EAP authentications. PEAP has been posted as an IETF Internet Draft by RSA, Cisco, and Microsoft and is available at <http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-05.txt>.

PEAP authentications always involve two phases. In the first phase, the end-user client authenticates Cisco Secure ACS. This requires a server certificate and authenticates Cisco Secure ACS to the end-user client, ensuring that the user or machine credentials sent in phase two are sent to a AAA server that has a certificate issued by a trusted CA. The first phase uses a TLS handshake to establish an SSL tunnel.

**Note**

Depending on the end-user client involved, the CA certificate for the CA that issued the Cisco Secure ACS server certificate is likely to be required in local storage for trusted root CAs on the end-user client computer.

In phase two, Cisco Secure ACS authenticates the user or machine credentials using an EAP authentication protocol. The EAP authentication is protected by the SSL tunnel created in phase one. The authentication type negotiated during the second conversation may be any valid EAP type, such as EAP-GTC (for Generic Token Card). Because PEAP can support any EAP authentication protocol, individual combinations of PEAP and EAP protocols are denoted with the EAP protocol within parentheses, such as PEAP(EAP-GTC). For the authentication protocols that Cisco Secure ACS supports in phase two of PEAP, see [Authentication Protocol-Database Compatibility, page 1-10](#).

One improvement in security offered by PEAP is identity protection. This is the potential of protecting the username in all PEAP transactions. After phase one of PEAP, all data is encrypted, including username information usually sent in clear text. The Cisco Aironet PEAP client sends user identity through the SSL tunnel only. The initial identity, used in phase one and which is sent in the clear, is the MAC address of the end-user client with “PEAP_” as a prefix. The Microsoft PEAP client does not provide identity protection; the Microsoft PEAP client sends the username in the clear in phase one of PEAP authentication.

PEAP and Cisco Secure ACS

Cisco Secure ACS supports PEAP authentication using either the Cisco Aironet PEAP client or the Microsoft PEAP client included with Microsoft Windows XP Service Pack 1. Cisco Secure ACS can support the Cisco Aironet PEAP client with PEAP(EAP-GTC) only. For the Microsoft PEAP client included with Windows XP Service Pack 1, Cisco Secure ACS supports only PEAP(EAP-MSCHAPv2). For information about which user databases support PEAP protocols, see [Authentication Protocol-Database Compatibility, page 1-10](#).

When the end-user client is the Cisco Aironet PEAP client and both PEAP(EAP-GTC) and PEAP(EAP-MSCHAPv2) are enabled on the Global Authentication Setup page, Cisco Secure ACS first attempts PEAP(EAP-GTC) authentication with the end-user client. If the client rejects this protocol (by sending an EAP NAK message), Cisco Secure ACS attempts authentication with PEAP(EAP-MSCHAPv2). For more information about enabling EAP protocols supported within PEAP, see [Global Authentication Setup, page 10-26](#).

Cisco Secure ACS can use PEAP(EAP-MSCHAPv2) to support machine authentication to Microsoft Windows Active Directory. The end-user client may limit the protocol used for user authentication to the same protocol used for machine authentication; that is, use of PEAP for machine authentication requires the use of PEAP for user authentication. For more information about machine authentication, see [Machine Authentication, page 13-16](#).

Cisco Secure ACS supports a session resume feature for PEAP-authenticated user sessions. When this feature is enabled, Cisco Secure ACS caches the TLS session created during phase one of PEAP authentication, provided that the user successfully authenticates in phase two of PEAP. If a user needs to reconnect and the original PEAP session has not timed out, Cisco Secure ACS uses the cached TLS session, resulting in faster PEAP performance and lessened AAA server load.

**Note**

Session timeout is based on the time that authentication succeeds. It is not dependent upon accounting.

You can enable the PEAP session resume feature and configure the timeout interval on the Global Authentication Setup page. For more information about enabling this feature, see [Global Authentication Setup, page 10-26](#).

Cisco Secure ACS also supports a fast reconnect feature. When the session resume feature is enabled, the fast reconnection feature causes Cisco Secure ACS to allow a PEAP session to resume without checking user credentials. In effect, enabling this feature allows Cisco Secure ACS to trust a user based on the cached TLS session from the original PEAP authentication. Because Cisco Secure ACS only caches a TLS session when phase two of PEAP authentication succeeds, the existence of a cached TLS session is proof that the user has successfully authenticated within the number of minutes defined by the PEAP session timeout option.

Changes to group assignment in an external user database are not enforced by the session resume feature. This is because group mapping does not occur when a user session is extended by the session resume feature. Instead, the user is mapped to the same Cisco Secure ACS group that the user was mapped to upon the beginning of the session. Upon the start of a new session, group mapping enforces the new group assignment.

The fast reconnect feature is particularly useful for wireless LANs, wherein a user may move the client computer so that a different wireless access point is in use. When Cisco Secure ACS resumes a PEAP session, the user reauthenticates without entering a password, provided that the session has not timed out. If the end-user client is restarted, the user must enter a password even if the session timeout interval has not ended.

You can enable the PEAP fast reconnect feature on the Global Authentication Setup page. For more information about enabling this feature, see [Global Authentication Setup, page 10-26](#).

PEAP and the Unknown User Policy

During PEAP authentication, the real username to be authenticated may not be known by Cisco Secure ACS until phase two of authentication. While the Microsoft PEAP client does reveal the actual username during phase one, the Cisco PEAP client does not; therefore, Cisco Secure ACS does not attempt to look up the username presented during phase one and the use of the Unknown User Policy is irrelevant during phase one, regardless of the PEAP client used.

When phase two of PEAP authentication occurs and the username presented by the PEAP client is unknown to Cisco Secure ACS, Cisco Secure ACS processes the username in the same way that it processes usernames presented in other authentication protocols. If the username is unknown and the Unknown User Policy is disabled, authentication fails. If the username is unknown and the Unknown User Policy is enabled, Cisco Secure ACS attempts to authenticate the PEAP user with unknown user processing.

For more information about unknown user processing, see [About Unknown User Authentication, page 16-4](#).

Enabling PEAP Authentication

This procedure provides an overview of the detailed procedures required to configure Cisco Secure ACS to support PEAP authentication.

**Note**

End-user client computers must be configured to support PEAP. This procedure is specific to configuration of Cisco Secure ACS only.

To enable PEAP authentication, follow these steps:

-
- Step 1** Install a server certificate in Cisco Secure ACS. PEAP requires a server certificate. For detailed steps, see [Installing a Cisco Secure ACS Server Certificate](#), page 10-35.

**Note**

If you have previously installed a certificate to support EAP-TLS or PEAP user authentication or to support HTTPS protection of remote Cisco Secure ACS administration, you do not need to perform this step. A single server certificate is sufficient to support all certificate-based Cisco Secure ACS services and remote administration; however, EAP-TLS and PEAP require that the certificate be suitable for server authentication purposes.

- Step 2** Enable PEAP on the Global Authentication Setup page. Cisco Secure ACS allows you to complete this step only after you have successfully completed Step 1. For detailed steps, see [Configuring Authentication Options](#), page 10-33.
- Step 3** Configure a user database. To determine which user databases support PEAP authentication, see [Authentication Protocol-Database Compatibility](#), page 1-10. Cisco Secure ACS is ready to perform PEAP authentication for most users. For more information, see [PEAP and the Unknown User Policy](#), page 10-11.
- Step 4** Consider enabling the Unknown User Policy to simplify PEAP authentication. For more information, see [PEAP and the Unknown User Policy](#), page 10-11. For detailed steps, see [Configuring the Unknown User Policy](#), page 16-16.
-

EAP-FAST Authentication

This section contains the following topics:

- [About EAP-FAST, page 10-13](#)
- [About Master Keys, page 10-15](#)
- [About PACs, page 10-17](#)
 - [Automatic PAC Provisioning, page 10-18](#)
 - [Manual PAC Provisioning, page 10-20](#)
- [Master Key and PAC TTLs, page 10-21](#)
- [Table 10-2](#)
- [Enabling EAP-FAST, page 10-25](#)

About EAP-FAST

The EAP Flexible Authentication via Secured Tunnel (EAP-FAST) protocol is a client-server security architecture that encrypts EAP transactions with a TLS tunnel. While similar to PEAP in this respect, it differs significantly in that EAP-FAST tunnel establishment is based upon strong secrets that are unique to users. These secrets are called Protected Access Credentials (PACs), which Cisco Secure ACS generates using a master key known only to Cisco Secure ACS. Because handshakes based upon shared secrets are intrinsically faster than handshakes based upon PKI, EAP-FAST is the significantly faster of the two solutions that provide encrypted EAP transactions. No certificate management is required to implement EAP-FAST.

EAP-FAST occurs in three phases:

- **Phase zero**—Unique to EAP-FAST, phase zero is a tunnel-secured means of providing an EAP-FAST end-user client with a PAC for the user requesting network access (see [Automatic PAC Provisioning, page 10-18](#)). Providing a PAC to the end-user client is the sole purpose of phase zero. The tunnel is established based on an anonymous Diffie-Hellman key exchange. If EAP-MSCHAPv2 authentication succeeds, Cisco Secure ACS provides the user a PAC. To determine which databases support EAP-FAST phase zero, see [Authentication Protocol-Database Compatibility, page 1-10](#).



Note Phase zero is optional and PACs can be manually provided to end-user clients (see [Manual PAC Provisioning, page 10-20](#)). You control whether Cisco Secure ACS supports phase zero by selecting the Allow automatic PAC provisioning check box in the Global Authentication Configuration page.

No network service is enabled by phase zero of EAP-FAST; therefore, even a successful EAP-FAST phase zero transaction is recorded in the Cisco Secure ACS Failed Attempts log.

- **Phase one**—In phase one, Cisco Secure ACS and the end-user client establish a TLS tunnel based upon the PAC presented by the end-user client. This requires that the end-user client has been provided a PAC for the user attempting to gain network access and that the PAC is based on a master key that has not expired. The means by which PAC provisioning has occurred is irrelevant; either automatic or manual provisioning may be used.

No network service is enabled by phase one of EAP-FAST.

- **Phase two**—In phase two, Cisco Secure ACS authenticates the user credentials with EAP-GTC, which is protected by the TLS tunnel created in phase one. No other EAP types are supported for EAP-FAST. To determine which databases support EAP-FAST phase two, see [Authentication Protocol-Database Compatibility, page 1-10](#).

Cisco Secure ACS authorizes network service with a successful user authentication in phase two of EAP-FAST and logs the authentication in the Passed Authentications log, if it is enabled. Also, if necessary, Cisco Secure ACS may refresh the end-user client PAC, which creates a second entry in the Passed Authentication log for the same phase two transaction.

EAP-FAST can protect the username in all EAP-FAST transactions. Cisco Secure ACS does not perform user authentication based on a username presented in phase one; however, whether the username is protected during phase one depends upon the end-user client. If the end-user client does not send the real username in phase one, the username is protected. The Cisco Aironet EAP-FAST client protects the username in phase one by sending `FAST_MAC address` in place of the username. After phase one of EAP-FAST, all data is encrypted, including username information usually sent in clear text.

Cisco Secure ACS supports password aging with EAP-FAST for users authenticated by Windows user databases. Password aging can work with either phase zero or phase two of EAP-FAST. If password aging requires a user to change passwords during phase zero, the new password would be effective in phase two. For more information about password aging for Windows user databases, see [Enabling Password Aging for Users in Windows Databases](#), page 6-26.

About Master Keys

EAP-FAST master keys are strong secrets that Cisco Secure ACS automatically generates and that only Cisco Secure ACS is aware of. Master keys are never sent to an end-user client. EAP-FAST requires master keys for two purposes:

- **PAC generation**—Cisco Secure ACS generates PACs using the active master key. For details about PACs, see [About PACs](#), page 10-17.
- **EAP-FAST phase one**—Cisco Secure ACS determines whether the PAC presented by the end-user client was generated by one of the master keys it is aware of, either the active master key or a retired master key.

To increase the security of EAP-FAST, Cisco Secure ACS changes the master key that it uses to generate PACs. Cisco Secure ACS uses time-to-live (TTL) values you define to determine when it generates a new master key and to determine the age of all master keys. Based on TTL values, Cisco Secure ACS assigns master keys one of the three following states:

- **Active**—An active master key is the master key used by Cisco Secure ACS to generate PACs. The duration that a master key remains active is determined by the Master key TTL setting. At any time, only one master key is active. When you define TTLs for master keys and PACs, Cisco Secure ACS permits only a PAC TTL that is shorter than the active master key TTL. This limitation ensures that a PAC is refreshed at least once before the expiration of the master key used to generate the PAC, provided that EAP-FAST users log in to the network at least once before the master key expires. For more information about how TTL values determine whether PAC refreshing or provisioning is required, see [Master Key and PAC TTLs](#), page 10-21.

When Cisco Secure ACS is configured to receive replicated EAP-FAST policies and master keys, a backup master key is among the master keys received. The backup master key is used only if the active master key retires

before the next successful master key replication. If the backup master key also retires before the next successful master key replication, EAP-FAST authentication fails for all users requesting network access with EAP-FAST.

**Tip**

If EAP-FAST authentication fails because the active and backup master keys have retired and Cisco Secure ACS has not received new master keys in replication, you can force Cisco Secure ACS to generate its own master keys by selecting the EAP-FAST Master Server check box and clicking Submit.

Cisco Secure ACS records the generation of master keys in the logs for the CSAuth service.

- **Retired**—When a master key becomes older than the Master key TTL settings, it is considered retired for as long as specified by the Retired master key TTL settings. Cisco Secure ACS can store up to 255 retired master keys. While a retired master key is not used to generate new PACs, Cisco Secure ACS needs it to authenticate PACs that were generated using it. When you define TTLs for master keys and retired master keys, Cisco Secure ACS permits only TTL settings that require storing 255 or fewer retired master keys. For example, if the master key TTL is 1 hour and the retired master key TTL is 4 weeks, this would require storing up to 671 retired master keys; therefore, Cisco Secure ACS presents an error message and does not allow these settings.

When a user gains network access using a PAC generated with a retired master key, Cisco Secure ACS provides the end-user client a new PAC generated with the active master key. For more information about Cisco Secure ACS with respect to the states of master keys and PACs, see [Master Key and PAC TTLs, page 10-21](#).

- **Expired**—When a master key becomes older than the sum of the master key TTL and retired master TTL settings, it is considered expired and Cisco Secure ACS deletes it from its records of master keys. For example, if the master key TTL is one hour and the retired master key TTL is one week, a master key expires when it becomes greater than one week and one hour old.

PACs generated by an expired master key cannot be used to access your network. An end-user client presenting a PAC that was generated with an expired master key must be provided a new PAC using automatic or manual provisioning before phase one of EAP-FAST can succeed.

About PACs

PACs are strong shared secrets that enable Cisco Secure ACS and an EAP-FAST end-user client to authenticate each other and establish a TLS tunnel for use in EAP-FAST phase two. Cisco Secure ACS generates PACs using the active master key and a username. An EAP-FAST end-user client stores PACs for each user accessing the network with the client. Additionally, a AAA server that supports EAP-FAST has a unique Authority ID. An end-user client associates a user's PACs with the Authority ID of the AAA server that generated them.

During EAP-FAST phase one, the end-user client presents the PAC that it has for the current user and for the Authority ID sent by Cisco Secure ACS at the beginning of the EAP-FAST transaction. Cisco Secure ACS determines whether the PAC was generated using one of the master keys it is aware of, either active or retired (a PAC generated using a master key that has since expired can never be used to gain network access). When an end-user client has a PAC generated with an expired master key, the end-user client must receive a new PAC before EAP-FAST phase one can succeed. The means of providing PACs to end-user clients, known as PAC provisioning, are discussed in [Automatic PAC Provisioning, page 10-18](#) and [Manual PAC Provisioning, page 10-20](#).

After end-user clients are provided PACs, Cisco Secure ACS refreshes them as dictated by master key and PAC TTL values. Cisco Secure ACS generates and sends a new PAC as needed at the end of phase two of EAP-FAST; however, if you shorten the master key TTL, you may in effect be requiring PAC provisioning to occur. For more information about how master key and PAC states determine whether Cisco Secure ACS sends a new PAC to the end-user client at the end of phase two, see [Master Key and PAC TTLs, page 10-21](#).

Regardless of the master key TTL values you define, a user will require PAC provisioning when the user does not use EAP-FAST to access the network before the master key used to generate the user's PAC has expired. For example, if the master key TTL is one week and the retired master key TTL is one week, each EAP-FAST end-user client used by someone who goes on vacation for two weeks will require PAC provisioning.

The following list contrasts the various means by which an end-user client can receive PACs:

- **PAC provisioning**—Required when an end-user client has no PAC or has a PAC that is based on an expired master key. For more information about how master key and PAC states determine whether PAC provisioning is required, see [Master Key and PAC TTLs, page 10-21](#).

Two means of PAC provisioning are supported:

- **Automatic provision**—Sends a PAC using a secure network connection. For more information, see [Automatic PAC Provisioning, page 10-18](#).
 - **Manual provision**—Requires that you use Cisco Secure ACS to generate a PAC file for the user, copy the PAC file to the computer running the end-user client, and import the PAC file into the end-user client. For more information, see [Manual PAC Provisioning, page 10-20](#).
- **PAC refresh**—Occurs automatically when EAP-FAST phase two authentication has succeeded and master key and PAC TTLs dictate that the PAC must be refreshed. For more information about how master key and PAC states determine whether a PAC is refreshed, see [Master Key and PAC TTLs, page 10-21](#).

PACs have the following two states, determined by the PAC TTL setting:

- **Active**—A PAC younger than the PAC TTL is considered active and can be used to complete EAP-FAST phase one, provided that the master key used to generate it has not expired. Regardless of whether a PAC is active, if it is based on an expired master key, PAC provisioning must occur before EAP-FAST phase one can succeed.
- **Expired**—A PAC older than the PAC TTL is considered expired. Provided that the master key used to generate the PAC has not expired, an expired PAC can be used to complete EAP-FAST phase one and, at the end of EAP-FAST phase two, Cisco Secure ACS will generate a new PAC for the user and provide it to the end-user client.

Automatic PAC Provisioning

Automatic PAC provisioning sends a new PAC to an end-user client over a secured network connection. Automatic PAC provisioning requires no intervention of the network user or a Cisco Secure ACS administrator, provided that both Cisco Secure ACS and the end-user client are configured to support automatic provisioning.

EAP-FAST phase zero requires EAP-MSCHAPv2 authentication of the user. Upon successful user authentication, Cisco Secure ACS establishes a Diffie-Hellman tunnel with the end-user client. Cisco Secure ACS generates a PAC for the user and sends it to the end-user client within this tunnel, along with the Authority ID and Authority ID information about this Cisco Secure ACS.

**Note**

Because EAP-FAST phase zero and phase two use different authentication methods (EAP-MSCHAPv2 in phase zero versus EAP-GTC in phase two), some databases that support phase two cannot support phase zero. Given that Cisco Secure ACS associates each user with a single user database, the use of automatic PAC provisioning requires that EAP-FAST users are authenticated with a database that is compatible with EAP-FAST phase zero. For the databases with which Cisco Secure ACS can support EAP-FAST phase zero and phase two, see [Authentication Protocol-Database Compatibility, page 1-10](#).

No network service is enabled by phase zero of EAP-FAST; therefore, Cisco Secure ACS logs a EAP-FAST phase zero transaction in the Failed Attempts log, including an entry that PAC provisioning occurred. After the end-user client has received a PAC through a successful phase zero, it sends a new EAP-FAST request to begin phase one.

**Note**

Because transmission of PACs in phase zero is secured by MS-CHAPv2 authentication and MS-CHAPv2 is vulnerable to dictionary attacks, we recommend that you limit use of automatic provisioning to initial deployment of EAP-FAST. After a large EAP-FAST deployment, PAC provisioning should be performed manually to ensure the highest security for PACs. For more information about manual PAC provisioning, see [Manual PAC Provisioning, page 10-20](#).

To control whether Cisco Secure ACS performs automatic PAC provisioning, you use the options on the Global Authentication Setup page in the System Configuration section. For more information, see [Authentication Configuration Options, page 10-27](#).

Manual PAC Provisioning

Manual PAC provisioning requires a Cisco Secure ACS administrator to generate PAC files, which must then be distributed to the applicable network users. Users must configure end-user clients with their PAC files. For example, if your EAP-FAST end-user client is the Cisco Aironet Client Utility (ACU), configuring the ACU to support EAP-FAST requires that you import a PAC file. For more information about configuring a Cisco ACU, see the applicable configuration guide for your ACU.

You can use manual PAC provisioning to control who can use EAP-FAST to access your network. If you disable automatic PAC provisioning, any EAP-FAST user denied a PAC cannot access the network. If your Cisco Secure ACS deployment includes network segmentation wherein access to each network segment is controlled by a separate Cisco Secure ACS, manual PAC provisioning enables you to grant EAP-FAST access on a per-segment basis. For example, if your company uses EAP-FAST for wireless access in its Chicago and Boston offices and the Cisco Aironet Access Points at each of these two offices are configured to use different Cisco Secure ACSes, you can determine, on a per-employee basis, whether Boston employees visiting the Chicago office can have wireless access.



Note

Replicating EAP-FAST master keys and policies affects the ability to require different PACs per Cisco Secure ACS. For more information, see [Table 10-2](#).

While the administrative overhead of manual PAC provisioning is much greater than automatic PAC provisioning, it does not include the risk of sending the PAC over the network. When you first deploy EAP-FAST, using manual PAC provisioning would require a lot of manual configuration of end-user clients; however, it is the most secure means for distributing PACs. We recommend that, after a large EAP-FAST deployment, PAC provisioning should be performed manually to ensure the highest security for PACs.

You can generate PAC files for specific usernames, groups of users, lists of usernames, or all users. When you generate PAC files for groups of users or all users, the users must be known or discovered users and cannot be unknown users. Cisco Secure ACS for Windows Server supports the generation of PAC files with CSUtil.exe. For more information about generating PACs with CSUtil.exe, see [PAC File Generation, page D-40](#).

Master Key and PAC TTLs

The TTL values for master keys and PACs determine their states, as described in [About Master Keys, page 10-15](#) and [About PACs, page 10-17](#). Master key and PAC states determine whether someone requesting network access with EAP-FAST requires PAC provisioning or PAC refreshing. [Table 10-1](#) summarizes Cisco Secure ACS behavior with respect to PAC and master key states.

Table 10-1 Master Key versus PAC States

Master key state	PAC active	PAC expired
Master key active	Phase one succeeds. PAC is <i>not</i> refreshed at end of phase two.	Phase one succeeds. PAC is refreshed at end of phase two.
Master key retired	Phase one succeeds. PAC is refreshed at end of phase two.	Phase one succeeds. PAC is refreshed at end of phase two.
Master key expired	PAC provisioning is required. If automatic provisioning is <i>enabled</i> , phase zero occurs and a new PAC is sent. The end-user client initiates a new EAP-FAST authentication request using the new PAC. If automatic provisioning is <i>disabled</i> , phase zero does not occur and phase one fails. You must use manual provisioning to give the user a new PAC.	PAC provisioning is required. If automatic provisioning is <i>enabled</i> , phase zero occurs and a new PAC is sent. The end-user client initiates a new EAP-FAST authentication request using the new PAC. If automatic provisioning is <i>disabled</i> , phase zero does not occur and phase one fails. You must use manual provisioning to give the user a new PAC.

Replication and EAP-FAST

The CiscoSecure Database Replication feature supports the replication of EAP-FAST settings, Authority ID, and master keys. Replication of EAP-FAST data occurs only if the following are true:

- On the Database Replication Setup page of the primary Cisco Secure ACS, under Send, you have selected the EAP-FAST master keys and policies check box.
- On the Global Authentication Setup page of the primary Cisco Secure ACS, you have enabled EAP-FAST and selected the EAP-FAST master server check box.
- On the Database Replication Setup page of the secondary Cisco Secure ACS, under Receive, you have selected the **EAP-FAST master keys and policies** check box.
- On the Global Authentication Setup page of the secondary Cisco Secure ACS, you have enabled EAP-FAST and deselected the EAP-FAST master server check box.

EAP-FAST-related replication occurs for three events:

- **Generation of master keys**—A primary Cisco Secure ACS sends newly generated active and backup master keys to secondary Cisco Secure ACSes. This occurs immediately after master key generation, provided that replication is configured properly and is not affected by replication scheduling on the Database Replication Setup page.
- **Manual replication**—All EAP-FAST components that can be replicated are replicated if you click Replicate Now on the Database Replication Setup page of the primary Cisco Secure ACS. Some of the replicated components are configurable in the HTML interface. Whether an EAP-FAST component is replicated or configurable is detailed in [Table 10-2](#).



Note EAP-FAST replication is not included in scheduled replication events.

- **Changes to EAP-FAST settings**—If, on a primary Cisco Secure ACS, you change any EAP-FAST configurable components that are replicated, Cisco Secure ACS begins EAP-FAST replication. Whether an EAP-FAST component is replicated or configurable is detailed in [Table 10-2](#).

The Database Replication log on the primary Cisco Secure ACS records replication of master keys. Entries related to master key replication contain the text “MKEYReplicate”.

Table 10-2 EAP-FAST Components and Replication

EAP-FAST Component	Replicated?	Configurable?
EAP-FAST Enable	No	Yes, on the Global Authentication Setup page.
Master key TTL	Yes	Yes, on the Global Authentication Setup page.
Retired master key TTL	Yes	Yes, on the Global Authentication Setup page.
PAC TTL	Yes	Yes, on the Global Authentication Setup page.
Authority ID	Yes	No, generated by Cisco Secure ACS.
Authority ID info	Yes	Yes, on the Global Authentication Setup page.
Client initial message	Yes	Yes, on the Global Authentication Setup page.
Master keys	Yes	No, generated by Cisco Secure ACS when TTL settings dictate.
EAP-FAST master server	No	Yes, on the Global Authentication Setup page.
Actual EAP-FAST server status	No	No, determined by Cisco Secure ACS.

The EAP-FAST master server setting has a significant effect upon EAP-FAST authentication and replication, as follows:

- Enabled**—When the EAP-FAST master server check box is selected, the “Actual EAP-FAST server status” is `Master` and Cisco Secure ACS ignores the EAP-FAST settings, Authority ID, and master keys it receives from a primary Cisco Secure ACS during replication, preferring instead to use master keys it generates, its unique Authority ID, and the EAP-FAST settings configured in its HTML interface.

Enabling the EAP-FAST master server setting requires providing for the end-user client a PAC from the primary Cisco Secure ACS that is different than the PAC from the secondary Cisco Secure ACS. Because the primary and secondary Cisco Secure ACSes send different Authority IDs at the beginning of the EAP-FAST transaction, the end-user client must have a PAC for each Authority ID. A PAC generated by the primary Cisco Secure ACS is not

accepted by the secondary Cisco Secure ACS in a replication scheme where the EAP-FAST master server setting is enabled on the secondary Cisco Secure ACS.

**Tip**

In a replicated Cisco Secure ACS environment, use the EAP-FAST master server feature in conjunction with disallowing automatic PAC provisioning to control EAP-FAST access to different segments of your network. Without automatic PAC provisioning, users must request PACs for each network segment.

- **Disabled**—When the EAP-FAST master server check box is not selected, Cisco Secure ACS continues to operate as an EAP-FAST master server until the first time it receives replicated EAP-FAST components from the primary Cisco Secure ACS. When “Actual EAP-FAST server status” displays the text `slave`, Cisco Secure ACS uses the EAP-FAST settings, Authority ID, and master keys it receives from a primary Cisco Secure ACS during replication, rather than using master keys it generates and its unique Authority ID.

**Note**

When you deselect the EAP-FAST master server check box, the “Actual EAP-FAST server status” remains `Master` until Cisco Secure ACS receives replicated EAP-FAST components and then the “Actual EAP-FAST server status” changes to `slave`. Until “Actual EAP-FAST server status” changes to `slave`, Cisco Secure ACS acts as a master EAP-FAST server, using master keys it generates, its unique Authority ID, and the EAP-FAST settings configured in its HTML interface.

Disabling the EAP-FAST master server setting eliminates the need for providing a different PAC from the primary and secondary Cisco Secure ACSes. This is because the primary and secondary Cisco Secure ACSes send the end-user client the same Authority ID at the beginning of the EAP-FAST transaction; therefore, the end-user client uses the same PAC in its response to either Cisco Secure ACS. Also, a PAC generated for a user by one Cisco Secure ACS in a replication scheme where the EAP-FAST master server setting is disabled is accepted by all other Cisco Secure ACSes in the same replication scheme.

For more information about replication, see [CiscoSecure Database Replication, page 9-1](#).

Enabling EAP-FAST

This procedure provides an overview of the detailed procedures required to configure Cisco Secure ACS to support EAP-FAST authentication.

**Note**

End-user clients must be configured to support EAP-FAST. This procedure is specific to configuring Cisco Secure ACS only.

Before You Begin

The steps in this procedure are a suggested order only. Enabling EAP-FAST at your site may require recursion of these steps or performing these steps in a different order. For example, in this procedure, determining how you want to support PAC provisioning comes after configuring a user database to support EAP-FAST; however, choosing automatic PAC provisioning places different limits upon user database support.

To enable Cisco Secure ACS to perform EAP-FAST authentication, follow these steps:

-
- Step 1** Configure a user database that supports EAP-FAST authentication. To determine which user databases support EAP-FAST authentication, see [Authentication Protocol-Database Compatibility, page 1-10](#). For user database configuration, see [Chapter 13, “User Databases”](#).



Note User database support differs for EAP-FAST phase zero and phase two.

Cisco Secure ACS supports use of the Unknown User Policy and group mapping with EAP-FAST, as well as password aging with Windows external user databases.

- Step 2** Determine master key and PAC TTL values. While changing keys and PACs more frequently could be considered more secure, it also increases the likelihood that PAC provisioning will be needed for machines left offline so long that the PACs on them are based on expired master keys.

Also, if you reduce the TTL values that you initially deploy EAP-FAST with, you may force PAC provisioning to occur because users would be more likely to have PACs based on expired master keys.

For information about how master key and PAC TTL values determine whether PAC provisioning or PAC refreshing is required, see [Master Key and PAC TTLs, page 10-21](#).

- Step 3** Determine whether you want to use automatic or manual PAC provisioning. For more information about the two means of PAC provisioning, see [Automatic PAC Provisioning, page 10-18](#), and [Manual PAC Provisioning, page 10-20](#).



Note We recommend limiting the use of automatic PAC provisioning to initial deployments of EAP-FAST, followed by using manual PAC provisioning for adding small numbers of new end-user clients to your network and for replacing PACs based on expired master keys.

- Step 4** Using the decisions during [Step 2](#) and [Step 3](#), enable EAP-FAST on the Global Authentication Setup page. For detailed steps, see [Configuring Authentication Options, page 10-33](#).

Cisco Secure ACS is ready to perform EAP-FAST authentication.

Global Authentication Setup

The Global Authentication Setup page provides a means to enable or disable some of the authentication protocols supported by Cisco Secure ACS. You can also configure other options for some of the protocols represented on the Global Authentication Setup page.

This section contains the following topics:

- [Authentication Configuration Options, page 10-27](#)
- [Configuring Authentication Options, page 10-33](#)

Authentication Configuration Options

The Global Authentication Setup page contains the following configuration options:

- **PEAP**—You can configure the following options for PEAP:
 - **Allow EAP-MSCHAPv2**—Whether Cisco Secure ACS attempts EAP-MSCHAPv2 authentication with PEAP clients.

**Note**

If both the Allow EAP-MSCHAPv2 and the Allow EAP-MSCHAPv2 check boxes are selected, Cisco Secure ACS negotiates the EAP type with the end-user PEAP client.

- **Allow EAP-GTC**—Whether Cisco Secure ACS attempts EAP-GTC authentication with PEAP clients.
- **Cisco client initial message**—The message you want displayed during PEAP authentication. The PEAP client initial display message is the first challenge a user of a Cisco Aironet PEAP client sees when attempting authentication. It should direct the user on what to do next, for example, “Enter your passcode.” The message is limited to 60 characters.
- **PEAP session timeout (minutes)**—The maximum PEAP session length you want to allow users, in minutes. A session timeout value greater than 0 (zero) enables the PEAP session resume feature, which caches the TLS session created in phase one of PEAP authentication. When a PEAP client reconnects, Cisco Secure ACS uses the cached TLS session to restore the session, which improves PEAP performance. Cisco Secure ACS deletes cached TLS sessions when they time out. The default timeout value is 120 minutes. To disable the session resume feature, set the timeout value to 0 (zero).
- **Enable Fast Reconnect**—Whether Cisco Secure ACS resumes sessions for PEAP clients without performing phase two of PEAP authentication. Deselecting the Enable Fast Reconnect check box causes Cisco Secure ACS to always perform phase two of PEAP authentication, even when the PEAP session has not timed out.

Fast reconnection can occur only when Cisco Secure ACS allows the session to resume because the session has not timed out. If you disable the PEAP session resume feature by entering 0 (zero) in the PEAP

session timeout (minutes) box, selecting the Enable Fast Reconnect check box has no effect on PEAP authentication and phase two of PEAP authentication always occurs.

- **EAP-FAST**—You can configure the following options for EAP-FAST:
 - **Allow EAP-FAST**—Whether Cisco Secure ACS permits EAP-FAST authentication.



Note If users access your network using a AAA client defined in the Network Configuration section as a RADIUS (Cisco Aironet) device, one or more of the LEAP, EAP-TLS, or EAP-FAST protocols must be enabled on the Global Authentication Setup page; otherwise, Cisco Aironet users cannot authenticate.

- **Master Key TTL**—The duration that a master key is used to generate new PACs. When the master key becomes older than the master key TTL, Cisco Secure ACS retires the master key and generates a new master key. The default master key TTL is one month.



Note Decreasing the master key TTL can cause retired master keys to expire because a master key expires when it is older than the sum of the master key TTL and the retired master key TTL; therefore, decreasing the master key TTL requires PAC provisioning for end-user clients with PACs based on the newly expired master keys.

For more information about master keys, see [About Master Keys, page 10-15](#).

- **Retired master key TTL**—The duration that PACs generated using a retired master key are acceptable for EAP-FAST authentication. In other words, the retired master key TTL defines the length of the grace period during which PACs generated with a master key that is no longer active are acceptable. When an end-user client gains network access using a PAC based on a retired master key, Cisco Secure ACS sends a new PAC to the end-user client. The default retired master key TTL is three months.

When a retired master key ages past the retired master key TTL, it expires and Cisco Secure ACS deletes it.



Note Decreasing the retired master key TTL is likely to cause some retired master keys to expire; therefore, end-user clients with PACs based on the newly expired master keys require PAC provisioning.



Note Decreasing the retired master key TTL can cause retired master keys to expire; therefore, decreasing the retired master key TTL requires PAC provisioning for end-user clients with PACs based on the newly expired master keys.

For more information about master keys, see [About Master Keys, page 10-15](#).

- **PAC TTL**—The duration that a PAC is used before it expires and must be replaced. If the master key used to generate it has not expired, new PAC creation and assignment are automatic. If the master key used to generate it has expired, in-band or out-of-band provisioning must be used to provide the end-user client with a new PAC. The default PAC TTL is one week.

For more information about PACs, see [About PACs, page 10-17](#).

- **Client initial display message**—Specifies a message to be sent to users who authenticate with an EAP-FAST client. Maximum length is 40 characters.



Note A user will see the initial display message only if the end-user client supports its display.

- **Authority ID Info**—A short description of this Cisco Secure ACS, sent along with PACs issued by Cisco Secure ACS. EAP-FAST end-user clients use it to describe the AAA server that issued the PAC. Maximum length is 64 characters.



Note Authority ID information is not the same as the Authority ID, which is generated automatically by Cisco Secure ACS and is not configurable. While the Authority ID is used by end-user clients to determine which PAC to send to Cisco Secure ACS, the Authority ID information is strictly the human-readable label associated with the Authority ID.

- **Allow automatic PAC provisioning**—Whether Cisco Secure ACS will provision an end-user client with a PAC using EAP-FAST phase 0. If this check box is selected, Cisco Secure ACS establishes a secured connection with the end-user client for providing a new PAC. If the check box is not selected, Cisco Secure ACS denies the user access and PAC provisioning must be performed out of band (manually).
- **EAP-FAST Master Server**—When this check box is not selected and when Cisco Secure ACS receives replicated EAP-FAST policies, Authority ID, and master keys, Cisco Secure ACS uses them rather than its own EAP-FAST policies, Authority ID, and master keys.

When this check box is selected, Cisco Secure ACS uses its own EAP-FAST policies, Authority ID, and master keys. For more information, see [Table 10-2](#).



Note Click Submit + Restart if you change the EAP-FAST master server setting.

- **Actual EAP-FAST server status**—This read-only option displays the state of Cisco Secure ACS with respect to EAP-FAST. If this option displays “Master”, Cisco Secure ACS generates its own master keys and Authority ID. If this option displays “Slave”, Cisco Secure ACS uses master keys and the Authority ID it receives during replication. For more information, see [Table 10-2](#).



Tip

If you deselect the EAP-FAST Master Server check box, EAP-FAST server status remains “Master” until Cisco Secure ACS receives replicated EAP-FAST components.

- **EAP-TLS**—You can configure the following options for EAP-TLS:
 - **Allow EAP-TLS**—Whether Cisco Secure ACS permits EAP-TLS authentication.

**Note**

If users access your network using a AAA client defined in the Network Configuration section as a RADIUS (Cisco Aironet) device, one or more of the LEAP, EAP-TLS, or EAP-FAST protocols must be enabled on the Global Authentication Setup page; otherwise, Cisco Aironet users cannot authenticate.

- **Certificate SAN comparison**—Whether authentication is performed by comparing the Subject Alternative Name (SAN) of the end-user client certificate to the username in the applicable user database.

**Note**

If you select more than one comparison type, Cisco Secure ACS performs the comparisons in the order listed. If the one comparison type fails, Cisco Secure ACS attempts the next enabled comparison type. Comparison stops after the first successful comparison.

- **Certificate CN comparison**—Whether authentication is performed by comparing the Common Name of the end-user client certificate to the username in the applicable user database.
- **Certificate Binary comparison**—Whether authentication is performed by a binary comparison of the end-user client certificate to the user certificate stored in the applicable user database. This comparison method cannot be used to authenticate users stored in an ODBC external user database.
- **EAP-TLS session timeout (minutes)**—The maximum EAP-TLS session length you want to allow users, in minutes. A session timeout value greater than 0 (zero) enables the EAP-TLS session resume feature. The session resume feature allows users to reauthenticate without a user lookup or certificate comparison provided that the session has not timed out. If the end-user client is restarted, authentication requires a certificate lookup even if the session timeout interval has not ended. The default timeout value is 120 minutes. To disable the session timeout feature, set the timeout value to 0 (zero).

- **LEAP**—The Allow LEAP (For Aironet only) check box controls whether Cisco Secure ACS performs LEAP authentication. LEAP is currently used only for Cisco Aironet wireless networking. If you disable this option, Cisco Aironet end-user clients configured to perform LEAP authentication cannot access the network. If all Cisco Aironet end-user clients use a different authentication protocol, such as EAP-TLS, we recommend that you disable this option.



Note If users access your network using a AAA client defined in the Network Configuration section as a RADIUS (Cisco Aironet) device, either LEAP, EAP-TLS, or both must be enabled on the Global Authentication Setup page; otherwise, Cisco Aironet users cannot authenticate.

- **EAP-MD5**—The Allow EAP-MD5 check box controls whether Cisco Secure ACS performs EAP-MD5 authentication. If you disable this option, end-user clients configured to perform EAP-MD5 authentication cannot access the network. If no end-user clients use EAP-MD5, we recommend that you disable this option.
- **AP EAP request timeout (seconds)**—Whether Cisco Secure ACS instructs Cisco Aironet Access Points (APs) to use the specified timeout value during EAP conversations. The value specified must be the number of seconds after which Cisco Aironet APs should assume that an EAP transaction with Cisco Secure ACS has been lost and should be restarted. A value of 0 (zero) disables this feature.

During EAP conversations, Cisco Secure ACS sends the value defined in the AP EAP request timeout box using the IETF RADIUS Session-Timeout (27) attribute; however, in the RADIUS Access-Accept packet at the end of the conversation, the value that Cisco Secure ACS sends in the IETF RADIUS Session-Timeout (27) attribute is the value specified in the Cisco Aironet RADIUS VSA Cisco-Aironet-Session-Timeout (01) or, if that attribute is not enabled, the IETF RADIUS Session-Timeout (27) attribute.



Note Cisco Aironet RADIUS VSA Cisco-Aironet-Session-Timeout (01) is not a true RADIUS VSA; instead, it represents the value that Cisco Secure ACS sends in the IETF RADIUS Session-Timeout attribute when the AAA client sending the RADIUS request is defined in the Network Configuration as authenticating with RADIUS (Cisco Aironet).

- **MS-CHAP Configuration**—The Allow MS-CHAP Version 1 Authentication and Allow MS-CHAP Version 2 Authentication check boxes control whether Cisco Secure ACS performs MS-CHAP authentication for RADIUS requests. The two check boxes allow you to further control which versions of MS-CHAP are permitted in RADIUS requests. If you disable a particular version of MS-CHAP, end-user clients configured to authenticate with that version using RADIUS cannot access the network. If no end-user clients are configured to use a specific version of MS-CHAP with RADIUS, we recommend that you disable that version of MS-CHAP.



Note For TACACS+, Cisco Secure ACS supports only MS-CHAP version 1. TACACS+ support for MS-CHAP version 1 is always enabled and is not configurable.

Configuring Authentication Options

Use this procedure to select and configure how Cisco Secure ACS handles options for authentication. In particular, use this procedure to specify and configure the varieties of EAP that you allow, and to specify whether you allow either MS-CHAP Version 1 or MS-CHAP Version 2, or both.

For more information on the EAP-TLS Protocol, see [EAP-TLS Authentication, page 10-2](#). For more information on the PEAP protocol, see [PEAP Authentication, page 10-8](#). For more information on the PEAP protocol, see [EAP-FAST Authentication, page 10-13](#). For details regarding how various password protocols are supported by the various databases, see [Authentication Protocol-Database Compatibility, page 1-10](#).

Before You Begin

For information about the options on the Global Authentication Setup page, see [Authentication Configuration Options, page 10-27](#).

To configure authentication options, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
- Step 2** Click **Global Authentication Setup**.
Cisco Secure ACS displays the Global Authentication Setup page.
- Step 3** Configure options, as applicable. For more information about the significance of the options, see [Authentication Configuration Options, page 10-27](#).
- Step 4** If you want to immediately implement the settings you have made, click **Submit + Restart**.
Cisco Secure ACS restarts its services and implements the authentication configuration options you selected.
- Step 5** If you want to save the settings you have made but implement them later, click **Submit**.



Tip You can restart Cisco Secure ACS services at any time by using the Service Control page in the System Configuration section.

Cisco Secure ACS saves the authentication configuration options you selected.

Cisco Secure ACS Certificate Setup

This section contains the following topics:

- [Installing a Cisco Secure ACS Server Certificate, page 10-35](#)
- [Adding a Certificate Authority Certificate, page 10-37](#)
- [Editing the Certificate Trust List, page 10-38](#)
- [Managing Certificate Revocation Lists, page 10-40](#)
- [Generating a Certificate Signing Request, page 10-45](#)

- [Using Self-Signed Certificates, page 10-47](#)
- [Updating or Replacing a Cisco Secure ACS Certificate, page 10-50](#)

Installing a Cisco Secure ACS Server Certificate

Perform this procedure to install (that is, enroll) a server certificate for your Cisco Secure ACS. You can perform certificate enrollment to support EAP-TLS and PEAP authentication, as well as to support HTTPS protocol for GUI access to Cisco Secure ACS. There are three basic options for how you obtain your server certificate; you may:

- Obtain a certificate from a CA
- Use an existing certificate from local machine storage
- Generate a self-signed certificate.

Before You Begin

You must have a server certificate for your Cisco Secure ACS before you can install it. With Cisco Secure ACS, certificate files must be in Base64-encoded X.509. If you do not already have a server certificate in storage, you can use the procedure in [Generating a Certificate Signing Request, page 10-45](#), or any other means, to obtain a certificate for installation.

If you are installing a server certificate that replaces an existing server certificate, the installation could affect the configuration of the CTL and CRL settings your Cisco Secure ACS. After you have installed a replacement certificate, you should determine whether you need to reconfigure any CTL or CRL settings.

If you want to use a server certificate from local machine storage, we recommend that you read *Extensible Authentication Protocol Transport Layer Security Deployment Guide for Wireless LAN Networks*, available on the Cisco Secure ACS CD and at <http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml>. This white paper provides information about how to add a certificate to machine storage and how to configure a Microsoft certification authority server for use with Cisco Secure ACS.

To install an existing certificate for use on Cisco Secure ACS, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **ACS Certificate Setup**.

Step 3 Click **Install ACS Certificate**.

Cisco Secure ACS displays the Install ACS Certificate page.

Step 4 You must specify whether Cisco Secure ACS reads the certificate from a specified file or uses a certificate already in storage on the local machine. Do one of the following:

- To specify that Cisco Secure ACS reads the certificate from a specified file, select the **Read certificate from file** option, and then type the full directory path and filename of the certificate file in the Certificate file box.
- To specify that Cisco Secure ACS uses a particular existing certificate from local machine certificate storage, select the **Use certificate from storage** option, and then type the certificate CN (common name/subject name) in the Certificate CN box.



Tip

Type the certificate CN only; omit the **cn=** prefix.

Step 5 If you generated the request using Cisco Secure ACS, in the Private key file box, type the full directory path and name of the file that contains the private key.



Note

If the certificate was installed in storage with the private key, you do not have the private key file and do not need to type it.



Tip

This is the private key associated with the server certificate.

Step 6 In the Private key password box, type the private key password.



Tip

If you used Cisco Secure ACS to generate the certificate signing request, this is the value you entered in *Private key password* on the Generate Certificate Signing Request page. If the private key file is unencrypted, leave this box empty.

Step 7 Click **Submit**.

To show that the certificate setup is complete, Cisco Secure ACS displays the Installed Certificate Information table, which contains the following certificate information:

- Issued to: *certificate subject*
 - Issued by: *CA common name*
 - Valid from:
 - Valid to:
 - Validity
-

Adding a Certificate Authority Certificate

Use this procedure to add new certification authority (CA) certificates to Cisco Secure ACS local certificate storage.

**Note**

If the clients and Cisco Secure ACS are getting their certificates from the same CA, you do not need to perform this procedure because Cisco Secure ACS automatically trusts the CA that issued its certificate.

When a user certificate is from an unknown CA (that is, one that is different from the CA that certifies the Cisco Secure ACS), you must specifically configure Cisco Secure ACS to trust that CA or authentication fails. Until you perform this procedure to explicitly extend trust by adding another CA, Cisco Secure ACS only recognizes certificates from the CA that issued its own certificate.

Configuring Cisco Secure ACS to trust a specific CA is a two-step process that comprises both this procedure of adding a CA's certificate and the procedure in [Editing the Certificate Trust List, page 10-38](#), where you signify that the particular CA is to be trusted. (Cisco Secure ACS comes configured with a list of popular CAs, none of which are enabled until you explicitly signify trustworthiness.)

To add a certificate authority certificate to your local storage, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **ACS Certification Authority Setup**.

Cisco Secure ACS displays the CA Operations table on the Certification Authorities Setup page.

Step 4 In the CA certificate file box, type the full path and filename for the certificate you want to use.

Step 5 Click **Submit**.

The new CA certificate is added to local certificate storage. And, if it is not already there, the name of the CA that issued the certificate is placed on the CTL.



Tip To use this new CA certificate to authenticate users, you must edit the certificate trust list to signify that this CA is trusted. For more information, see [Editing the Certificate Trust List, page 10-38](#).

Editing the Certificate Trust List

Cisco Secure ACS uses the CTL to verify the client certificates. For a CA to be trusted by Cisco Secure ACS, its certificate must be installed, and the Cisco Secure ACS administrator must explicitly configure the CA as trusted by editing the CTL. If the Cisco Secure ACS server certificate is replaced, the CTL is erased; you must configure the CTL explicitly each time you install or replace a Cisco Secure ACS server certificate.



Note The single exception to the requirement that a CA must be explicitly signified as trustworthy occurs when the clients and Cisco Secure ACS are getting their certificates from the same CA. You do not need to add this CA to the CTL because Cisco Secure ACS automatically trusts the CA that issued its certificate.

How you edit your CTL determines the type of trust model you have. Many use a restricted trust model wherein very few, privately controlled CAs are trusted. This model provides the highest level of security but restricts adaptability and scalability. The alternative, an open trust model, allows for more CAs or public CAs. This open trust model trades increased security for greater adaptability and scalability.

We recommend that you fully understand the implications of your trust model before editing the CTL in Cisco Secure ACS.

Use this procedure to configure CAs on your CTL as trusted or not trusted. Before a CA can be configured as trusted on the CTL, you must have added the CA to the local certificate storage; for more information, see [Adding a Certificate Authority Certificate, page 10-37](#). If a user's certificate is from a CA that you have not specifically configured Cisco Secure ACS to trust, authentication fails.

To edit the CTL, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Cisco Secure ACS Certificate Setup**.

Step 3 Click **Edit Certificate Trust List**.

The Edit the Certificate Trust List (CTL) table appears.



Warning

Adding a public CA, which you do not control, to your CTL, may reduce your system security.

Step 4 To configure a CA on your CTL as trusted, select the corresponding check box.



Tip

You can select, or deselect, as many CAs as you want. Deselecting a CA's check box configures the CA as not trusted.

Step 5 Click **Submit**.

Cisco Secure ACS configures the specified CA (or CAs) as trusted or not trusted in accordance with selecting or deselecting check boxes.

Managing Certificate Revocation Lists

Certificate revocation lists (CRLs) are the means by which Cisco Secure ACS determines that the certificates employed by users seeking authentication are still valid, according to the CA that issued them.

This section contains the following topics:

- [About Certificate Revocation Lists, page 10-40](#)
- [Certificate Revocation List Configuration Options, page 10-41](#)
- [Adding a Certificate Revocation List Issuer, page 10-42](#)
- [Editing a Certificate Revocation List Issuer, page 10-44](#)
- [Deleting a Certificate Revocation List Issuer, page 10-44](#)

About Certificate Revocation Lists

When a digital certificate is issued, you generally expect it to remain valid throughout its predetermined period of validity. However, various circumstances may call for invalidating the certificate earlier than expected. Such circumstances might include compromise or suspected compromise of the corresponding private key, or a change in the CAs issuance program. Under such circumstances, a CRL provides the mechanism by which the CA revokes the legitimacy of a certificate and calls for its managed replacement.

Cisco Secure ACS performs certificate revocation using the X.509 CRL profile. A CRL is a signed and time-stamped data structure issued by a CA (or CRL issuer) and made freely available in a public repository (for example, in an LDAP server). Details on the operation of the X.509 CRL profile are contained in RFC3280.

CRL functionality in Cisco Secure ACS includes the following:

- **Trusted publishers and repositories configuration**—In the Cisco Secure ACS HTML interface, you can view and configure CRL issuers and their CRL Distribution Points (CDPs) and periods.
- **Retrieval of CRLs from a CDP**—Using a transport protocol (LDAP or HTTP), Cisco Secure ACS is configured to periodically retrieve CRLs for each CA you configure. These CRLs are stored for use during EAP-TLS authentication. Note that there is no timestamp mechanism; Cisco Secure ACS waits for a specified period of time and then automatically downloads

the CRL. If the new CRL differs from the existing CRL, the new version is saved and added to the local cache. CRL retrievals appear in the log for the CSAuth service only when you have configured the level of detail in service logs to “full”. The status, date, and time of the last retrieval is shown on the Certificate Revocation List Issuer edit page of the Cisco Secure ACS HTML interface.



Note Automatic CRL retrieval scheduling only functions if EAP-TLS is enabled.

- **Verification of certificate status**—During EAP-TLS authentication, Cisco Secure ACS checks the certificate presented by the user against the corresponding CRL issued by the CA of the user’s certificate. If, according to the CRL currently stored by Cisco Secure ACS, the certificate has been revoked, authentication fails.

CRL issuers can only be added in association with trusted CAs (that is, CAs on the CTL). If you install a new server certificate for Cisco Secure ACS, your CTL is cleared of all trust relationships. While you must reestablish CAs on the CTL, the associated CRLs that you previously configured remain in place and do not have to be reconfigured.

Certificate Revocation List Configuration Options

The Certificate Revocation List Issuers edit page contains the following configuration options:

- **Name**—A name you give this CRL issuer.
- **Description**—A description you give this CRL issuer.
- **Issuer’s Certificate**—The CA certificate to be used when verifying the issuer’s signature over the CRL data. This list is derived from the contents of your configured CTL.
- **CRL Distribution URL**—The URL you enter that specifies the URL that Cisco Secure ACS should use to retrieve the CRL. You can specify a URL that uses HTTP or LDAP. Be sure you specify a URL for the CRL corresponding to the CA you selected from the Issuer’s Certificate list. Alternatively, you could specify the URL for the file itself; but this is only necessary in the case where the repository URL lists multiple files.

- **Retrieve CRL every**—The quantity and period of time that Cisco Secure ACS should wait between retrieving a CRL. For example 10 Days or 2 Months.
- **Retrieve on “Submit”**—Selecting this option causes Cisco Secure ACS to immediately attempt to contact the distribution URL and obtain the current CRL when the new CRL request page is submitted for processing. We recommend that you select this option when first obtaining a CRL to ensure that the CRL is obtained successfully.

The Certificate Revocation List Issuers edit page also contains a line, at the bottom of the table, titled Last Retrieve date:. This entry lists the status and the date and time of the last CRL retrieval or retrieval attempt.

Adding a Certificate Revocation List Issuer

Before You Begin

Before adding a CRL issuer to Cisco Secure ACS, you should ensure that you have listed the corresponding CA on the system’s CTL, and you have determined the URL of the CRL distribution repository for the appropriate issuer and class of certificate. For the automatic CRL retrieval function to operate, ensure that you have enabled EAP-TLS.

To add a certificate revocation list issuer to Cisco Secure ACS, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **ACS Certificate Setup**.
 - Step 3** Click **Certificate Revocation Lists**.
Cisco Secure ACS displays the CRL Issuers edit page.
 - Step 4** Click **Add**.
 - Step 5** In the Name box, type a name for this CRL issuer.
 - Step 6** In the Description box, type a description for this CRL issuer.
 - Step 7** In the Issuer’s Certificate box, use the drop-down arrow to select from the list the CA certificate associated with this CRL issuer.

**Tip**

Only CRL Issuers that are listed on the CTL are listed as possible selections. That is, you must list an entity as trusted on the CTL before you can select their Issuer's Certificate.

Step 8 In the CRL Distribution URL box, type the URL for CRL distribution repository.

**Tip**

The URL must specify the CRL itself when the repository contains multiple files.

Step 9 In the Retrieve CRL every box, type the quantity and period of time that Cisco Secure ACS should wait between retrieving a CRL.

Step 10 Select the **Retrieve on “Submit”** option to have Cisco Secure ACS attempt to obtain the current CRL when the page is submitted for processing.

**Tip**

Selecting the Retrieve on “Submit” option is recommended. If Cisco Secure ACS cannot obtain the CRL from the distribution repository you listed, it displays the following error message: `Failed to retrieve CRL. Verify the CRL Distribution URL.`

Step 11 Click **Submit**.

The specified CRL is added to Cisco Secure ACS (or is scheduled to be added if the Retrieve on “Submit” option was not selected).

**Tip**

You can refer to the Last Retrieve date: box to see the status, date, and time of the last retrieval attempt.

Editing a Certificate Revocation List Issuer

To edit a certificate revocation list issuer, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Certificate Revocation Lists**.

Cisco Secure ACS displays the CRL Issuers edit page.

Step 4 Click the name of the CRL issuer you want to edit.

The system displays the details of the CRL issuer that you chose.

Step 5 Edit the information and settings you want to change.

Step 6 Click **Submit**.

The corresponding CRL is changed in Cisco Secure ACS to that of the edited issuer (or is scheduled to be changed if the Retrieve on “Submit” option was not selected).



Tip You can refer to the **Last Retrieve date:** box to see the status, date, and time of the last CRL retrieval attempt.

Deleting a Certificate Revocation List Issuer

To delete a certificate revocation list issuer, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Certificate Revocation Lists**.

Cisco Secure ACS displays the CRL Issuers edit page.

Step 4 Click the name of the CRL issuer you want to delete.

The system displays the details of the CRL issuer that you selected.

Step 5 Click **Delete**.

The specified CRL issuer, and all CRLs from that issuer, is deleted from Cisco Secure ACS.

Generating a Certificate Signing Request

You can use Cisco Secure ACS to generate a certificate signing request (CSR). After you generate a CSR, you can submit it to a CA to obtain your certificate. You perform this procedure to generate the CSR for future use with a certificate enrollment tool.

**Note**

If you already have a server certificate, you do not need to use this portion of the ACS Certificate Setup page.

To generate a certificate signing request, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup** and then click **Generate Certificate Signing Request**.

Cisco Secure ACS displays the Generate Certificate Signing Request page.

Step 3 In the Certificate subject box, type values for the certificate fields required by the CA you want to submit the CSR to. A CN field is mandatory. The format is:

field=value, field=value, . . .

where *field* is the field name, such as CN, and *value* is the applicable value for the field, such as acs01primary. You can type a maximum of 256 characters in the “Certificate subject” box. Separate multiple values with commas. For example:

```
CN=acs01primary, O=WestCoast, C=US, S=California
```

The following table defines the valid fields that you can include in the “Certificate subject” box.

Field	Field Name	Min. Length	Max. Length	Required?
CN	commonName	1	64	Yes
OU	organizationalUnitName	—	—	No
O	organizationName	—	—	No
S	stateOrProvinceName	—	—	No
C	countryName	2	2	No
E	emailAddress	0	40	No
L	localityName	—	—	No

- Step 4** In the Private key file box, type the full directory path and name of the file in which the private key is saved, for example, `c:\privateKeyFile.pem`.
- Step 5** In the Private key password box, type the private key password (that you have invented).
- Step 6** In the Retype private key password box, retype the private key password.
- Step 7** From the Key length list, select the length of the key to be used.



Tip The choices for Key length are 512 or 1024 bits. The default and more secure choice is 1024 bits.

- Step 8** From the Digest to sign with list, select the digest (or hashing algorithm). The choices for are MD2, MD5, SHA, and SHA1. The default is SHA1.
- Step 9** Click **Submit**.
Cisco Secure ACS displays a CSR on the right side of the browser.
- Step 10** Submit the CSR to the CA of your choice.
After you receive the certificate from the CA, you can perform the steps in [Installing a Cisco Secure ACS Server Certificate, page 10-35](#).

Using Self-Signed Certificates

You can use Cisco Secure ACS to generate a self-signed digital certificate to be used for PEAP authentication protocol or for HTTPS support of Cisco Secure ACS administration. This capability supports TLS/SSL protocols and technologies without the requirement of interacting with a CA.

This section contains the following topics:

- [About Self-Signed Certificates, page 10-47](#)
- [Self-Signed Certificate Configuration Options, page 10-48](#)
- [Generating a Self-Signed Certificate, page 10-49](#)

About Self-Signed Certificates

Cisco Secure ACS supports TLS/SSL-related protocols, including PEAP and HTTPS, that require the use of digital certificates. Employing self-signed certificates is a way for administrators to meet this requirement without having to interact with a certification authority (CA) to obtain and install the certificate for the Cisco Secure ACS. The self-signed certificate feature in Cisco Secure ACS allows the administrator to generate the self-signed digital certificate and use it for PEAP authentication protocol or for HTTPS support in web administration service.

Other than the lack of interaction with a CA to obtain the certificate, installing a self-signed certificate requires exactly the same actions as any other digital certificate. Although Cisco Secure ACS does not support the replication of self-signed certificates, you can export a certificate for use on more than one Cisco Secure ACS. To do this, you copy the certificate file (.cer format) and the corresponding private key file (.pvk format) to another Cisco Secure ACS where you then install the certificate in the standard manner. For information on installing certificates, see [Installing a Cisco Secure ACS Server Certificate, page 10-35](#).

To ensure that a self-signed certificate interoperates with the client, refer to your client documentation. You may find that you must import the self-signed server certificate as a CA certificate on your particular client.

Self-Signed Certificate Configuration Options

The Generate Self-Signed Certificate edit page contains the following mandatory configuration fields:

- **Certificate subject**—The subject for the certificate, prefixed with “cn=”. We recommend using the Cisco Secure ACS name. For example, “cn=ACS11”. The Certificate subject field here can contain a number of content entries as comma-separated items; these include:
 - **CN**—common name (the mandatory entry)
 - **OU**—organizational unit name
 - **O**—organization name
 - **S**—state or province
 - **E**—email address
 - **L**—locality name

For example, the Certificate subject field might appear as follows:

```
cn=ACS 11, O=Acme Enterprises, E=admin@acme.com
```

- **Certificate file**—The full path and filename for the certificate file that you want to generate. For example, “c:\acs_server_cert\acs_server_cert.cer”. When you submit this page, Cisco Secure ACS creates the certificate file using the location and filename you specify.
- **Private key file**—The full path and filename for the private key file you want to generate. For example, “c:\acs_server_cert\acs_server_cert.pvk”. When you submit this page, Cisco Secure ACS creates the private key file using the location and filename you specify.
- **Private key password**—A private key password for the certificate. Minimum length for the private key password is 4 characters, and the maximum length is 64 characters.
- **Retype private key password**—The private key password typed again, to ensure accuracy.
- **Key length**—Select the key length from the choices listed. The choices include 512 bits, 1024 bits, and 2048 bits.

- **Digest to sign with**—Select the hash digest to be used to encrypt the key from the choices listed. The choices include SHA1, SHA, MD2, and MD5.
- **Install generated certificate**—Select this check box if you want Cisco Secure ACS to install the self-signed certificate that it generates when you click Submit. If you employ this option, Cisco Secure ACS services must be restarted after you submit the page for the new settings to be adopted. If you do not select this option, the certificate file and private key file are generated and saved, but are not installed into local machine storage.

Generating a Self-Signed Certificate

All fields on the Generate Self-Signed Certificate page are mandatory. For information on the fields' contents, see [Self-Signed Certificate Configuration Options, page 10-48](#).

To generate a self-signed certificate, follow these steps:

-
- Step 1** In the navigation bar, click **System Configuration**.
 - Step 2** Click **ACS Certificate Setup**.
 - Step 3** Click **Generate Self-Signed Certificate**.
Cisco Secure ACS displays the Generate Self-Signed Certificate edit page.
 - Step 4** In the Certificate subject box, type the certificate subject in the form `cn=XXXX`. You can enter additional information here, for information see [Self-Signed Certificate Configuration Options, page 10-48](#).
 - Step 5** In the Certificate file box, type the full path and file name for the certificate file.
 - Step 6** In the Private key file box, type the full path and file name for the private key file.
 - Step 7** In the Private key password box, type the private key password.
 - Step 8** In the Retype private key password box, retype the private key password.
 - Step 9** In the Key length box, select the key length.
 - Step 10** In the Digest to sign with box, select the hash digest to be used to encrypt the key.

Step 11 To install the self-signed certificate when you submit the page, select the **Install generated certificate** option.



Note If you use the Install generated certificate option you must restart Cisco Secure ACS services after submitting this form to adopt the new settings.



Tip If you do not select the Install generated certificate option, the certificate file and private key file are generated and saved when you click Submit in the next step, but are not installed into local machine storage.

Step 12 Click **Submit**.

The specified certificate and private key files are generated and stored, as specified. The certificate becomes operational, if you also selected the Install generated certificate option, only after you restart Cisco Secure ACS services.

Updating or Replacing a Cisco Secure ACS Certificate

Use this procedure to update or replace an existing Cisco Secure ACS certificate that is out-of-date or out-of-order.



Caution This procedure eliminates your existing Cisco Secure ACS certificate and erases your CTL configuration.

To install a new ACS certificate, follow these steps:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **ACS Certificate Setup**.

Cisco Secure ACS displays the Installed Certificate Information table on the ACS Certificate Setup page.



Note If your Cisco Secure ACS has not already been enrolled with a certificate, you do not see the Installed Certificate Information table. Rather, you see the Install new certificate table. If this is the case, you can proceed to Step 5.

Step 3 Click **Enroll New Certificate**.

A confirmation dialog box appears.

Step 4 To confirm that you intend to enroll a new certificate, click **OK**.

The existing Cisco Secure ACS certificate is removed and your CTL configuration is erased.

Step 5 You can now install the replacement certificate in the same manner as an original certificate. For detailed steps, see [Installing a Cisco Secure ACS Server Certificate, page 10-35](#).
