



Cisco Secure Access Control Server Deployment Guide

Contents

Introduction	4
Cisco Secure ACS	5
RADIUS	5
TACACS+	6
Deployment Planning.....	8
Databases	9
Local Database	9
Windows Active Directory.....	9
Generic LDAP	10
Open Database Connectivity.....	10
RSA Token Card Servers	11
RADIUS-Enabled Token Servers	11
Remote AAA Server (Proxy).....	11
Unknown User Policy	12
Authentication Protocols.....	13
EAP	13
Password-Based: PAP, EAP-GTC	13
Challenge-Response-Based: CHAP, MS-CHAP, EAP-MD5	14
Mutual Authentication: LEAP, PEAP, EAP-FAST, EAP-TLS	14
Certificate-Based: EAP-TLS, PEAP, EAP-FAST	15
Encrypted Tunnel: PEAP, EAP-FAST, EAP-TLS, PEAP-TLS	16
Most Secure: PEAP-TLS, EAP-FAST, EAP-TLS.....	16
Commonly Used Authentication Protocols	16
Centralized Configuration Management.....	18
Database Replication	18
Replication Timeout.....	20
Authentication Services Availability	21
Cascade Replication	23
Replication Recommendations	24
Provisioning	25
Logging Capabilities	27
Cisco Secure ACS Logs	27
Configuring Cisco Secure ACS Logs.....	27
Selecting the Correct Log Format.....	28
Cisco Secure ACS for Windows or Cisco Secure ACS Solution Engine.....	29
Performance and Scaling	29
Number of Cisco Secure ACS Systems Required	30
Network Access Policy	31
Downloadable Access Control Lists	31
VLANs	32
Timeouts.....	32
Time-of-Day Access	32
Network Access Restrictions	32
Network Access Profiles	33
General Scenarios.....	35
Dialup Access.....	35
Remote Access Using VPN	35
Wireless Network	36
LAN Network	37
Device Administration Policy	38
AAA Protocol	38
NAR.....	38
Shell Access Authorization	38

Privilege Level	38
Command Authorization	38
Cisco IOS CLI View and Cisco IOS XR Task Assignments	39
Session Timeout	39
Idle Timeout	39
Max Sessions	40
Limit User to Number of Hours of Online Time	40
Limit User to Number of Sessions	40
Time-of-Day Restrictions	40
Enable Password	40
Integration with Network Management Software	40
Logging	40
Separating Device Administration Users and General Network Users	41
Scenario: Large Network	42
Scaling	42
Deployment Plan	42
Phase One: Remote Access	42
Phase Two: Wireless Access	48
Phase Three: USA Rollout	54
Phase Four: Global Rollout	54
Conclusion	56
For More Information	58

Introduction

This document discusses planning, design, and implementation practices for deploying Cisco Secure Access Control Server (ACS) for Windows in an enterprise network. It discusses Cisco Secure ACS performance, network topology, access requirements and integration of external databases. This document also covers the difference between Cisco Secure ACS for Windows and Cisco Secure ACS Solution Engine (appliance version), where applicable. The information in this document is based on Cisco Secure ACS versions 4.0, 4.1 and 4.2.

Note: All Cisco Secure ACS configurations presented in this paper are to help the user design their AAA infrastructure. Please refer to the Cisco Secure ACS Users Guide for complete configuration information.

Cisco Secure ACS

Cisco Secure ACS is an authentication, authorization, and accounting (AAA) access control server. Cisco Secure ACS provides access control to network access servers (NAS) through AAA, an architectural framework for configuring a set of three independent security functions consistently. AAA provides a modular framework for performing the following services:

- **Authentication:** Provides a method for identifying users, including login and password dialog, challenge and response, messaging support, and depending on the security protocol selected, encryption.
- **Authorization:** Provides a method for implementing the access control policy, including one-time authorization or authorization for each service, per-user account list and profile, support for user groups, and support of IP, Internetwork Packet Exchange (IPX), AppleTalk Remote Access (ARA), and Telnet.
- **Accounting:** Provides a method for collecting and sending security server information used for billing, auditing, and reporting, such as user identities, start and stop time, executed commands (such as Point-to-Point Protocol [PPP]), number of packets, and number of bytes.

Cisco Secure ACS uses two distinct protocols for AAA services: Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS+).

RADIUS

RADIUS provides authentication and authorization in a single step. The RADIUS server returns a single response with authentication approval status and any related access information available. Four types of RADIUS packets are used for authentication.

Access-Request Packet

The RADIUS client sends the Access-Request packet to a RADIUS server. The RADIUS server uses the information to determine whether a user is allowed network access.

To authenticate a user, a RADIUS client must transmit a packet with the Code field set to 1 (Access-Request). On receipt of an Access-Request from a valid RADIUS client, the RADIUS server must send an appropriate reply.

An Access-Request contains the following attributes:

- User-Name.
- User-Password or CHAP-Password (An Access-Request must not contain both a User-Password and a CHAP-Password).
- NAS-IP-Address or NAS-Identifier or both.
- NAS-Port or NAS-Port-Type or both, unless the type of access being requested does not involve a port or the RADIUS client does not distinguish among its ports.

An Access-Request may contain additional attributes as a hint to the server, but the server is not required to honor the hint.

RADIUS uses a method based on the RSA Message Digest Algorithm MD5 to hide a User-Password when it is present.

Access-Accept Packet

The RADIUS server sends Access-Accept packets, and provides specific configuration information necessary to begin delivery of service to the user. If all attribute values received in an Access-Request are acceptable, the RADIUS server must transmit a packet with the Code field set to 2 (Access-Accept).

On receipt of an Access-Accept packet, the Identifier field is matched with a pending Access-Request. The Response Authenticator field must contain the correct response for the pending Access-Request. The RADIUS client discards invalid packets.

Access-Reject Packet

If any of the attribute values received in an Access-Request are not acceptable, the RADIUS server must send a packet with the Code field set to 3 (Access-Reject). The RADIUS server may include one or more Reply-Message attributes with a text message which the RADIUS client may display to the user.

Access-Challenge Packet

If the RADIUS server wants to send the user a challenge requiring a response, the RADIUS server must respond to the Access-Request by transmitting a packet with the Code field set to 11 (Access-Challenge). The Access-Challenge is only used with Extensible Authentication Protocol (EAP). Otherwise, the RADIUS client treats the receipt of an Access-Challenge as an Access-Reject.

For details on EAP, see the “Authentication Protocols” section.

To support new features which vendors add to their network access servers and other network access equipment, RADIUS allows for the definition of vendor-specific attributes (VSA) in addition to the base set of “dictionary” attributes defined by the Internet Engineering Task Force (IETF). VSAs are derived from IETF attribute 26.

Following is a VSA structure:

```

0           8           16           24           32
+-----+-----+-----+-----+
| Type   | Length | Vendor-Id   |
+-----+-----+-----+-----+
| Vendor-Id (cont) | Vndr-Typ | Vndr-Len |
+-----+-----+-----+-----+
| Vendor Data ...
+-----+-----+-----+-----+
```

The text of the IETF proposed standards is available at:

- <http://www.faqs.org/rfcs/rfc2865.html>
- <http://www.faqs.org/rfcs/rfc2866.html>
- <http://www.faqs.org/rfcs/rfc2868.html>

TACACS+

TACACS+ is an AAA protocol developed by Cisco. TACACS+ separates the authentication, authorization, and accounting steps. This architecture allows for separate authentication solutions while still using TACACS+ for authorization and accounting. For example, it is possible to use the Kerberos Protocol for authentication and TACACS+ for authorization and accounting. After an AAA

client passes authentication through a Kerberos server, the AAA client requests authorization information from a TACACS+ server without the necessity to re-authenticate the AAA client by using the TACACS+ authentication mechanism.

TACACS+ authentication has three packet types: Start, Continue and Reply. Start and Continue are always sent by the TACACS+ client and Reply is always sent by the TACACS+ server.

Authentication begins when the TACACS+ client sends a Start message to the TACACS+ server. The Start message describes the type of authentication to be performed, and may contain the username and some authentication data. The TACACS+ client sends the Start packet only as either the first message in a TACACS+ authentication session, or the packet immediately following a restart. The TACACS+ client may send a restart in a Reply packet. A Start packet always has "seq_no" equal to 1.

In response to a Start packet, the TACACS+ server sends a Reply. The Reply message indicates whether the authentication is done, or whether it should continue. If the Reply indicates that authentication should continue, then it will also indicate what new information is required. The TACACS+ client will return the information in a Continue message.

The TACACS+ server must always send a Reply to both the Start and the Continue messages, the only exception being if the TACACS+ client indicates an abort in the Continue, in which case the session is immediately aborted.

TACACS+ also has the ability to support custom attributes which are similar to RADIUS VSAs.

The text of the TACACS+ proposed standards is available at <http://tools.ietf.org/html/draft-grant-tacacs-02>

An in-depth comparison of TACACS+ and RADIUS is located at <http://www.cisco.com/warp/public/480/10.html>

As a rule, Cisco recommends RADIUS for providing network access, such as with 802.1X or virtual private networks (VPNs), because it is a standard; and TACACS+ for network device access, because of its ability to support more extensive capabilities such as command filtering.

Deployment Planning

This section of the document covers various aspects of Cisco Secure ACS that influences its deployment in the network. These aspects include:

- **Databases:** Databases supported and how they affect the deployment decision.
- **Authentication Protocols:** Authentication protocols, including password types, and how they relate with each other.
- **Cisco Secure ACS for Windows or Cisco Secure ACS Solution Engine:** How to decide which type will work best in a given environment.
- **Centralized Management:** How to centrally manage a number of Cisco Secure ACS systems.
- **Logging:** Types of log, how to configure them, and how to choose the correct storage format.
- **Performance and Scaling:** Taking all the other aspects into consideration, how to decide the number of Cisco Secure ACS systems to deploy and where to deploy them.

Some of these items will be pre-determined while others will require the deployment team to make a decision based on various related factors. For example, the organization may already have a Lightweight Directory Access Protocol (LDAP) server in place for user data. This limits the type of passwords available, which will, in turn, limit the authentication protocols available.

Databases

The database is one of the most influential factors in making deployment decisions for Cisco Secure ACS. The size of the user base, distribution of users throughout the network, access requirements, and type of database employed all contribute toward how the Cisco Secure ACS is used. The type of database may influence the password type, which will also limit the availability of authentication protocols. The database type may also control the format of Cisco Secure ACS that can be used.

Local Database

The Cisco Secure ACS local database provides full feature support. The local database provides the maximum speed for authentication. It may have regional scalability problems, which can be minimized using database replication. However, replication requires a primary/secondary relationship between Cisco Secure ACS systems. Replication keeps AAA servers synchronized by copying selected configuration items from a primary Cisco Secure ACS installation over the configuration of a secondary Cisco Secure ACS installation, completely replacing those configuration items on the secondary. This restricts maintenance of user accounts to the primary Cisco Secure ACS installation. Another drawback is that if an organization has an existing database for users, the organization must maintain both databases separately.

Windows Active Directory

In organizations in which a substantial Windows Active Directory (AD) user database already exists, Cisco Secure ACS can take advantage of the work already invested in building the database without any additional input. This eliminates the need for separate databases. When the NAS presents the username to Cisco Secure ACS, Cisco Secure ACS searches its database to locate a match. If Cisco Secure ACS does not find a match and Cisco Secure ACS is configured to check the Windows AD user database, the username and password are forwarded to Windows AD for authentication against those in the Windows AD user database. Upon match confirmation, the username (but not the password) is stored in the Cisco Secure ACS user database. Authentication requests in future will authenticate much faster because Cisco Secure ACS goes directly to the Windows AD user database for authentication. Group mapping allows greater flexibility of user privileges. Cisco Secure ACS assigns privileges from the user's group to the just authenticated user.

Domain Controller (DC) trust relationships extend the number of users available for authentication by Cisco Secure ACS. Timeouts may be a problem using DC trust relationships because of the sometimes-present latency in NT networking. Another problem is that authenticating against the Windows AD user database does not allow storage of third-party passwords (for example, Challenge Handshake Authentication Protocol [CHAP]).

Generic LDAP

Cisco Secure ACS supports authentication of users against records kept in a directory server using generic LDAP. Cisco Secure ACS interacts with the most popular directory servers, including Novell and Netscape. You can use Password Authentication Protocol (PAP) and clear text passwords when authenticating against the directory server. These services do not support CHAP or Microsoft CHAP (MS-CHAP). This may be an issue when trying to use network devices that are limited to using one of these protocols (for example, Lightweight Extended Authentication Protocol [LEAP]). Group mappings are available, as with Windows 2000 Server or Windows Server 2003.

A white paper on LDAP authentication can be accessed at

http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_white_paper09186a0080092566.shtml

Open Database Connectivity

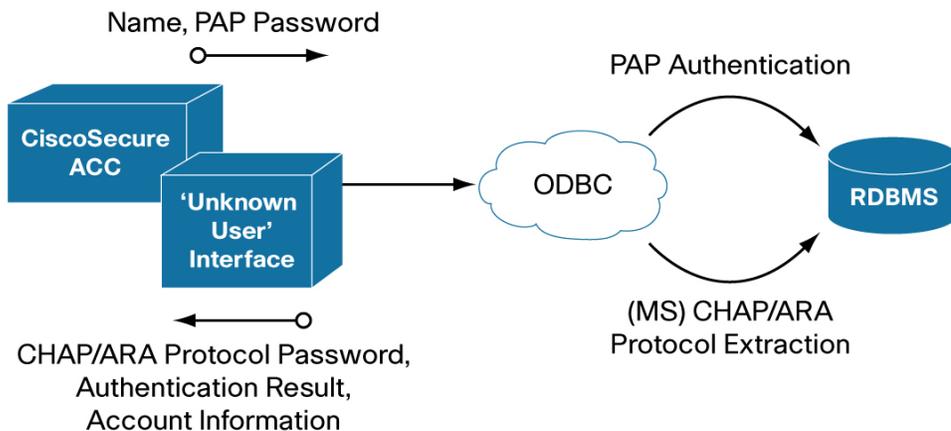
Cisco Secure ACS supports authentication against a relational database that is compliant with Open Database Connectivity (ODBC). This enables use of existing user records. ODBC is a standardized application-programming interface (API) that follows the specifications of the Structured Query Language (SQL) Access Group. The Windows ODBC feature enables you to create a Data Source Name (DSN) which specifies the database and other important parameters necessary for communicating with the database. Cisco Secure ACS passes the user information to the relational database through the ODBC connection. The relational database must have a stored procedure that queries the appropriate tables and returns to the Cisco Secure ACS. If the returned values indicate that the username and password provided are valid, Cisco Secure ACS grants the user access. Otherwise, Cisco Secure ACS denies the user access (See Figure 1). Because of the ODBC feature that allows password extraction, ODBC can authenticate clear text, PAP, CHAP, MS-CHAP, and ARA Protocol passwords.

Note that the Cisco Secure ACS Solution Engine cannot use ODBC authentication. This is because the Cisco Secure ACS Solution Engine is a closed appliance and the required ODBC agent cannot be loaded.

A complete description of configuring an ODBC database for authentication is located in the "User Guide for Cisco Secure Access Control Server 4.1", located at:

http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.1/user/UsrDb.html#wpmkr462612

Figure 1. ODBC External Database Authentication



RSA Token Card Servers

Cisco Secure ACS for Windows supports only the RSA token card server natively. See note below. Cisco Secure ACS for Windows supports mapping users authenticated by an RSA token server to a single group. Cisco Secure ACS for Windows supports PPP (ISDN and Async) and Telnet for RSA SecurID token servers by acting as a token card client to the RSA SecurID token server. To use this client, you must install the RSA token card agent software on the computer that is running Cisco Secure ACS for Windows. Cisco Secure ACS for Windows supports the RSA SecurID token server custom interface for authentication of users. You can create only one RSA SecurID configuration within Cisco Secure ACS for Windows. Many networks require a token card for one-time password (OTP) authentication. This method is very secure but has several caveats. First, you cannot combine it with encrypted password protocols (CHAP and MS-CHAP). There is no need because of the nature of OTP. However, this causes a problem, as with LDAP, because of trying to use network devices that are limited to using one of these protocols (such as LEAP). Another problem is that group mappings are not available. The token card server should be located reasonably close to the Cisco Secure ACS installation because of possible network latency issues.

Note: The Cisco Secure ACS Solution Engine prior to version 4.2 does not support native RSA SecurID. To support token server capabilities with Cisco Secure ACS Solution Engine prior to version 4.2, you must use the RADIUS-enabled token server option. The Cisco Secure ACS Solution Engine running Cisco Secure ACS 4.2 will have native RSA support and the information above will be applicable.

RADIUS-Enabled Token Servers

Cisco Secure ACS supports token servers by using the built-in RADIUS server found in the token server. Rather than using a vendor-proprietary API, Cisco Secure ACS sends standard RADIUS authentication requests to the RADIUS authentication port on the token server. This feature enables Cisco Secure ACS to support any IETF RFC 2865-compliant token server. You can create multiple instances of RADIUS token servers. Cisco Secure ACS provides a means for specifying a user group assignment in the RADIUS response from the RADIUS-enabled token server. Group specification always takes precedence over group mapping. Cisco Secure ACS also supports mapping users authenticated by a RADIUS-enabled token server to a single group. Group mapping only occurs if group specification does not occur. You can use this feature as a RADIUS-only authentication as well.

Remote AAA Server (Proxy)

Proxy enables Cisco Secure ACS to automatically forward an authentication request from a NAS to another AAA server.

After successful authentication of the request, the remote AAA server passes the authorization privileges for the user back to the forwarding Cisco Secure ACS. Cisco Secure ACS then passes the user's profile information back to the NAS. This powerful tool can expand the use of Cisco Secure ACS by minimizing the number of users configured in the local database. Another advantage is that the organization is not limited to Cisco Secure ACS. You can use other vendors' AAA products.

One disadvantage, however, is that a user must supply his or her name along with a previously defined string (for example, "mary.smith@corporate.com" where "@corporate.com" is a character string defined in the server's Distribution Table as being associated with another specific Cisco Secure ACS). Another disadvantage is that it creates a problem when performing NAS filtering.

You must use the NAS IP address of the forwarding Cisco Secure ACS rather than the IP address of the NAS generating the request.

Unknown User Policy

The Unknown User Policy is a form of authentication forwarding. In essence, this feature is an extra step in the authentication process. If a username does not exist in the Cisco Secure ACS internal database, Cisco Secure ACS forwards the authentication request of an incoming username and password to external databases with which it is configured to communicate. The external database must support the authentication protocol used in the authentication request.

The Unknown User Policy enables Cisco Secure ACS to use a variety of external databases to attempt authentication of unknown users. This feature provides the foundation for a basic single sign-on capability by integrating network and host-level access control. Because external user databases handle the incoming authentication requests, there is no need to maintain the credentials of users (such as passwords) within Cisco Secure ACS. This eliminates the necessity of entering every user multiple times and prevents data entry errors inherent in manual procedures.

Unknown Users are users who do not have a user account in the Cisco Secure ACS internal database. This means that the user has not received authentication from Cisco Secure ACS or that the user account was deleted. If the Unknown User Policy is configured in Cisco Secure ACS, Cisco Secure ACS attempts to authenticate these users with external user databases.

Discovered Users are users whose accounts Cisco Secure ACS creates in the Cisco Secure ACS internal database after successful authentication using the Unknown User Policy. All discovered users were unknown users at one point. When Cisco Secure ACS creates a discovered user, the user account contains only the username, a Password Authentication list setting that reflects the database that provided authentication for the user, and a Group to which the user is assigned by the list setting of Mapped By External Authenticator, which enables group mapping.

Note: Cisco Secure ACS does not import credentials (such as passwords, certificates and so on) for a discovered user.

The authentication process for discovered users is identical to the authentication process for known users who are authenticated with external user databases.

Authentication Protocols

Cisco Secure ACS supports a number of authentication options, including the authentication protocol and the password type. This section discusses the various authentication protocols that Cisco Secure ACS supports along with the associated password types.

EAP

EAP is an IETF standard described in RFC 3748. EAP provides an infrastructure for network access clients and authentication servers to host plug-in modules for current and future authentication methods and technologies. The EAP designers originally created EAP as an extension to PPP to allow for the development of arbitrary network access authentication methods.

With PPP authentication, the authentication protocol is a fixed series of messages sent in a specific order. With EAP, you do not select the specific authentication mechanism during the link establishment phase of the PPP connection. The PPP peers negotiate to perform EAP during the connection authentication phase. When the peer reaches the connection authentication phase, the peers negotiate the use of a specific EAP authentication scheme known as an EAP method. Once the peers agree on the EAP method, EAP allows for an open-ended exchange of messages between the access client and the authenticating server that can vary based on the parameters of the connection.

Password-Based: PAP, EAP-GTC

Password-based authentication has been the mainstay of computer security for many years. The use of clear text passwords, though cost-effective, does have inherent security risks, including capture and spoofing. These risks can be mitigated by encrypting the password using methods such as RADIUS MD5 password encryption

PAP

RFC 1334 describes the PAP password as part of the PPP authentication protocol. PAP is essentially a clear text password that provides a simple method for the peer to establish its identity using a two-way handshake. PAP is not a strong authentication method. The NAS sends passwords over the PPP connection “in the clear” and there is no protection from playback or repeated trial and error attacks. This issue can be mitigated in several ways. First, it is difficult to “listen” on a PPP connection, which is generally a modem connection or other electronic link. Also, the communication between the AAA client and Cisco Secure ACS encrypts the password to some level through either the RADIUS or TACACS+ protocol.

EAP-GTC

Cisco created PEAPv1/EAP-GTC to allow the use of a general purpose inner authentication protocol. RFC 3748 defines Extensible Authentication Protocol-Generic Token Card (EAP-GTC). It carries a text challenge from the authentication server, and a reply back from the supplicant. EAP-GTC does not protect the authentication data in any way but depends on the encrypted tunnel created by Protected Extensible Authentication Protocol (PEAP).

Challenge-Response-Based: CHAP, MS-CHAP, EAP-MD5

Challenge-response-based passwords provide additional security to clear text passwords by hashing the password at both the client and server sides. This one-way encryption of the password provides additional security from casual sniffing of the network.

CHAP/MS-CHAP

CHAP can be used to periodically verify the identity of the peer using a three-way handshake. This is done upon initial link establishment, and may be repeated anytime after the link has been established.

Following steps are involved in the authentication process:

1. After the Link Establishment phase is complete, the authenticator sends a “challenge” message to the peer.
2. The peer responds with a value calculated using a “one-way hash” function.
3. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication. Otherwise, the authenticator terminates the connection.
4. At random intervals, the authenticator sends a new challenge to the peer, and repeats Steps 1 to 3.

MS-CHAPv2 provides mutual authentication between peers by piggybacking a peer challenge on the Response packet and an authenticator response on the Success packet.

EAP-MD5

EAP-MD5 is another IETF open standard as defined in RFC 3748. EAP-MD5 provides a one-way authentication mechanism using a hashed password. EAP-MD5 uses password-based authentication through a challenge/response method directly over the connection medium, and because of this, is prone to offline dictionary attacks, particularly in a wireless environment. Moreover, EAP-MD5 does not provide mutual authentication, which means the client could connect to an unauthorized wireless access point (AP). EAP-MD5 is also unable to generate keying material for use as encryption keys, resulting in the dependency on manual key changes. EAP-MD5 is now widely regarded as unsuitable as a wireless authentication method because of these limitations.

Mutual Authentication: LEAP, PEAP, EAP-FAST, EAP-TLS

Mutual authentication or two-way authentication refers to two parties authenticating each other suitably. In technology terms, it refers to a client or user authenticating themselves to a server and that server authenticating itself to the user in such a way as to assure both of the other’s identity. Typically, this does not require user interaction.

LEAP

Cisco introduced LEAP because of the absence of suitable standards with the original 802.11 specification. LEAP leverages the MS-CHAP password hashing for security. LEAP offers stronger authentication than EAP-MD5, but still lacks Transport Layer Security (TLS) support for end-to-end protection. This means that the authentication credentials are susceptible to offline dictionary attacks. In addition, because the LEAP client does not authenticate the server’s identity, this can inhibit its ability to distinguish between a wireless AP authorized by a corporate IT administrator and a rogue wireless AP on the same corporate network.

PEAP

Cisco, Microsoft, and RSA Security developed PEAP. PEAP is a method to securely transmit authentication information, including passwords, over wired or wireless networks. PEAP uses only server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server, which protects the ensuing exchange of authentication information from casual inspection.

There are three PEAP sub-types certified for the updated WPA and WPA2 standard. They are PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC and PEAP/EAP-TLS.

PEAPv0/EAP-MSCHAPv2

PEAPv0/EAP-MSCHAPv2 is the most common form of PEAP in use due to its inclusion in the Windows operating system. The inner authentication protocol is MS-CHAPv2. After EAP-TLS, PEAPv0/EAP-MSCHAPv2 is probably the second most widely supported EAP standard in the world.

PEAPv1/EAP-GTC

Cisco, Microsoft, and RSA Security created the original PEAPv1/EAP-GTC. It allows the use of an inner authentication protocol other than MS-CHAPv2. Until recently, PEAPv1/EAP-GTC had no native Windows operating system support.

PEAP/EAP-TLS

PEAP/EAP-TLS (also known as PEAP-TLS) allows Cisco Secure ACS to authenticate clients with PEAP by using EAP-TLS as the phase-two inner method. This enables certificate-based authentication to occur within a secure tunnel, encrypting identity information. Since EAP-TLS normally relies on client-side certificates for authentication, the PEAP tunnel will protect the client's certificate content.

EAP-FAST

Cisco developed the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) to replace LEAP. RFC 4851 defines the EAP-FAST protocol. EAP-FAST works in two stages. The first stage establishes a TLS tunnel using a pre-shared key called a Protected Authentication Credential (PAC). The second has the client send user information across the tunnel for authentication. PACs are automatically refreshed when they expire as part of the EAP-FAST protocol. The authentication server does not store PACs. Rather than store a PAC for each user, the authentication server generates PACs from a "master key". EAP-FAST is provisioned automatically (Automatic or In-band Provisioning) or manually.

EAP-TLS

RFC 2716 defines EAP-TLS. EAP-TLS provides good security, because TLS uses Public Key Infrastructure (PKI) to secure communication to the RADIUS server. Even though EAP-TLS provides excellent security, the need for client-side certificates may be too high an overhead for some users.

Certificate-Based: EAP-TLS, PEAP, EAP-FAST

Client certificate is optional for PEAP and EAP-FAST.

PKI is a management system designed to administer asymmetrical cryptographic keys and public key certificates. It acts as a trusted component that guarantees the authenticity of the binding between a public key and security information, including identity, involved in securing a transaction

with public key cryptography. PKI protects information in several essential ways. It authenticates identity, validates the identity of each party in an Internet transaction, verifies integrity, ensures that the message or document the certificate “signs” has not been changed or corrupted in transit online, protects information from interception during transmission, replaces lost user IDs or passwords, authorizes transactions and ensures privacy.

Encrypted Tunnel: PEAP, EAP-FAST, EAP-TLS, PEAP-TLS

An encrypted tunnel uses a tunneling protocol which encapsulates one protocol or session inside a higher layer protocol or a protocol at the same layer. In the case of 802.1X, the encrypted tunnel encapsulates another EAP method that provides the actual user authentication. Encrypted tunnels are good for securing authentication methods that are vulnerable when not encapsulated in an encrypted tunnel.

PEAP, PEAP-TLS and EAP-TLS create encrypted tunnels using a PKI certificate.

EAP-FAST creates encrypted tunnels using PACs.

Most Secure: PEAP-TLS, EAP-FAST, EAP-TLS

Because PEAP-TLS, EAP-FAST, and EAP-TLS use encrypted tunnels and other mechanisms to secure data transferred between the client and the RADIUS server, they are the most secure methods today for authentication.

Commonly Used Authentication Protocols

Remote Access and Device Administration: OTP over PAP

Wired/Wireless Windows shops: MS-CHAP, PEAP-MS-CHAP

PKI shops: PEAP-TLS

Tables 1 to 3 show the relationship among password types, authentication types and external databases. For example, MS-CHAP password type cannot be used with the LDAP external database. As a result, neither the LEAP nor MS-PEAP authentication methods can be used because each of these authentication types exclusively depend on the MS-CHAP password.

Table 1. Password to Database Compatibility

Database	Clear Text	PAP/GTC	MS-CHAP	CHAP	Group Mapping
Cisco Secure ACS Local	Y	Y	Y	Y	N
Windows AD	Y	Y	N	Y	Y
Generic LDAP	Y	Y	N	N	Y
RDBMS (ODBC) ¹	Y	Y	Y	Y	Y
RSA Token Server (OTP) ¹	Y	Y	N	N	N
RADIUS Token Server (OTP)	Y	Y	Y ²	Y ²	Y
Remote AAA Server (proxy)	Y	Y	Y ²	Y ²	Y ²

¹ Cisco Secure ACS for Windows

² If supported by remote AAA server

Table 2. EAP to Database Compatibility

Database	LEAP	EAP-MD5	Cisco PEAP	EAP-FAST	MS-PEAP	EAP-TLS
Cisco Secure ACS Local	Y	Y	Y	Y	Y	Y
Windows AD	Y	N	Y	Y		Y
Generic LDAP	N	N	Y	Y	N	Y
RDBMS (ODBC) ¹	Y	Y	Y	Y	Y	Y
One-Time Password	N	N	Y	Y	N	N

1 Cisco Secure ACS for Windows

Table 3. Comparison of EAP Types

Features	LEAP	EAP-MD5	Cisco PEAP	EAP-FAST	MS-PEAP	EAP-TLS
Password Support	Y	Y	Y	Y	Y	N
One-Time Password Support	N	N	Y	Y	N	N
Windows Password Change	N	N	Y	Y	Y	N
Server Certificate Required	N	N	Y	N	Y	Y
Client Certificate Required	N	N	N	N	N	Y
LDAP/AD Database Support	AD only	N	Y	Y	AD only	Y
Multi-Operating System Support	Y	N	Y	Y	Y	N
Single -Sign-On for Windows	Y	N	N	Y	Y	Y

Centralized Configuration Management

When maintaining two or more Cisco Secure ACS systems in a network, which requires the servers to have the same configuration, it is helpful to centralize the configuration in one location to maintain the consistency of the configuration. This is particularly important as the number of Cisco Secure ACS systems grows. This section discusses the tools available in Cisco Secure ACS to provide centralized configuration management.

Database Replication

Cisco Secure ACS replication is used to replicate Cisco Secure ACS configuration from a primary Cisco Secure ACS system to other secondary Cisco Secure ACS systems in the network. Cisco Secure ACS replication helps by automatically copying configuration changes to other Cisco Secure ACS systems in the network. This eases configuration provisioning since most configurations can be done on a designated primary Cisco Secure ACS system. It also gives administrators the ability to maintain multiple redundant Cisco Secure ACS systems more easily, which provides for greater scaling and availability.

The following items for configuring database replication are configured in Cisco Secure ACS:

- Configuration components for replication: What is replicated
- Replication scheduling: When replication takes place
- Replication frequency: How often systems are replicated
- Replication partners: Which systems are replicated
- Secondary server configuration: How the client is to be configured
- Reports and event (error) handling: What information to include in the logs

Administrators can select which of the following configuration components to replicate (See figure 2):

- User and Group Database
- Group Database only
- Network Configuration Device tables
- Distribution Table
- Interface Configuration
- Interface Security Settings
- Password validation settings
- EAP-FAST master keys and policies
- Network Access Profiles

Note that there are two columns for replication components, Send and Receive. This permits the administrator to decide which configuration components are to be sent from the primary Cisco Secure ACS system to the secondary Cisco Secure ACS systems. This also allows the administrator to select which of the configuration components will be used on the individual secondary Cisco Secure ACS systems. For normal circumstances the selections in the primary Cisco Secure ACS system Send column and the secondary Cisco Secure ACS system Receive column should match exactly. If the primary Cisco Secure ACS system sends a configuration component that is not selected on the secondary Cisco Secure ACS system, the secondary Cisco

Secure ACS systems will simply ignore that configuration component. Conversely, if the primary Cisco Secure ACS system does not send a configuration component that is selected on the secondary Cisco Secure ACS system, the secondary Cisco Secure ACS systems will simply not attempt to use that component. This separate allows the administrator some flexibility in differentiating replication configuration components to individual secondary Cisco Secure ACS systems.

Cisco Secure ACS replication can be run manually, automatically as part of cascade replication or scheduled by either regular interval or at specific times during the week. For specific times scheduling, an administrator selects the desired day(s) of the week and specific times during each day to run replication. Administrators must select the Cisco Secure ACS systems to which they want to replicate from a list of configured Cisco Secure ACS systems. Administrators must configure the Cisco Secure ACS secondaries for replication. This includes which replication components that the secondary will accept from primary and which primaries can replicate to the secondary. See figure 2. Administrators can also configure how the replication logs are stored and managed. See figure 3. Options include local database, syslog, ODBD (Cisco Secure ACS for Windows only) and remote agent (Cisco Secure Solution Engine only).

Cisco Secure ACS replication has the following caveats:

- Cisco Secure ACS replication will completely overwrite any component designated for replication to or from another Cisco Secure ACS replication partner in favor of the replicated component; that is, the replication may be characterized as being destructive. For example, if you check the Receive check box for user and group database, any user records in the secondary database prior to the replication will be lost upon receipt of the primary Cisco Secure ACS system's database.
- Cisco Secure ACS replicates entire components. Replicated components include, but are not limited to Users/User Groups (or User Groups only),
- The bandwidth required for replication between Cisco Secure ACS systems depends on what components of the configuration are being replicated. Generally, the user/groups configuration will be the largest replication component. To get a rough estimate of the size of the data transfer during replication, perform an ACS backup and check the size of the backup file. The replication data transfer will be no larger than the size of the backup file, because Cisco Secure ACS uses a similar technique for packaging the configuration data for replication as it does for backup. Cisco Secure ACS does not replicate configuration changes, but instead replicates whole components. The various replication components are listed in System Configuration->Database Replication Setup. For example, Interface Configuration is a component. Cisco Secure ACS will replicate the entire interface configuration during replication. If an automatic replication schedule has been configured, then Cisco Secure ACS will only replicate components that have changed since the last replication.
- Cisco Secure ACS replication is unidirectional. This means the data flow in replication is one way and configuration changes performed on a secondary Cisco Secure ACS system cannot be sent to the primary Cisco Secure ACS system. As describe above, the configuration on the secondary Cisco Secure ACS system will be overwritten during the next replication. Any components that are replicated should not be changed at the secondary Cisco Secure ACS.

For example, a common component that might be changed on a secondary is user passwords. User password changes should not be allowed on secondary Cisco Secure ACS system. To accommodate user password changes, the user should access the primary Cisco Secure ACS system. One method to allow this is to make a process change so that only the master Cisco Secure ACS system is updated. For example, if users are allowed to update their passwords through TACACS+ devices, a workaround is to designate a TACACS+ device just for password updates. This device will update the master Cisco Secure ACS only. All password change on the secondaries will be disallowed by disabling telnet change password:

```
System Configuration > Local Password Management > Remote Change  
Password
```

Check the box:

```
Disable TELNET Change Password against this ACS and return the  
following message to the users telnet session
```

The user base will need to be educated to use this particular TACACS+ device for password updates.

- The following items cannot be replicated:
 - IP pool definitions (for more information, see About IP Pools Server in the User Guide for Cisco Secure Access Control Server 4.1).
 - ACS certificate and private key files.
 - Unknown user group mapping configuration.
 - Dynamically-mapped users.
 - Settings on the Cisco Secure ACS Service Management page in the System Configuration section.
 - RDBMS Synchronization settings.
 - Third-party software, such as RSA ACE client software.

Replication Timeout

The timer for the replication process on the Cisco Secure ACS primary system controls the entire replication process starting from queuing the first secondary Cisco Secure ACS system until the primary completes sending the transfer file to the last Cisco Secure ACS secondary system. Note that the timer does not run while the primary is building the transfer files. Looking at Table 4, the replication timer on the primary starts at step 4. The timer is cumulative for replication to all secondaries. This means that the timeout must be long enough from the first queuing to the end of the last transfer. In Table 4, this would be steps 4 through 8.

The following may slow down replication:

- Slow or busy network link between the primary and the secondary. This will affect only the primary and the secondary on the slow link.
- Busy primary, usually indicated by high CPU usage. This may be caused by high authentication usage or by another process running on the server. This will affect the entire replication process from the primary side.
- Busy secondary, usually indicated by high CPU usage. This may be caused by high authentication usage or by another process running on the server. This will only affect the primary for the specific secondary replication.

Large transfer files generally do not cause any problems. Test results indicate that replication of a large internal database (100,000 users and 5,000 network device entries) on a LAN takes 1.5 to 2.0 minutes.

The timeout on a secondary controls only the secondary. Issues affecting one secondary do not affect other secondaries.

Authentication Services Availability

During the replication process, the authentication service stops briefly on each of the Cisco Secure ACS systems (although not at the same time). On the sending Cisco Secure ACS system, service stops only once at the beginning while the appropriate components are collated and prepared for sending. On the receiving Cisco Secure ACS system, service is stopped when the incoming components are restored. Service is normal during transmission of the replication between Cisco Secure ACS systems. Table 4 shows replication sequencing between the primary Cisco Secure ACS system and two secondary Cisco Secure ACS systems.

Figure 2. Database Replication Configuration (Cisco Secure ACS)

Replication Components ?

Component	Send	Receive
User and Group Database	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Group Database only	<input type="checkbox"/>	<input type="checkbox"/>
Network Configuration Device tables	<input type="checkbox"/>	<input type="checkbox"/>
Distribution Table	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Interface Configuration	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Interface Security Settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Password validation settings	<input checked="" type="checkbox"/>	<input type="checkbox"/>
EAP-FAST master keys and policies	<input type="checkbox"/>	<input type="checkbox"/>
Network Access Profiles	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Outbound Replication ?

Scheduling

Manually
 Automatically triggered cascade
 Every minutes
 At specific times...

	00:00	06:00	12:00	18:00	24:00
Mon					
Tue					
Wed					
Thu					
Fri					
Sat					
Sun					

Partners

<p style="text-align: center; font-size: small;">AAA Servers</p> <div style="border: 1px solid gray; padding: 2px;"> acs-po-03 acs-po-2 acs_eclipse_ru-1 acsse1112-2 ACSSE_1113-1 Eclipse-1 Eclipse-RU-3 </div>	<input type="button" value=">"/> <input type="button" value="<"/>	<p style="text-align: center; font-size: small;">Replication</p> <div style="border: 1px solid gray; padding: 2px;"> acsse-1112-3 </div>
---	--	--

Inbound Replication ?

Accept replication from

Replication settings ?

Replication timeout: minutes

Figure 3. CSV Database Replication File Configuration (Cisco Secure ACS)

CSV Database Replication File Configuration

Enable Logging ?

Log to CSV Database Replication report

Log File Management ?

Generate New File

- Every day
- Every week
- Every month
- When size is greater than KB

Directory

Manage Directory

- Keep only the last files
- Delete files older than days

Table 4. Replication Sequencing

	ACS Primary	ACS Secondary 1	ACS Secondary 2
1	ACS AAA services offline		
2	Create transfer file		
3	ACS AAA services online		
4	Queuing transfer to ACS Secondary 1/Queuing transfer to ACS Secondary2		
5	Transfer to ACS Secondary 2 started	Replication starting/receiving transfer file	
6	Transfer to ACS Secondary 1 completed	Transfer complete/ACS AAA services offline	
7	Transfer to ACS Secondary 2 started	Rebuilding database	Replication starting/receiving transfer file
8	Transfer to ACS Secondary 2 completed	Database rebuild complete/ACS AAA services online	Transfer complete/ACS AAA services offline

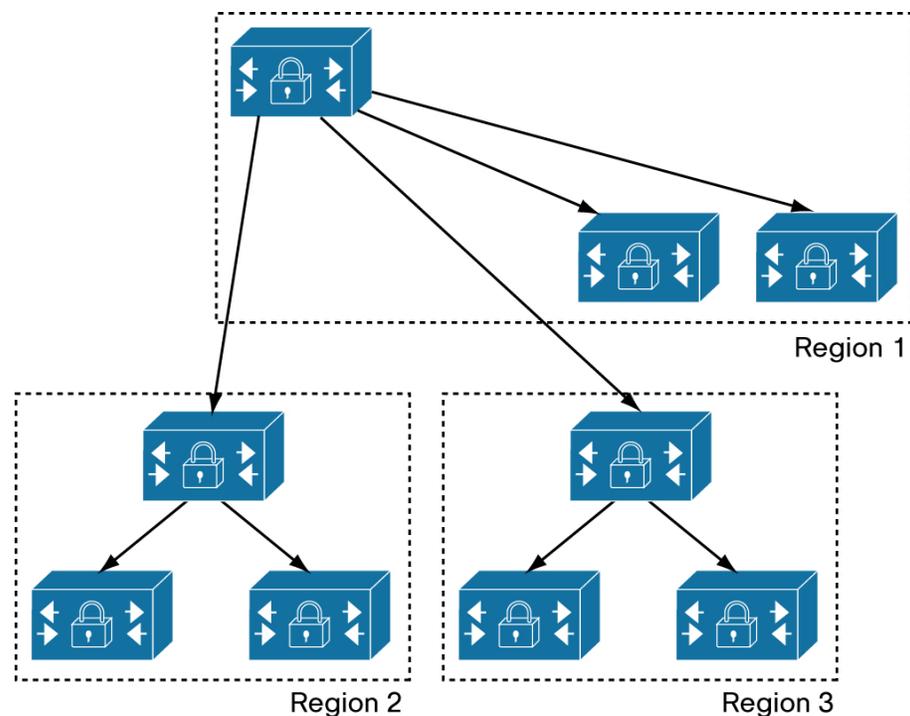
Cascade Replication

In cascade replication, a secondary Cisco Secure ACS system performs database replication to the configured list of secondary Cisco Secure ACS systems when database replication from a primary Cisco Secure ACS system completes. You use this option to build a propagation hierarchy of Cisco Secure ACS systems, relieving a primary Cisco Secure ACS system from the burden of propagating the replicated components to every other Cisco Secure ACS system. Figure 4 provides an example scenario. Because database replication in Cisco Secure ACS is a “top down” approach, using the cascade method minimizes replication-induced downtime on the primary Cisco Secure ACS system. In addition, cascade replication helps minimize the effects of a slow network link from region to region by doing only one file transfer instead of multiple file transfers across the link. Administrators have the option to either use the Automatically triggered cascade (Figure 2) or

schedule the cascade replication for a different time to accommodate local regional needs. Figure 4 shows a hypothetical scenario for replication where each region has both a primary and a secondary Cisco Secure ACS deployed. In this scenario, replication is done to the secondary Cisco Secure ACS systems to avoid multiple replications across the WAN.

Configuring replication components for cascade replication requires the administrator to select replication components in both the Send and Receive columns on the cascading Cisco Secure ACS system. Again, these two columns will usually have the same configuration. However, there may be cases where one or more of the replication components sent from the primary Cisco Secure ACS system will not be replicated to the regional secondary Cisco Secure ACS systems, or additional replication components that are only locally configured need to be replicated with the region.

Figure 4. Cascade Database Replication (Cisco Secure ACS)



Replication Recommendations

Cisco recommends the following additional considerations for replication deployment:

- Do not perform replication during periods of high authentication rates.
- The replication timeout is cumulative. Increase the replication timeout as necessary to accommodate any latency. For example, if you have 35 Cisco Secure ACS secondaries and are experiencing replication timeout failures, increase the timeout to allow for a 10-minute replication cycle to each secondary.
 - 35 servers X 10 minutes / server = 350 minutes.
- In the above case, you can use cascade replication to lessen the issues of delayed transmissions.
- Remove the replication primary Cisco Secure ACS system from authentication duties.

Provisioning

Web-based GUI (requires JRE)

Cisco Secure ACS provides a flexible administration mechanism to configure, maintain, and protect its AAA functionality. You can perform nearly all Cisco Secure ACS administration tasks through the Cisco Secure ACS web interface. You can view the Cisco Secure ACS web interface through a web browser and can use the web interface to easily modify the Cisco Secure ACS configuration from any connection on your LAN or WAN. The web interface not only makes viewing and editing user and group information possible, it can also be used to restart services, add remote administrators, change AAA client information, back up the system, view reports from anywhere on the network, and more.

Web Interface Security

Accessing the web interface requires a valid administrator name and password. The Cisco Secure ACS Login page encrypts the administrator credentials before sending them to Cisco Secure ACS.

Administrative sessions will timeout after a configurable length of idle time. Regardless, it is recommended that you log out of the web interface after each session. You can enable a secure socket layer (SSL) for administrative sessions. This method ensures encryption of all communication between the web browser and Cisco Secure ACS. Your browser must support SSL.

CSUtil Command-line Executable (Cisco Secure ACS for Windows)

The CSUtil command-line utility allows the administrator to configure many parts of the Cisco Secure ACS database, apart from a number of other functions. These functions are:

- Locating CSUtil.exe and related files
- Combining options using CSUtil Command Syntax
- Backing up Cisco Secure ACS with CSUtil.exe
- Restoring Cisco Secure ACS with CSUtil.exe
- Initializing Cisco Secure ACS internal database
- Creating Cisco Secure ACS internal database dump file
- Loading Cisco Secure ACS internal database from a dump file
- Cleaning up Cisco Secure ACS internal database
- User and AAA client import option
- Exporting user list to a text file
- Exporting group information to a text file
- Decoding error numbers
- Adding and deleting user-defined RADIUS vendors and VSAs
- Generating PAC file
- Export, add, and delete posture-validation attributes
- Adding external audit device type attributes

For more information on CSUtil, see *User Guide for Cisco Secure Access Control Server 4.1*.

RDBMS Synchronization

Cisco Secure ACS for Windows

The RDBMS Synchronization feature enables you to update the Cisco Secure ACS internal database with information from an ODBC-compliant data source. The ODBC-compliant data source can be the RDBMS database of a third-party application. It can also be an intermediate file or database that a third-party system updates. Regardless of where the file or database resides, Cisco Secure ACS reads the file or database via the ODBC connection.

Cisco Secure ACS Solution Engine

The RDBMS Synchronization feature provides the ability to update the Cisco Secure ACS internal database with information from a text file on an FTP server. A third-party application can generate the test file. Cisco Secure ACS gets the file from the FTP server, reads the file, and performs the configuration actions specified in the file.

You can configure synchronization to occur on a regular schedule. You can also perform synchronizations manually, updating the Cisco Secure ACS internal database on request.

Synchronization performed by a single Cisco Secure ACS can update the internal databases of other Cisco Secure ACS systems, so that you only need to configure RDBMS Synchronization on one Cisco Secure ACS. Cisco Secure ACS systems listen on TCP port 2000 for synchronization data. RDBMS Synchronization communication between Cisco Secure ACS systems is encrypted using 128-bit encrypted, proprietary algorithm.

For more information on RDBMS Synchronization, see the User Guide for Cisco Secure Access Control Server 4.1.

Note: Starting with Cisco Secure ACS 4.2, RDBMS Synchronization will have increasing capabilities, including invocation.

Cisco Secure ACS for Windows: The administrator will be able to invoke “dbsync” from the command-line and the .csv file will be easier to access.

Cisco Secure ACS Solution Engine: The administrator will be able to invoke “dbsync” from an SSL connection to the appliance. The use of FTP to move the .csv file from an FTP server will still be required.

Logging Capabilities

Cisco Secure ACS produces a variety of logs. You can download many of these logs, or view them in the Cisco Secure ACS web interface as HTML reports.

Cisco Secure ACS logs a variety of user and system activities to different formats and targets. These topics describe the information that you can log. You can use these logs for troubleshooting and diagnostics, compliance and auditing, building reports and billing.

Cisco Secure ACS Logs

<i>Network</i>	<i>Configuration audit</i>
TACACS+ Accounting	Administration Audit
TACACS+ Administration	User Password Changes
RADIUS Accounting	<i>System Logs</i>
VoIP Accounting	Cisco Secure ACS Backup and Restore
Passed Authentications	RDBMS Synchronization
Failed Attempts	Database Replication
Logged-in Users	Cisco Secure ACS Service Monitoring
<i>Configuration reports</i>	Appliance Status Page
Disabled Accounts	Appliance Administration Audit
Entitlement Reports	
User Entitlement Reports	
Administrator Entitlement Reports	

Configuring Cisco Secure ACS Logs

You can enable and configure logging for individual logs. Cisco Secure ACS can log information to multiple loggers simultaneously.

- **Configuring Critical Loggers:** critical logger for accounting logs guarantees delivery of these logs to at least one logger. It is recommended that you configure a syslog logger as a critical logger, because according to syslog standards, you cannot guarantee syslog message.
- **Configuring a Comma Separated Value (CSV) Log:** the standard internal log storage, viewed by the Cisco Secure ACS log viewer. Windows allows rollover based on frequency or size, specification of log directory, and optional purging of files based on age or number. The Cisco Secure ACS Solution Engine has a fixed log file rollover at 10 MB, and retains the most recent seven log files.
- **Configuring Syslog Logging:** to record AAA-related logs and audit logs to a syslog logger. You can configure each log to go to a separate syslog server. You can configure up to two servers per log file.

- **Configuring an ODBC Log (Cisco Secure ACS for Windows):** to record AAA-related logs and audit logs to an ODBC logger. You can configure the SQL create table statement before or after configuring the ODBC log in Cisco Secure ACS.
- **Configuring and Enabling Remote Logging (Cisco Secure ACS for Windows):** remote logging for AAA-related logs and audit logs. You must first configure the remote logging server, and then configure remote logging on each Cisco Secure ACS that will send information to the remote logging server.
- **Configuring Logging to Cisco Secure ACS Remote Agents (Cisco Secure ACS Solution Engine):** for remote logging of AAA-related logs and audit logs to installed Cisco Secure ACS Remote Agents. You can configure multiple remote agent destinations. You can log to all destinations, or use as a failover list.
- **Configuring Service Logs:** contains a log of the events that Cisco Secure ACS encounters when it attempts to monitor services such as CSAdmin. This includes events for the Active Service Monitor, CSMon, which is itself a service. This report is on by default.
- **Providing Service Logs for Customer Support:** to create a package.cab file for debugging. Cisco Secure ACS has a number of debug logs including CSAdmin, CSAAuth, CSDBSync, CSLog, CSMon, CSRADIUS and CSTacacs. You can set the log level to None, Low, or Full. You should set the log level to Full for diagnostics. Starting with Cisco Secure ACS 4.1.3, Cisco Secure ACS provides a session key for correlation between logs. Diagnostic log is only for local logging. The Support command on the Cisco Secure ACS Solution Engine allows debug log download.

Selecting the Correct Log Format

For small installations of one or two Cisco Secure ACS systems, use of the internal .csv file is recommended. If using Cisco Secure ACS for Windows, you can use the remote logging option to consolidate logs on one system.

For medium to large installations, use of the syslog option for offloading logs to a remote server is now recommended. This has several advantages including the ability to “steer” different logs to different servers and allowing the use of a dedicated log server for log consolidation.

Cisco Secure ACS for Windows or Cisco Secure ACS Solution Engine

Cisco Secure ACS for Windows can be considered when:

- The administrator prefers hardware selection and has existing practices for Windows server management.
- The organization runs virtual data centers (with VMware ESX).
- Cisco Secure ACS Solution Engine can be considered when server procurement is an additional hurdle for the organization.

Though it is possible to have an AAA environment of both server and appliance versions of Cisco Secure ACS, creating a mixed environment is not recommended.

Table 5 highlights some of the differences between Cisco Secure ACS Solution Engine and Cisco Secure ACS for Windows.

Table 5. Cisco Secure ACS Solution Engine vs. Cisco Secure ACS for Windows

	Cisco Secure ACS Solution Engine	Cisco Secure ACS for Windows
Operating System	Closed and hardened operating system	Customer controlled and maintained operating system
AD Authentication	Requires Cisco Secure ACS Remote Agents on a domain-joined Windows server	Cisco Secure ACS communicates directly with Windows for faster authentication
RDBMS Authentication	No ODBC/RDBMS support	Supports authentication to RDBMS via ODBC
OTP	No proprietary RSA support. Must use RADIUS for OTP. Group mapping support. (Starting with version 4.2, Cisco Secure ACS Solution Engine will support proprietary RSA OTP).	Proprietary RSA OTP interface supported. Group mapping support only with RADIUS.
Centralized Logging	Cisco Secure ACS Remote Agents provides an encrypted channel as well as an unencrypted system.	Unencrypted syslog

Performance and Scaling

This section discusses performance testing conducted on Cisco Secure ACS version 4.1. Testing was performed on several types of servers, different user databases and multiple authentication protocols. Table 6 shows the types of servers used to conduct this testing. Table 7 shows results achieved from the testing.

Table 6. Test Platforms

Cisco Secure ACS Product	Platform Configuration
Solution Engine 1112 (4.1)	Pentium IV, 3.2 GHz, 1 GB RAM, Windows 2000 Server
Cisco Secure ACS 4.1	Pentium, 2.8 GHz, 2 GB RAM, Windows Server 2003
Cisco Secure ACS 4.0	Pentium, 2.8 GHz, 2 GB RAM, Windows Server 2003

Numbers are derived in transactions per second (TPS) from Solution Engine clients for Cisco Secure ACS. Data provided in Table 6 is only for authentication. Authentication rates are sustained rates. Peak rates may be higher.

Number of Cisco Secure ACS Systems Required

In general, you can calculate the minimum number of Cisco Secure ACS systems required to support a given size of user database in two steps using the following formulae:

1. $tRate = nUsers / tAuth$
2. $nACS = tRate / Authrate$

Where:

- nACS is the number of Cisco Secure ACS systems required
- nUser is total number of users in the environment. A user can be viewed as an "authentication".
- tAuth is the period of time the users are expected to authenticate into the network .
- tRate is the expected authentication rate for all users.
- Authrate is the number of authentications per second expected from Cisco Secure ACS for a specific authentication protocol. For example, the Authrate for PEAP is 20.09 authentications per second.

In Example 1 the customer has 30,000 users. They expect all of the users to log into the network over a ten minute period. They will be using EAP-FAST as the supplicant.

Example 1 Calculating Number of Cisco Secure ACS Systems Required

```
nUsers      = 30,000
tAuth       = 10 minutes = 600 seconds
Authrate    = 33.07 authentications / second
tRate       = 30000 / 600 = 50 authentications / second
nACS        = 50 / 33.07 = 1.51 or 2 Cisco Secure ACS systems
```

Table 7. Baseline Performance Test Results Matrix (Cisco Secure ACS 4.1)

Protocol	Authentications/Second
TACACS+	151.13
PAP	201.39
MS-CHAP	187.06
LEAP	52.30
EAP-FAST v1a	33.07
PEAP-TLS	20.09
PEAPv0	34.51
EAP-TLS	32.12

The values in Table 7 are the result of tests run in a laboratory environment. Please use these values as baselines for general planning purposes. The actual performance numbers that you experience will vary due to other factors, such as server hardware, network configuration, network traffic, user repository and so on.

Network Access Policy

Network access is a broad concept. In general, it defines how users can connect to the LAN, or from the LAN to outside resources (that is, the Internet). This connection may occur in a number of ways including, but not limited to, dial-in, ISDN, wireless bridges, and secure Internet connections. Each method has its own advantages and disadvantages, and poses a challenge in providing AAA services. This closely ties network access policy to the enterprise network topology. In addition to the method of access, other decisions, such as specific network routing (access lists), time-of-day access, individual restrictions on NAS access (access control lists), and so on, can also affect how you deploy Cisco Secure ACS.

You can implement network access policies for employees who telecommute or for mobile users who dial in over an ISDN or a Public Switched Telephone Network (PSTN). Such policies can be enforced at the corporate campus with Cisco Secure ACS and the access server (AS5850, VPN concentrator, and so on). Within the enterprise network, network access policies can control access for individual employees.

Cisco Secure ACS network access policy provides control by using central authentication and authorization for remote users. The Cisco Secure ACS database maintains all user IDs, passwords, and privileges. Cisco Secure ACS access policies can be downloaded in the form of access control lists (ACLs) to network access servers such as the Cisco AS5850 Network Access Server, or by allowing access during specific periods, or on specific access servers.

Some policy configuration examples are listed in the following sections.

Downloadable Access Control Lists

Downloadable Access Control Lists (dACLs) are an alternative to configuring ACLs in the RADIUS Cisco AV attribute [26/9/1] of each user or user group, or assigning an ACL number or name for an ACL defined on a device. You can create a dACL once, give it a name, and then assign the dACL to each applicable user or user group by referencing its name. This method is more efficient than configuring the RADIUS Cisco AV pair attribute for each user or user group or locally on the network device.

You can use dACLs to create sets of ACL definitions that you can apply to many users or user groups. These sets of ACL definitions are ACL contents. Also, by incorporating Network Access Filters (NAFs), you can control the ACL contents sent to the AAA client from which a user is seeking access. That is, a dACL comprises one or more ACL content definitions, each of which is associated with a NAF or associated to all AAA clients by default. (The NAF controls the applicability of specified ACL contents based on the AAA client's IP address. For more information on NAFs and how they regulate dACLs, see "About Network Access Filters" in the User Guide for Cisco Secure Access Control Server 4.1.

The dACLs operate in the following manner:

1. When Cisco Secure ACS grants a user access to the network, Cisco Secure ACS determines if it assigns a dACL to that user or the user's group.
2. If Cisco Secure ACS locates an assigned dACL, Cisco Secure ACS determines whether an ACL content entry is associated with the AAA client that sent the RADIUS authentication request.

3. Cisco Secure ACS sends, as part of the user session, a RADIUS Access-Accept packet with attribute specifying the named ACL and the version of the named ACL.
4. If the AAA client responds that it does not have the current version of the ACL in its cache (that is, the ACL is new or has changed), Cisco Secure ACS sends the ACL (new or updated) to the device.

To use a dACL on a particular AAA client, the AAA client must:

- Use RADIUS for authentication
- Support dACLs

Examples of Cisco devices that support dACLs are:

- PIX Firewalls
- VPN 3000-series concentrators, ASA and PIX devices
- Devices running Cisco IOS Software Release 12.3(8)T or later

For more details, see the User Guide for Cisco Secure Access Control Server 4.1.

VLANs

Switches running Cisco IOS Software Release 12.1(14)EA1 and later support 802.1X with virtual LAN (VLAN) assignment. After successful 802.1X authentication of a port, the RADIUS server sends the VLAN assignment to configure the switch port. The RADIUS server database maintains the username-to-VLAN mappings, assigning the VLAN based on the username of the client connected to the switch port. You can use this feature to limit network access for certain users.

The RADIUS attributes required are:

[64] Tunnel-Type = VLAN

[65] Tunnel-Medium-Type = 802

[81] Tunnel-Private-Group-ID = VLAN name or VLAN ID

Timeouts

Cisco Secure ACS supports two types of timeouts in the AAA return attributes:

Session Timeout: The allowed time an online session is to run.

Idle Timeout: An inactivity timer that will end a session if it expires.

Time-of-Day Access

You can define the allowed time during which users can access the network.

Network Access Restrictions

A Network Access Restriction (NAR) is a definition, which you make in Cisco Secure ACS, of additional conditions that must be met before a user can access the network. Cisco Secure ACS applies these conditions by using information from attributes that your AAA clients sent. Although you can set up NARs in several ways, they are all based on matching attribute information that an AAA client sent. Therefore, you must understand the format and content of the attributes that your AAA clients send if you want to employ effective NARs.

In setting up an NAR, you can choose whether the filter operates positively or negatively. That is, in the NAR you can specify whether to permit or deny network access, based on the information sent from AAA clients when compared to the information stored in the NAR. However, if a NAR does not encounter sufficient information to operate, it defaults to denied-access. Table 8 shows these conditions.

Table 8. NAR Permit or Deny Conditions

	IP-Based	Non-IP-Based	Insufficient Information
Permit	Access Granted	Access Denied	Access Denied
Deny	Access Denied	Access Granted	Access Denied

Cisco Secure ACS supports two types of NAR filters:

- **IP-based Filters:** IP-based NAR filters limit access based on the IP addresses of the end-user client and the AAA client. For more information on this type of NAR filter, see “About IP-Based NAR Filters” in the User Guide for Cisco Secure Access Control Server 4.1.
- **Non-IP-based Filters:** Non-IP-based NAR filters limit access based on a simple string comparison of a value sent from the AAA client. The value may be the calling line identification (CLID) number, the Dialed Number Identification Service (DNIS) number, the MAC address, or other value originating from the client. For this type of NAR to operate, the value in the NAR description must exactly match the value sent from the client, including whatever format used. For example, the telephone number (217) 555-4534 does not match 217-555-4534. For more information on this type of NAR filter, see “About Non-IP-based NAR Filters” in the User Guide for Cisco Secure Access Control Server 4.1.

Network Access Profiles

Typical organizations have various kinds of users who access the network in different ways and for different purposes. Correspondingly, you must apply different security policies to different use cases. For example, you might have to apply a tighter and more limiting security policy to the wireless access points of your building’s lobby area as opposed to the physically secured production plant. You might have to treat remote-access users who use a VPN differently from users who log in from behind a firewall. Users who connect through certain subnetworks might require a different authentication from other users. Wireless access is often treated more strictly than wired access, as is any form of remote access (for example, dial, VPN, home wireless).

A Network Access Profile (NAP), also known as a profile, is essentially a classification of network-access requests for applying a common policy. You can use NAPs to aggregate all policies required for a certain location in the network. Alternatively, you can aggregate all policies that handle the same device type, for example, VPNs or Access Points (APs).

Note: NAPs allow you to configure specific protocols and databases for authentication. This lets you tailor the authentication methods to the type of network access. For example, you can have one NAP for VPN remote access that requires a one-time password server for authentication, and another NAP for wireless access that requires the use of PEAP with EAP-MSCHAP using AD for authentication.

For more details, refer to <http://www.cisco.com/warp/public/cc/so/neso/vpn/index.shtml>

Upon receiving a packet, Cisco Secure ACS evaluates the profile filters to classify the packet. When a profile matches, Cisco Secure ACS applies the configuration and policies that are associated with the profile during packet processing. Cisco Secure ACS uses a first-match strategy on the first access request of the transaction. If Cisco Secure ACS does not find a matching profile, Cisco Secure ACS reverts to the global configuration settings.

Note: NAPs do not support the TACACS+ protocol in Cisco Secure ACS.

You must configure the following NAP components in advance.

NAFs

NAFs are groupings of AAA client configurations (which might represent multiple network devices), network device groups (NDGs), or IP addresses of specific AAA client devices. You can use a NAF to group (and name) a disparate set of devices.

You can also use NAFs to differentiate user requests on the same type of device. For example, while you undertake a Cisco IOS Software upgrade for Cisco Aironet wireless APs (perhaps to enable some new encryption protocol), you might require a separate NAP for upgraded and nonupgraded APs.

Note: If you want to aggregate NDGs and use them as a filter to assign users to a profile, you must configure NAFs before you set up a profile.

RADIUS Authorization Components

Shared Radius Authorization Components (RACs) contain groups of RADIUS attributes that you can dynamically assign to user sessions based on a policy. Using the NAP configuration, you can map a policy type with set conditions, such as NDG and posture, to a shared RAC.

Posture Validation

Posture validation works with Network Access Control (NAC). NAC uses the network infrastructure to enforce security policy compliance on all devices seeking access to network computing resources.

Security policy compliance limits damage from emerging security threats. By using NAC, customers can allow network access only to compliant and trusted end-point devices (such as PCs, servers, and PDAs), and can restrict the access of noncompliant devices.

Downloadable ACLs

See *Downloadable Access Control Lists* section.

Protocol Types

You can use Protocol Types to classify a user request based on the type of protocol used to request access to the network, such as PEAP or EAP-FAST. To use this option, you may require some configuration in the global setup.

For information on the other options, see the User Guide for Cisco Secure Access Control Server 4.1.

The remote-access policy is part of the overall corporate security policy.

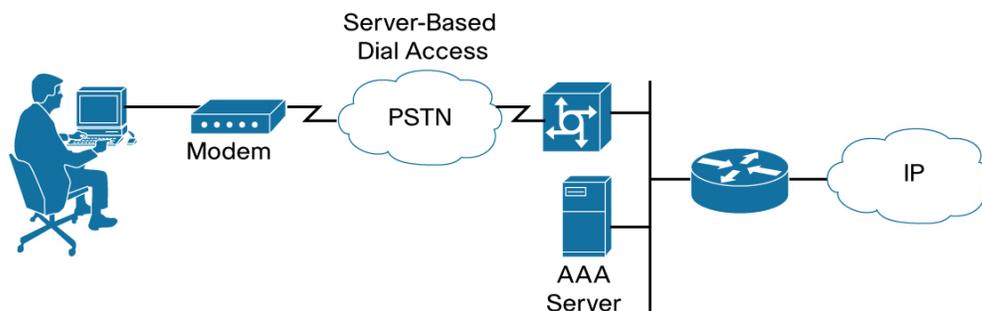
General Scenarios

Each of the following basic scenarios will use specific policy configurations in Cisco Secure ACS.

Dialup Access

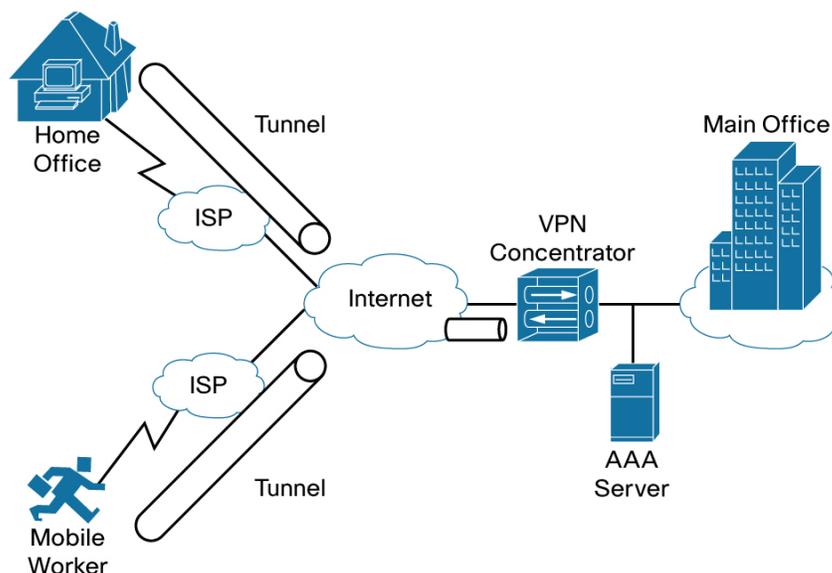
In the traditional model of dialup access (a PPP connection), a user employing a modem or ISDN connection is granted access to an intranet through a NAS. Typically, the policy features used with dialup access are NARs, especially non-IP-based NARs with DNIS, CLID, and so on. Dialup access policies may also incorporate session and idle timeouts, and max-sessions. If dialup access is using RADIUS, you can also leverage NAPs to provide additional granularity for returned RADIUS attributes. Figure 5 shows a typical dialup environment.

Figure 5. Dialup Environment



Remote Access Using VPN

VPNs use advanced encryption and tunneling to permit organizations to establish secure, end-to-end, private network connections over third-party networks, such as the Internet or extranet (See Figure 6). Typically, the policy features used with VPN access are downloadable ACLs and NARs, especially IP-based NARs. VPN access policies may also incorporate session and idle timeouts, and max-sessions. If VPN access uses RADIUS, you can also leverage NAPs to provide additional granularity for returned RADIUS attributes, downloadable ACLs, and so on.

Figure 6. Enterprise VPN Solution

A more in-depth discussion on implementing VPN solutions is available at

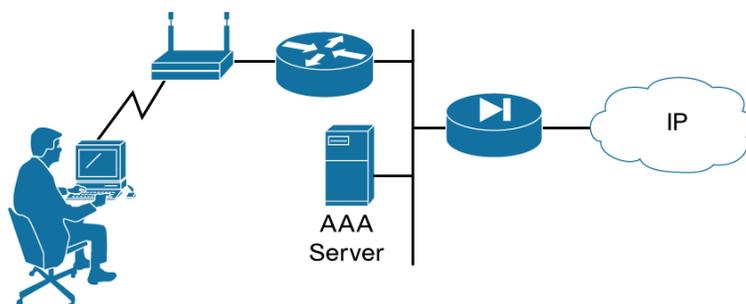
http://www.cisco.com/warp/public/cc/so/neso/vpn/vpne/vpn21_rg.htm

Wireless Network

The wireless network AP is a relatively new client for AAA services. The wireless AP provides a bridged connection for mobile clients into the LAN. The 802.1X standard controls access to the AP. Authentication is necessary because of ease of access to the AP. Encryption is also a necessity because of the ease of eavesdropping on communications. As such, security plays an even bigger role than in the dialup or VPN access. To protect user credentials in this exposed environment, use of EAP is strongly encouraged. As discussed earlier about EAP types, each EAP type has its restrictions on password type, available external database and security provided.

As with other access methods, wireless access policies may also incorporate NARs, session and idle timeouts, and max-sessions. Also, if the wireless access supports it, you can also provide VLAN information to control network access. Because EAP uses RADIUS, you can also leverage NAPs to provide additional granularity for returned RADIUS attributes, VLANs, and so on.

Figure 7 shows a typical wireless LAN.

Figure 7. Figure 7 Wireless LAN

For more information on deploying Cisco Secure ACS in a wireless network, refer to the whitepaper available at

http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_white_paper09186a00801495a1.shtml

LAN Network

With the advent of 802.1X on switches, network administrators now have the ability to control network access and enforce policy as an authorized result of the authentication at the switch port. As with the wireless LAN, LAN access at the switch requires the use of EAP. The most significant access policy that Cisco Secure ACS can provide to the switch is to assign a VLAN for the user session. As with other access methods, LAN access policies may also incorporate NARs, session and idle timeouts, and max-sessions. Since EAP uses RADIUS, you can use NAPs to provide additional granularity for returned RADIUS attributes, VLANs, and so on.

Device Administration Policy

Managing a network is a matter of scale. Providing a policy for administrative access to the network devices depends directly on the size of the network and the number of administrators required to maintain it. You can perform local authentication on the network device but it is not very scalable. The use of network management tools can help in large networks but the use of local authentication on each device will result in a single login on the network device. This does not promote adequate device security. The use of Cisco Secure ACS allows for a centralized administrator database. You can add and delete administrators at one location.

Cisco Secure ACS uses a number of policy tools.

AAA Protocol

TACACS+ is the recommended AAA protocol choice for controlling NAS administrative access because of its ability to provide command filtering of a NAS administrator's access to the device and command logging.

RADIUS, because of the one-time transfer of authorization information at the time of authentication acceptance, does not provide command authorization or logging. However, RADIUS may be required because it is the only AAA protocol supported by a device.

NAR

NARs, as discussed earlier, provide absolute control of access to a given network device. NARs work with both TACACS+ and RADIUS.

Shell Access Authorization

If you configure TACACS+ authorization, you must check the Shell box to permit exec access to the network device.

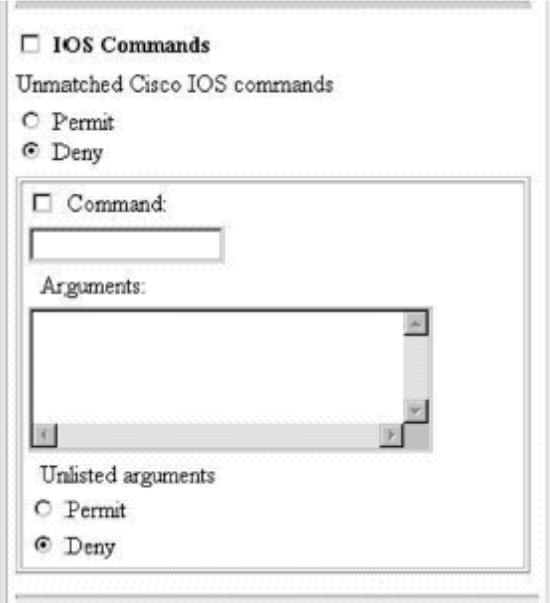
Privilege Level

Privilege level assigns the privilege level for device access at the time of login. Using privilege level requires authorization to be active. Available for both TACACS+ (distinct A/V pair) and RADIUS (requires a VSA).

Command Authorization

Cisco Secure ACS can filter command access on a device using TACACS+ command authorization mechanism. This allows the administrator to set up a centralized set of rules to control access to the network device. When configured to use command authorization, the network device sends commands to the Cisco Secure ACS for parsing. Cisco Secure ACS determines whether the device administrator has permission to use the command (See Figure 8). Greater flexibility is available in using Command Authorization Sets. Find more information on Command Authorization Sets at

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs41/user/spc.htm

Figure 8. Command Authorization Configuration


Cisco IOS CLI View and Cisco IOS XR Task Assignments

Device administrators can configure the Cisco IOS CLI and Cisco IOS XR device operating systems to control administrative access on the local device. This control is similar to TACACS+ command authorization but does not require a network connection. Cisco IOS CLI uses a feature called CLI View and Cisco IOS XR uses a feature called Tasks. In each system, Cisco Secure ACS passes the View ID or Task ID to the device via TACACS+ or RADIUS A/V pairs for AAA authenticated/authorized users.

For TACACS+ connections, use the **Custom attributes** box for Shell configuration. The respective View and Tasks entries are:

```
cli-view-name=<cli-view-role-name>
  (example: cli-view-name=view_one)
task="<permissions>:<taskid name>, #<usergroup name>, ..."
  (example: task="rwx:bgp,#operator")
```

To assign the CLI View name or Task ID via RADIUS, you will have to assign a VSA or RADIUS attribute 26. To configure the CLI View name option or Task ID option, check **[009\001] Cisco-av-pair** under **Cisco IOS/PIX 6.x RADIUS Attributes** and enter either:

```
cli view name=<cli view role name>
  (example: cli-view-name=view_one)
task="<permissions>:<taskid name>, #<usergroup name>, ..."
  (example: task="rwx:bgp,#operator")
```

Session Timeout

This is the Absolute time for a login available for both TACACS+ and RADIUS.

Idle Timeout

Idle timeout provides an inactivity timer available for both TACACS+ and RADIUS.

Max Sessions

Cisco Secure ACS keeps track of the number of current sessions that the user has at any given time and prevents the user from accessing the network or a device when exceeding that number. Because Max Sessions requires accounting to be active, it may be of limited use in an environment with multiple Cisco Secure ACS systems. Max Sessions is available for both TACACS+ and RADIUS.

Limit User to Number of Hours of Online Time

Because this feature requires accounting to be active, it may be of limited use in an environment with multiple Cisco Secure ACS systems. Online timer is available for both TACACS+ and RADIUS.

Limit User to Number of Sessions

Cisco Secure ACS keeps track of number of individual sessions that the user has made and prevents the user from accessing the network or a device when exceeding that number. Because this feature requires accounting to be active, it may be of limited use in an environment with multiple Cisco Secure ACS systems. Session limit is available for both TACACS+ and RADIUS.

Time-of-Day Restrictions

Limits access by time of day. Like NARs, time-of-day restriction is absolute. Because this feature requires accounting to be active, it may be of limited use in an environment with multiple Cisco Secure ACS systems. Time-of-day is available for both TACACS+ and RADIUS.

Enable Password

Use Cisco Secure ACS to manage the "enable password" for network devices. Enable password is only available with TACACS+.

Integration with Network Management Software

Cisco Secure ACS provides command authorization for users who are using management applications to configure managed network devices. Unique command authorization set types that contain a set of permissions support command authorization. These permissions determine the actions that users with particular roles can perform within the management application. This is only available with TACACS+.

Logging

Session logging

The TACACS+ and RADIUS accounting reports contain a record of all successful authentications for the applicable item during the period covered by the report. Information captured includes time/date, username, type of connection, amount of time logged in, and bytes transferred.

Administration (command) logging

TACACS+ command accounting for logging administration information from the network device.

For more information regarding TACACS+ and device administration, see the whitepaper Device Administration with Cisco Secure.

Separating Device Administration Users and General Network Users

It is important to keep general network users from accessing network devices. Even though a general user might not intend to disrupt the system, inadvertent access may cause accidental disruption to network access. Separating general users from administrative users falls into the realm of AAA and the Cisco Secure ACS.

The easiest and recommended method to perform such separation is to use RADIUS for the general remote-access user and TACACS+ for the administrative user. An issue likely to arise is that an administrator might also require remote network access like a general user. This poses no problem with Cisco Secure ACS. The administrator can have both RADIUS and TACACS+ configurations in Cisco Secure ACS. Using authorization, RADIUS users can have PPP (or another network access protocol) set as the permitted protocol. Under TACACS+, the administrator can be configured only to allow shell (exec) access.

For example, if the administrator is dialing into the network as a general user, the NAS would use the PPP protocol for password control and RADIUS as the authenticating and authorizing protocol. In turn, if the same administrator is remotely connecting to the network device to make configuration changes, the device would use the TACACS+ protocol for authentication and authorization. Because this administrator was configured on Cisco Secure ACS with permission for shell under TACACS+, the administrator has authorization to log in to that device. This does require that the NAS have two separate configurations on Cisco Secure ACS, one for RADIUS and one for TACACS+.

Example 2 shows a NAS configuration under Cisco IOS Software.

Example 2 Sample Cisco IOS Software Configuration for Separating PPP and Shell Logins

```
aaa new-model
tacacs-server host <ip-address>
tacacs-server key <secret-key>
radius-server host <ip-address>
radius-server key <secret-key>
aaa authentication ppp default group radius
aaa authentication login default group tacacs+ local
aaa authentication login console none
aaa authorization network default group radius
aaa authorization exec default group tacacs+ none
aaa authorization command 15 default group tacacs+ none
username <user> password <password>
line con 0
login authentication no_tacacs
```

Conversely, if a general user tried to use the remote-access login into a network device, Cisco Secure ACS would check and approve the user's username and password, but the authorization process would fail because that user would not have credentials that allow shell (exec) access to the device.

Scenario: Large Network

Binary Flip Flops is a multinational manufacturing company with corporate sites in Los Angeles, Chicago, New York, Frankfurt, and Singapore. The design team has decided to deploy wireless and remote-access capabilities throughout the company network. The company has also decided that remote access and wireless connections will use different authentication methods. Remote access to VPN concentrators will use RSA OTP for authentication and wireless will use the corporate AD database for authentication. Because of this dual authentication requirement, the deployment team decided to leverage NAP. They will accomplish this deployment in stages.

Scaling

Before testing and rollout can begin, the team needs to determine the number of Cisco Secure ACS systems required throughout the company network. The five sites will each have their own Cisco Secure ACS installation. The number of users at each site is:

Chicago: 20,000 Los Angeles: 15,000 New York: 12,000 Frankfurt: 3,000 Singapore: 5,000

The design team wants the capability of logging in the wireless users using EAP-FAST at each site in a 10-minute period. They consider VPN users to have negligible impact on the servers. Using the formulae in “Performance and Scaling” section, the number of Cisco Secure ACS systems required can be calculated.

Chicago

- $nUsers = 20,000$
- $tAuth = 10 \text{ minutes} = 600 \text{ seconds}$
- $Authrate = 33.07 \text{ authentications / second (EAP-FAST)}$
- $tRate = 20000 / 600 = 33.33 \text{ authentications / second}$
- $nACS = 33.33 / 33.07 = .998 \text{ or } 1 \text{ Cisco Secure ACS system}$

Since the other sites have fewer employees than the Chicago site, they will each also require one Cisco Secure ACS system. The design team has decided to have two Cisco Secure ACS systems at each site for redundancy for a total of ten Cisco Secure ACS systems.

Deployment Plan

Following is the deployment plan:

- Phase One: Limited remote access rollout in Chicago
- Phase Two: Limited wireless rollout in Chicago
- Phase Three: Rollout to all of USA
- Phase Four: Rollout to rest of the world

Phase One: Remote Access

Design considerations include:

- User database
- Authentication protocol
- Cisco Secure ACS for Windows or Cisco Secure ACS Solution Engine

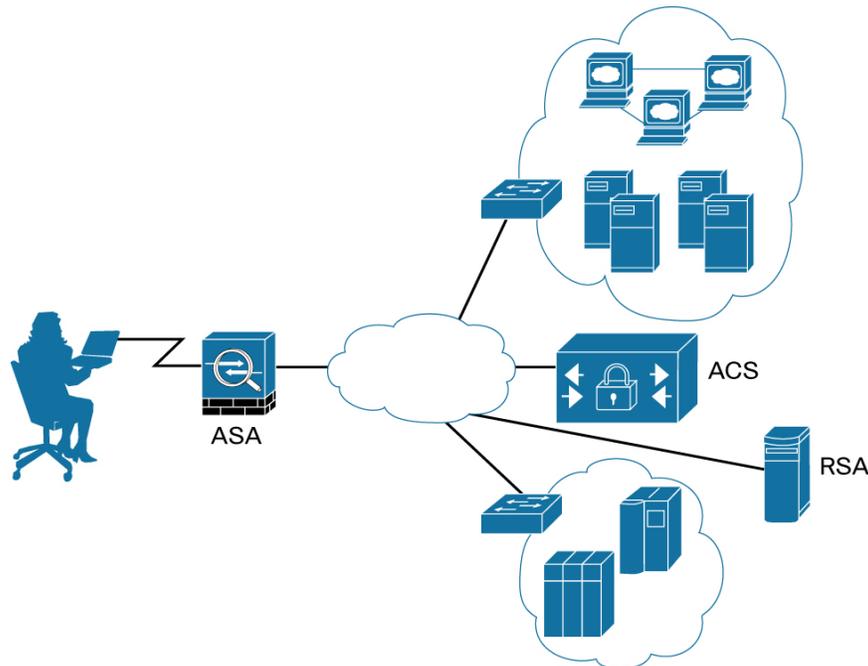
- Management (configuration, replication, logging)
- Scalability and performance

In this scenario, the design team decided to use RSA SecurID OTP for the extra password security that it provides. The use of OTP is common for remote access. The other decision, which is to use Cisco Secure ACS Solution Engine, further dictates the use of the RADIUS interface for RSA SecurID OTP. The team selected Cisco Secure ACS Solution Engine because the company purchase criteria made it easier to procure. Management of the Cisco Secure ACS Solution Engine will be done through the web interface. Two Cisco Secure ACS Solution Engines will be used for redundancy, and replication will be done from a primary to a secondary. Load balancing provides access for the ASA VPN concentrators to the two Cisco Secure ACS systems. Both Cisco Secure ACS systems will be in the same location. The company will add Cisco Secure ACS systems as traffic increases.

Because both Cisco Secure ACS installations will be performing authentication for both remote access and wireless, which require different authentication methods, Cisco Secure ACS will require the separation of the wireless and VPN configurations into separate NDG. Additionally, Cisco Secure ACS will require the use of NAP and NAF for separation of RADIUS policies between wireless and remote access.

Figure 9 shows the general concept.

Figure 9. Remote Access Design



Cisco Secure ACS Configuration

Configuration aspects include:

- RADIUS OTP Servers
- VPN concentrators and grouping: NDGs, NAFs
- Authorization parameters: dACLs
- NAP

The first step is to configure Cisco Secure ACS to use the RSA RADIUS server for external database authentication. To configure Cisco Secure ACS as a RADIUS client to the RSA RADIUS server:

1. Choose **Network Access Profiles > Database Configuration > RADIUS Token Server Create New Configuration**.
2. Enter the name *ChicagoA Configuration*. This will take you back to the RADIUS Token Server page.
3. In **External User Database Configuration** box, choose **ChicagoA Configuration**, and click **Configure**.

The configuration is a basic RADIUS client configuration (See Figure 10).

Figure 10. Adding RADIUS OTP Server for RSA

RADIUS Token Server - ChicagoA Configuration.

RADIUS Configuration	
Primary Server Name/IP:	10.10.10.10
Secondary Server Name/IP:	10.10.10.11
Shared Secret:	Rtfl45fwerdmky!
Authentication Port:	1812
Timeout (seconds):	10
Retries:	3
Failback Retry Delay (minutes):	5

Once you have configured Cisco Secure ACS as a RADIUS client to the RSA RADIUS server for external database authentication, you need to create entries in Cisco Secure ACS for the VPN concentrators. These are standard network device entries in the NDG "ASAs-Chicago", as shown in Figure 11.

Figure 11. Configured AAA Clients

ASAs-Chicago AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
<u>ASA1</u>	10.10.10.5	RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)
<u>ASA2</u>	10.10.10.6	RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)

NAFs are required to specify the devices used to indicate the appropriate NAP. You can access NAFs through **Shared Profile Components** in the navigation bar. Figure 12 shows the configuration page for the NAF named “ASAs”. Figure 13 shows the configured “ASAs” NAF.

Figure 12. Configuring NAF

Network Access Filtering

Name:

Description:

Network Device Groups	Selected Items
(Not Assigned)	NDG:ASAs-Chicago
<input type="button" value="->"/>	

Figure 13. Configured NAF

Network Access Filtering ?	
Name	Description
ASAs	ASAs for Remote Access

One of the primary attributes in the “ASAs” NAF is dACLs. Figure 14 shows the dACL definition for VPN access and Figure 15 shows the completed dACL listed in **Shared Profile Components**.

Figure 14. Configuring dACL

Downloadable IP ACL Content

Name:

ACL Definitions
<pre> permit TCP any host 100.160.0.1 eq 80 log permit TCP any host 100.160.0.2 eq 23 log permit TCP any host 100.160.0.3 range 20 30 permit 6 any host HOSTNAME1 permit UDP any host HOSTNAME2 neq 53 deny 17 any host HOSTNAME3 lt 137 log deny 17 any host HOSTNAME4 gt 138 deny ICMP any 100.161.0.0 0.0.255.255 log permit TCP any host HOSTNAME5 neq 80 </pre>

Figure 15. Configured dACL

Downloadable IP ACLs 	
Name	Description
dACL1	Remote Access ACLs

Now you can configure the NAP. To configure the NAP:

1. Enter a name for the NAP (See Figure 16).
2. Check the **Active** check box to set the NAP as active.
3. From the **Network Access Filter** drop-down list, choose the NAF that will match the NAP to the appropriate network devices.

Figure 16. Configuring NAP

Profile Setup 	
Name:	Remote_Access
Description:	<div style="border: 1px solid gray; height: 80px;"></div>
Active:	<input checked="" type="checkbox"/>
Network Access Filter:	ASAs 

Figure 17 shows the configured NAP.

Figure 17. Configured NAP

Network Access Profiles 				
	Name	Policies	Description	Active
<input type="radio"/>	<u>Remote_Access</u>	<u>Protocols</u> <u>Authentication</u> <u>Posture Validation</u> <u>Authorization</u>		YES
<input type="button" value="Add Profile"/>		<input type="button" value="Add Template Profile"/>		
		<input type="button" value="Up"/> <input type="button" value="Down"/>		
The Up/Down buttons submit and save the sort order to the database.				
<input checked="" type="radio"/> Deny access when no profile matches				
<input type="radio"/> Grant access using global configuration, when no profile matches				

Now you can configure the authentication protocol for the NAP (See Figure 18) and the authentication external database (See Figure 19). These are PAP and RADIUS token server respectively.

Figure 18. Configuring Authentication Protocol for NAP

Figure 19. Configuring External Database

The last step is to select the Action or the RADIUS authorization. In this case, the dACL (See Figure 20) that was defined earlier.

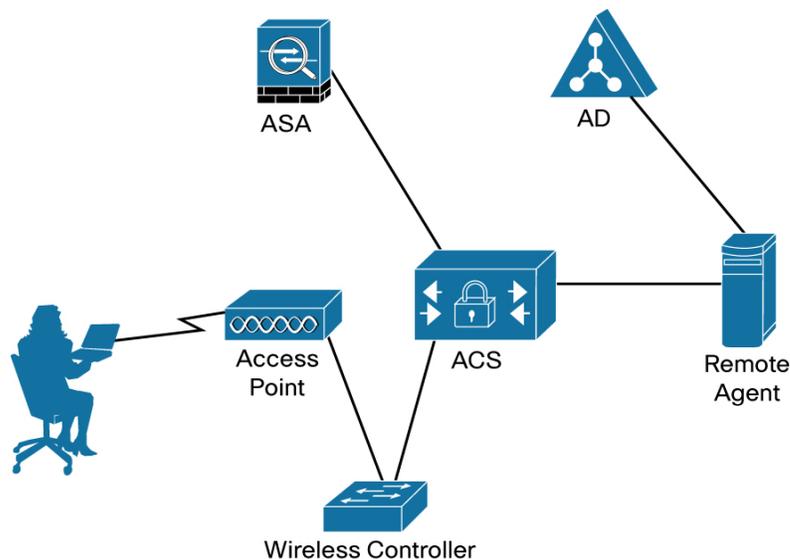
Figure 20. Configuring Authorization Rules

Authorization Rules for Remote_Access					
Condition			Action		
User Group	System Posture Token	Deny Access	Shared RAC	Downloadable ACL	
<input type="radio"/> Any	Any	<input type="checkbox"/>	<input type="checkbox"/>	dACL1	
If a condition is not defined or there is no matched condition:			<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Include RADIUS attributes from user's group <input type="checkbox"/> Include RADIUS attributes from user record					
<input type="button" value="Add Rule"/> <input type="button" value="Delete"/> <input type="button" value="Up"/> <input type="button" value="Down"/>					
The Up/Down buttons submit and save the sort order to the database.					
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>					

Phase Two: Wireless Access

Design considerations include:

- User database
- Authentication protocol
- Cisco Secure ACS for Windows or Cisco Secure ACS Solution Engine
- Management (configuration, replication, logging)
- Scalability and performance

Figure 21. Wireless Design

For wireless, the design team decided to use Windows AD for authentication. The use of AD is common for wireless access. The other decision, which is to use the Cisco Secure ACS Solution Engine, further dictates the use of the Cisco Secure ACS Remote Agents for accessing AD. The design team also selected EAP-FAST as the supplicant for the client systems because of its security and ease of deployment.

Cisco Secure ACS Configuration

Configuration aspects include:

- Wireless controllers and grouping
- Remote agent for AD authentication
- Authorization parameters (VLANs, group mappings, and so on)
- NAP

The first step is to configure the NDG that will contain the wireless devices as well as to configure the wireless devices themselves. The configuration of the wireless NDG and the wireless devices is similar to the configuration for ASAs described earlier. The resulting NDG is “Wireless-Chicago” (See Figure 22). The resulting wireless device configurations are shown in Figure 23. Note that the authentication method is “RADIUS (Cisco Airespace)” for these devices. This ensures proper attributes configuration for these devices.

Figure 22. Configured NDGs

Network Device Groups 			
Network Device Group	AAA Clients	AAA Servers	Remote Agents
ASAs-Chicago	2	0	0
Wireless-Chicago	2	0	0
(Not Assigned)	0	2	1

Figure 23. Configuring AAA Clients in “Wireless-Chicago” NDG

Wireless-Chicago AAA Clients 		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
WC1	10.10.10.12	RADIUS (Cisco Airespace)
WC2	10.10.10.13	RADIUS (Cisco Airespace)

In addition to NDGs and device configurations, Cisco Secure ACS requires the configuration of NAFs in conjunction with NAPs. The wireless NAF needs to be configured the same way as the ASA NAF described earlier.

To configure the wireless NAF, choose “Wireless-Chicago”. This results in the global NAF configuration shown in Figure 24.

Figure 24. Configured NAF

Network Access Filtering 	
Name	Description
ASAs	ASAs for Remote Access
Wireless	Wireless Controllers

The next step is to set up the remote agent. The remote agent is required for AD authentication on the Cisco Secure ACS Solution Engine.

4. Click **Submit**. This will take you back to the previous page. Click the domain you want to map.
5. Click **Add mapping** (See Figure 26). There may be a short delay while the remote agent retrieves group information from Windows and forwards it to Cisco Secure ACS.
6. In the **NT Groups** list of the **Define NT group set** box, click the group which you want to add to the Windows group set.
7. Click **Add to Selected**. This adds the group name to the **Selected** list.
8. In the Cisco Secure group list, click the Cisco Secure ACS group that will be the default group for the Windows users who belong to the defined Windows group set.
9. Click **Submit**.

Figure 26. Domain Group Mappings

Group Mappings for Domain : FLOP	
NT groups	ACS group
HR, *	HR
Finance, *	Finance
<input type="button" value="Add mapping"/>	<input type="button" value="Add manual mapping"/>
<input type="button" value="Order mappings"/>	

RACs are configurable sets of RADIUS attributes that you can assign to user or user group sessions dynamically based on a policy. You need to use the NAP configuration to create an authorization policy that maps from set conditions such as NDGs and posture to the shared RAC.

To add an RAC:

1. Choose **Shared Profile Components > RADIUS Authorization Components**.
2. Click **Add**.
3. Enter the name you want to assign to the RAC.
4. Choose the desired vendor attribute from the drop-down list, and click **Add**.
5. Click **Submit**. Figure 27 shows the configured RACs.

Repeat the procedure for the number of RACs that you require.

Figure 27. RADIUS Authorization Components

RADIUS Authorization Components	
Name	Description
VLAN-Finance	Vlan for Finance
VLAN-HR	Vlan for HR

The 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 the EAP-FAST tunnel establishment is based on strong secrets that are unique to users. Cisco Secure ACS generates these secrets called PACs by using a master key known only to Cisco Secure ACS. Because handshakes based on shared secrets are intrinsically faster than handshakes based on 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.

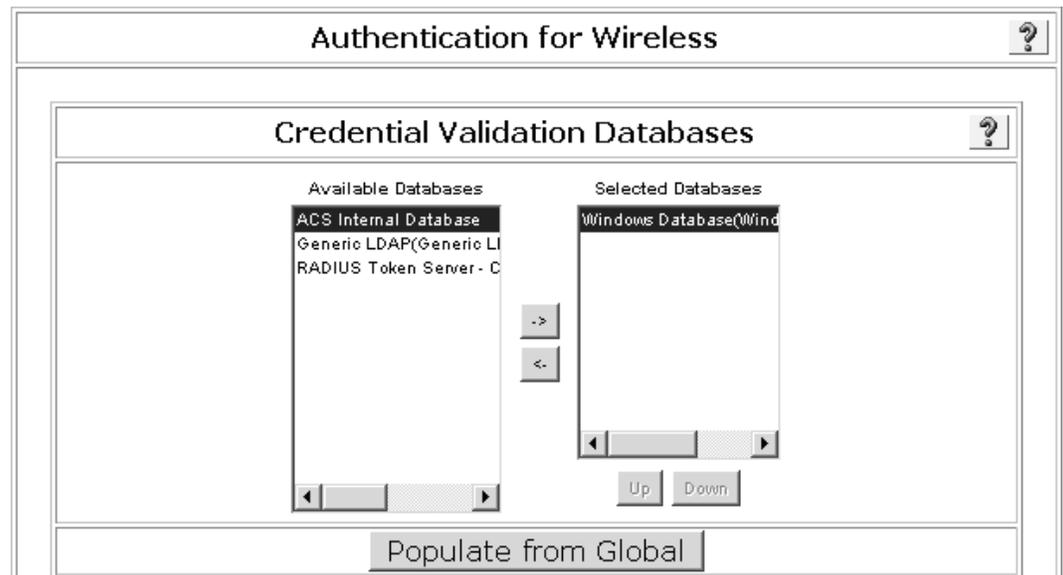
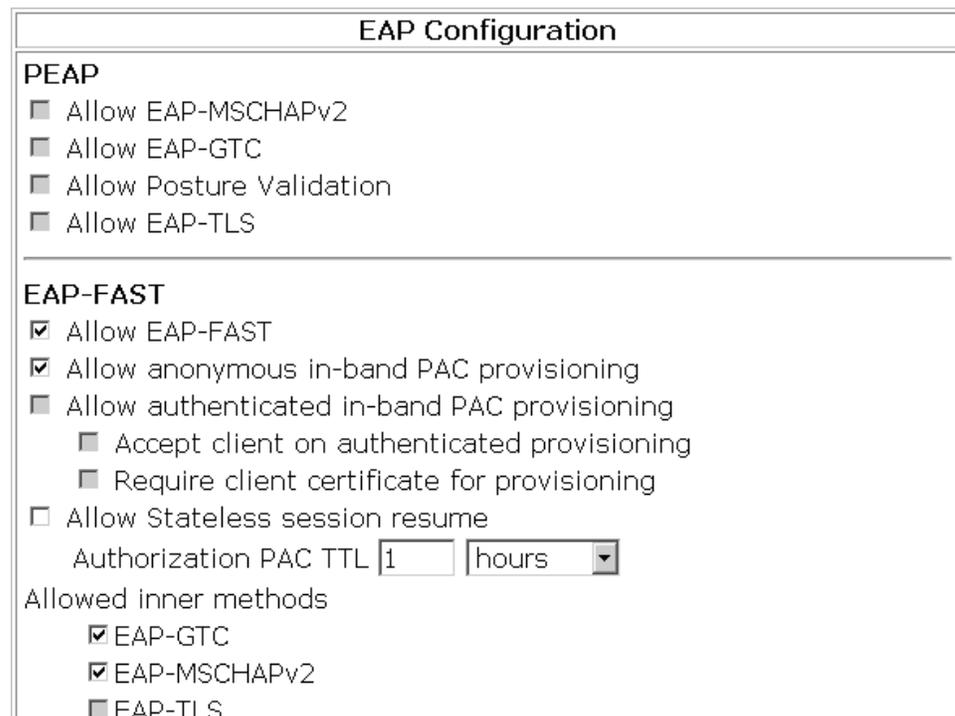
EAP-FAST occurs in three phases. The first phase is phase zero. Phase zero is a tunnel-secured means of providing an EAP-FAST end-user client with a PAC for the user requesting network access. Providing a PAC to the end-user client is the sole purpose of phase zero. Cisco Secure ACS and supplicant establish the tunnel based on an anonymous Diffie-Hellman key exchange. This optional phase of EAP-FAST does require the configuration of a certificate on Cisco Secure ACS. This can be a self-signed certificate or a server certificate provided by a third-party certificate server. The standard certificate configuration for Cisco Secure ACS is required. Figure 28 shows a successful certificate configuration.

Figure 28. Cisco Secure ACS Certificate Installation

Install ACS Certificate



At this point, you can configure the NAP for wireless devices. You can do this in the same manner as was done for the remote access NAP. Figure 29 shows the authentication configuration for AD. Figure 30 shows the configuration for EAP-FAST in the Protocols section of the NAP.

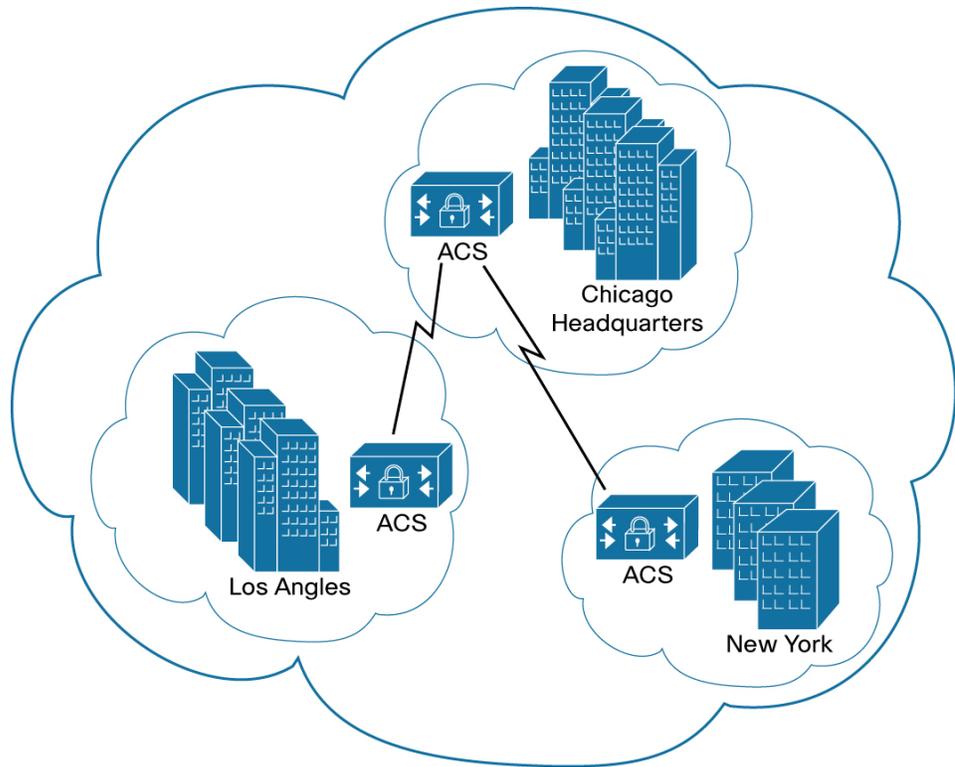
Figure 29. NAP Active Directory Configuration**Figure 30.** Figure 30 EAP-FAST NAP Selection

Once the network access profile is complete, Cisco Secure ACS is ready.

Phase Three: USA Rollout

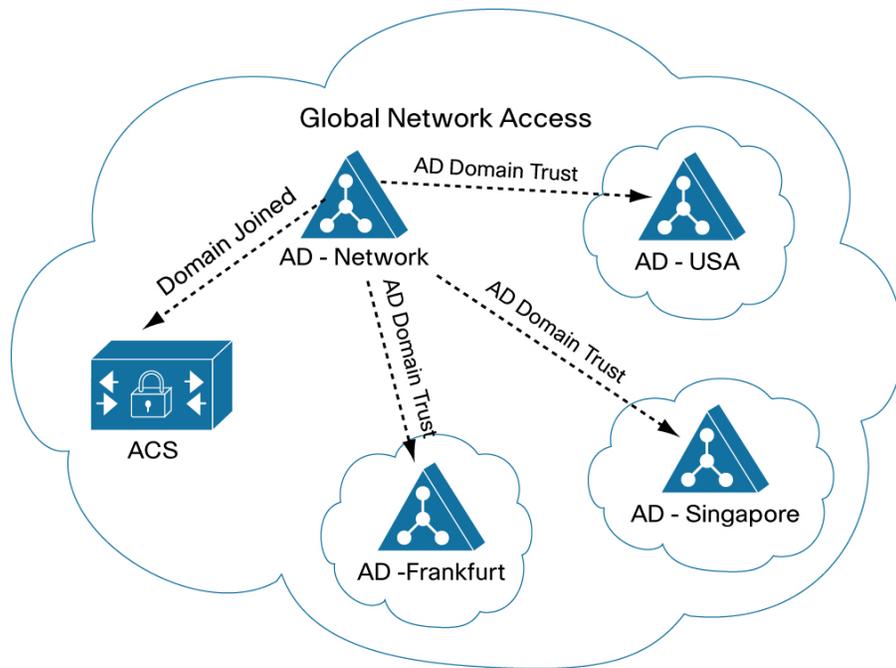
After the successful testing of the network access in Chicago, Binary Flip Flops rolls out the network access configuration to Los Angeles and New York.

Figure 31. USA Rollout



Phase Four: Global Rollout

Once Binary Flip Flops is satisfied that the USA rollout is successful, the plan is rolled to the rest of their subsidiaries in Singapore and Germany.

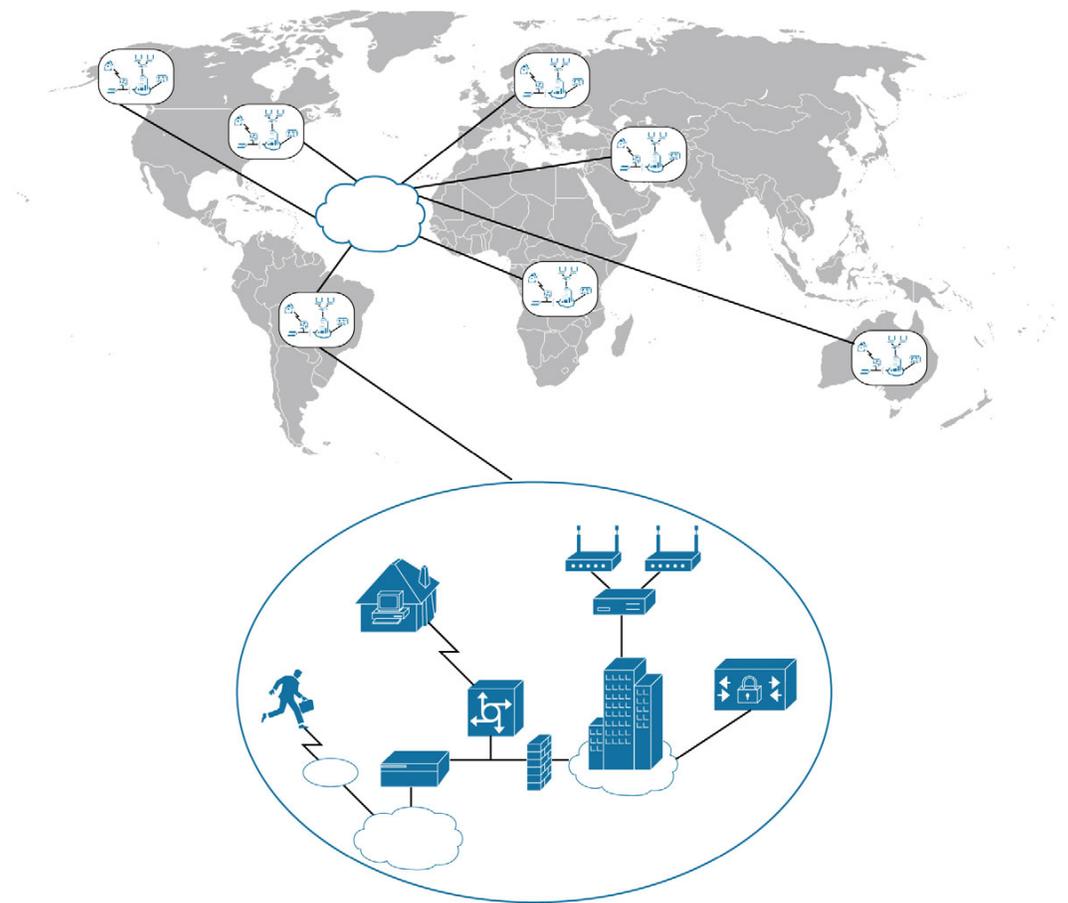
Figure 32. Figure 32 Global Rollout

Conclusion

The factors that govern how you deploy Cisco Secure ACS are closely interconnected. There is a close relation between network topology and network speed/reliability. Access and security policies are connected to network topology and database issues. Almost any combination is possible. When AAA was first conceived, the main purpose was to provide a centralized point of control for user access through dial-in services. As the user base grew, we saw a wider distribution in the locations of the access servers. We also saw the need for increase in AAA security services. First regional and then global requirements became common. Today, Cisco Secure ACS is required to provide AAA services for dial-in access, dial-out access, wireless, VLAN access, firewalls, VPN concentrators, and administrative control. The list continues to grow. As networks combine through acquisitions and mergers, multiple databases are increasingly used.

It is possible to have a large, dispersed, mixed environment. A combination of remote access via dial-in and VPN, along with local access via wireless is becoming more popular. Add to the mix, local access control via VLAN authentication, and a complex intranet emerges. Figure 33 shows how complex the enterprise network can become. These environments require multiple Cisco Secure ACS deployment.

The inclusion of external databases in this topology necessitates the deployment of multiple installations of the database server as well. If different databases are in use, the administrator will have to configure Cisco Secure ACS regionally to accommodate the differing formats. For instance, if North America is using LDAP but Asia is using Active Directory (AD), the North American Cisco Secure ACS should check the LDAP database first. It can also be configured to check the Asian AD database, but because there will be fewer requests to that database, it can be further down the list in external database configuration. The converse is true for the Asian Cisco Secure ACS. If regions share a common database, synchronized installations should be located in each region and served by their own Cisco Secure ACS. In the event that there is a single, centrally administered, unified database, we recommend that there be multiple Cisco Secure ACS and database installations throughout the regions. You can use database replication and synchronization to permit timely access to the local LAN.

Figure 33. Figure 33 World Deployment Scheme

If a regional topology has no central “campus” but is distributed with similarly sized “mini campuses” that are interconnected with T1, fiber optics, or similar technology, a central Cisco Secure ACS can be employed to service the AAA needs of each building. The possibility of compromising the link is low, and access speeds should be adequate to handle timely authentication.

For More Information

The complete product documentation can be found at

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/acs41/index.htm

Additional whitepapers can be found at

http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_white_papers_list.html

Additional configuration guides can be found at

http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_configuration_examples_list.html



Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)