



Overview

This chapter contains an overview of the Cisco Secure Access Control Server Release 4.0 Solution Engine, hereafter referred to as ACS.

The following topics are presented:

- [Introduction to ACS, page 1-1](#)
- [ACS Features, Functions and Concepts, page 1-2](#)
- [Managing and Administrating ACS, page 1-15](#)
- [ACS Specifications, page 1-21](#)

Introduction to ACS

ACS is a scalable, high-performance Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System (TACACS+) security server. As the centralized control point for managing enterprise network users, network administrators, and network infrastructure resources, ACS provides a comprehensive identity-based network-access control solution for Cisco intelligent information networks.

ACS extends network-access security by combining traditional authentication, authorization, and accounting (AAA - pronounced “triple A”) with policy control. ACS enforces a uniform network-access security policy for network administrators and other network users.

ACS supports a broad variety of Cisco and other network-access devices (NADs), also known as AAA clients, including:

- Wired and wireless LAN switches and access points
- Edge and core routers
- Dialup and broadband terminators
- Content and storage devices
- Voice over IP (VoIP)
- Firewalls
- Virtual private networks (VPNs)

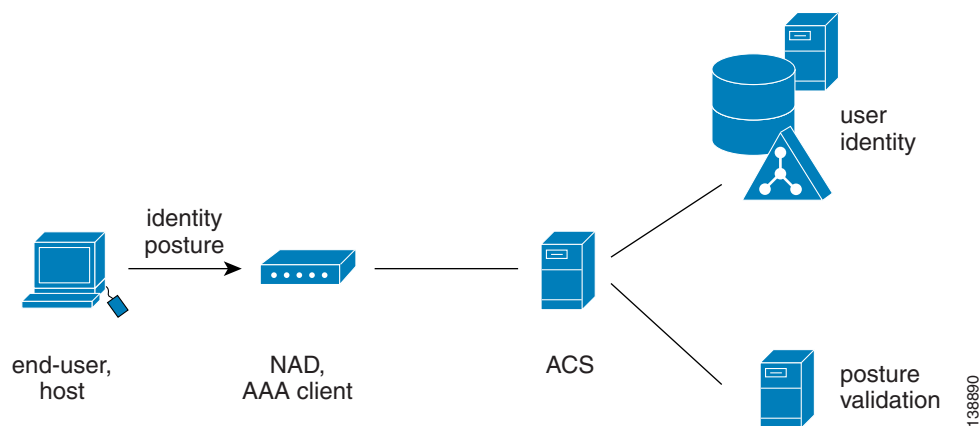
[Figure 1-1 on page 1-2](#) illustrates the role of ACS as a traditional network access control/AAA server.

Figure 1-1 A Simple AAA Scenario



ACS is a critical component of the Cisco Network Admission Control (NAC) framework. Cisco NAC is a Cisco Systems-sponsored industry initiative that uses the network infrastructure to enforce security-policy compliance on all machines seeking to access network computing resources, thereby limiting damage from viruses and worms. With NAC, network access to compliant and trusted PCs can be permitted, while the access of noncompliant devices can be restricted. See [Figure 1-2](#).

Figure 1-2 ACS Extended to NAC



ACS is also an important component of the Cisco Identity-Based Networking Services (IBNS) architecture. Cisco IBNS is based on Extensible Authentication Protocol (EAP) and on port-security standards such as IEEE 802.1x (a standard for port-based network-access control) to extend security authentication, authorization, and accounting from the perimeter of the network to every connection point inside the LAN. New policy controls such as per-user quotas, virtual LAN (VLAN) assignments, and access-control lists (ACLs) can be deployed, due to the extended capabilities of Cisco switches and wireless access points to query ACS over the RADIUS protocol.

ACS Features, Functions and Concepts

ACS incorporates many technologies to render AAA services to network-access devices, and provides a central access-control function.

This section contains the following topics:

- [ACS as the AAA Server, page 1-3](#)
- [AAA Protocols—TACACS+ and RADIUS, page 1-3](#)
- [Additional Features in ACS Version 4.0, page 1-4](#)

ACS as the AAA Server

From the perspective of the NAD, ACS functions as the AAA server. You must configure the device, which functions as a AAA client from the ACS perspective, to direct all end-user host access requests to ACS, via the TACACS+ or RADIUS protocols.

TACACS+ is traditionally used to provide authorization for network administrative operations on the network infrastructure itself; RADIUS is universally used to secure the access of end-users to network resources.

Basically, the NAD serves as the network gatekeeper, and sends an access request to ACS on behalf of the user. ACS verifies the username, password and possibly other data by using its internal database or one of the configured external identity directories. ACS ultimately responds to the NAD with an access denied or an access-accept message with a set of authorization attributes. When ACS is used in the context of the NAC architecture, additional machine data, known as *posture*, is validated as well, before the user is granted access to the network.

AAA Protocols—TACACS+ and RADIUS

ACS can use the TACACS+ and RADIUS AAA protocols.

Table 1-1 compares the two protocols.

Table 1-1 TACACS+ and RADIUS Protocol Comparison

Point of Comparison	TACACS+	RADIUS
Transmission Protocol	TCP—Connection-oriented transport-layer protocol, reliable full-duplex data transmission	UDP—Connectionless transport-layer protocol, datagram exchange without acknowledgments or guaranteed delivery
Ports Used	49	Authentication and Authorization: 1645 and 1812 Accounting: 1646 and 1813
Encryption	Full packet encryption	Encrypts only passwords up to 16 bytes
AAA Architecture	Separate control of each service: authentication, authorization, and accounting	Authentication and authorization combined as one service
Intended Purpose	Device management	User access control

TACACS+

ACS conforms to the TACACS+ protocol as defined by Cisco Systems in draft 1.78. For more information, refer to the Cisco IOS software documentation at <http://www.cisco.com>.

RADIUS

ACS conforms to the RADIUS protocol as defined in the draft of April 1997 and in the following Requests for Comments (RFCs):

- RFC 2138, Remote Authentication Dial In User Service
- RFC 2139, RADIUS Accounting
- RFC 2284

- RFC 2865
- RFC 2866
- RFC 2867
- RFC 2868
- RFC 2869

The ports used for authentication and accounting have changed in RADIUS RFC documents. To support the older and newer RFCs, ACS accepts authentication requests on port 1645 and port 1812. For accounting, ACS accepts accounting packets on port 1646 and 1813.

In addition to support for standard Internet Engineering Task Force (IETF) RADIUS attributes, ACS includes support for RADIUS vendor-specific attributes (VSAs). We have predefined the following RADIUS VSAs in ACS:

- Cisco Building Broadband Service Manager (BBSM)
- Cisco IOS/PIX 6.0
- Cisco VPN 3000/ASA/PIX 7.x+
- Cisco VPN 5000
- Cisco Airespace
- Ascend
- Juniper
- Microsoft
- Nortel

ACS also supports up to 10 RADIUS VSAs that you define. After you define a new RADIUS VSA, you can use it as you would one of the RADIUS VSAs that come predefined in ACS. In the Network Configuration section of the ACS web interface, you can configure AAA clients to use a user-defined RADIUS VSA as the AAA protocol. In Interface Configuration, you can enable user-level and group-level attributes for user-defined RADIUS VSAs. In User Setup and Group Setup, you can configure the values for enabled attributes of a user-defined RADIUS VSA.

For more information about creating user-defined RADIUS VSAs, see [Custom RADIUS Vendors and VSAs, page 9-19](#).

Additional Features in ACS Version 4.0

ACS release 4.0 provides the following features that help fortify and protect networked business systems:

- **SNMP Support**—Cisco Secure ACS provides Simple Network Management Protocol (SNMP) support for the appliance only. The SNMP agent provides read-only SNMP v1 and SNMP v2c support. The supported Management Information Bases (MIBs) include:
 - MIB-II (1213) for Network Management of TCP/IP-based internets
 - MIB-II and LAN Manager MIB-II for Windows
 - Host Resources MIB (RFC 1514/2790)

You use the appliance configuration page to configure the SNMP agent.

ACS release 4.0 does not introduce new features to the SNMP support.

- **Cisco NAC support**—ACS 4.0 acts as a policy decision point in NAC deployments. Using configurable policies, it evaluates and validates the credentials received from the Cisco Trust Agent (CTA, posture), determines the state of the host, and sends a per-user authorization to the network-access device: ACLs, a policy based access control list, or a private VLAN assignment. Evaluation of the host credentials can enforce many specific policies, such as OS patch level and antivirus DAT file version. ACS records the policy evaluation result for use with monitoring systems. ACS 4.0 also allows hosts without the appropriate agent technology to be audited by third party Audit Vendors, before granting network access. ACS policies can be extended with external policy servers to which ACS forwards posture credentials. For example, credentials specific to an antivirus vendor can be forwarded to the vendor's antivirus policy server, and audit policy requests can be forwarded to third-party audit products. For more information, see [Chapter 14, “Posture Validation.”](#)
- **Scalability improvements**—ACS 4.0 has been upgraded to use an industry standard relational database management system (RDBMS), improving the number of devices (AAA clients) by tenfold and the number of users by threefold. There have also been significant improvements in performance (transactions per second) across the protocol portfolio that ACS supports.
- **Network Access Profiles**—ACS 4.0 supports a new feature called Network Access Profiles (NAPs). Profiles allow administrators to classify access requests according to network location, membership in a network device group (NDG), protocol type, or other specific RADIUS attribute values sent by the network-access device through which the user connects. You can map AAA policies to specific profiles. For example, you can apply a different access policy for wireless access and remote (VPN) access. For more information, see [Chapter 15, “Network Access Profiles.”](#)
- **Extended replication components**—ACS 4.0 has improved and enhanced replication. Administrators now can replicate NAPs, and all related configurations, including:
 - posture validation settings
 - AAA clients and hosts
 - external database configuration
 - global authentication configuration
 - network device groups
 - dictionaries
 - shared-profile components
 - additional logging attributes
- **Cisco Security Agent (CSA) integration**—The ACS Solution Engine ships with a preinstalled, standalone CSA. This integration in the base appliance image helps to protect the ACS Solution Engine from day-zero attacks. The behavior-based technology available with CSA protects the ACS Solution Engine against the constantly changing threats from viruses and worms.
- **EAP Flexible Authentication via Secured Tunnel (EAP-FAST) support**—ACS supports the EAP-FAST protocol, a new publicly accessible IEEE 802.1X EAP type developed by Cisco Systems. Unlike Protected Extensible Authentication Protocol (PEAP), the EAP-FAST protocol protects authentication in a Transport Layer Security (TLS) tunnel that does not require the use of certificates. Cisco developed EAP-FAST to support customers who cannot enforce a strong password policy and wish to deploy an 802.1X EAP type that:
 - Does not require digital certificates
 - Supports a variety of user and password database types
 - Supports password expiration and change
 - Is flexible, easy to deploy, and easy to manage

For example, a customer who uses Cisco Lightweight and Efficient Application Protocol (LEAP) can migrate to EAP-FAST for protection from dictionary attacks. ACS supports EAP-FAST supplicants that are available on Cisco-compatible client devices, and Cisco Aironet 802.11a/b/g PCI and CardBus WLAN client adapters.

- **Downloadable IP ACLs** — ACS 4.0 extends per-user ACL support to any Layer 3 network device that supports this feature, such as Cisco PIX® firewalls, Cisco VPN solutions, and Cisco IOS routers. You can define sets of ACLs that can be applied per user or per group. This feature complements NAC support by enforcing the correct ACL policy. When used in conjunction with network-access filters (NAFs), you can apply downloadable ACLs differently per device. You can, therefore, tailor ACLs uniquely per user, per access device.
- **Certification Revocation List (CRL) Comparison**—ACS 4.0 supports certificate revocation by using the X.509 CRL profile. A CRL is a time-stamped list identifying revoked certificates; the list is signed by a certificate authority or CRL issuer, and made freely available in a public repository. ACS 4.0 periodically retrieves the CRLs from provisioned CRL Distribution Points by using Lightweight Directory Access Protocol (LDAP) or HyperText Transfer Protocol (HTTP), and stores them for use during EAP-Transport Layer Security (EAP-TLS) authentication. If the retrieved CRL contains the certificate that the user presents during an EAP-TLS authentication, ACS fails the authentication and denies access to the user. This capability is crucial due to frequent organizational changes and protects valuable company assets in case of fraudulent network use.
- **Machine Access Restrictions (MAR)**—ACS 4.0 includes MARs as an enhancement of Windows machine authentication. When Windows machine authentication is enabled, you can use MARs to control authorization of EAP-TLS, EAP-FASTv1a, and Microsoft Protected Extensible Authentication Protocol (PEAP) users who authenticate with a Windows external user database. Users who access the network with a computer that has not passed machine authentication within a configurable length of time are given the authorizations of a user group that you specify and which you can configure to limit authorization as needed. Alternatively, you can deny network access altogether.
- **Network Access Filter (NAF)**—ACS 4.0 includes NAFs as a new type of Shared Profile Component. NAFs provide a flexible way to apply network-access restrictions and downloadable ACLs on network device names, network device groups, or their IP address. NAFs applied by IP addresses can use IP address ranges and wildcards. This feature introduces granular application of network-access restrictions and downloadable ACLs, which previously supported only the use of the same access restrictions or ACLs to all devices. You can use NAFs to define flexible network device restriction policies to be defined, a requirement that is common in large environments.

Authentication

Authentication determines user identity and verifies the information. Traditional authentication uses a name and a fixed password. More secure methods use technologies such as Challenge Authentication Handshake Protocol (CHAP) and One-time Passwords (OTPs). ACS supports a variety of these authentication methods.

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

This section contains the following topics:

- [Authentication Considerations, page 1-7](#)
- [Authentication and User Databases, page 1-7](#)
- [Authentication Protocol-Database Compatibility, page 1-7](#)

- [Passwords, page 1-8](#)
- [Other Authentication-Related Features, page 1-11](#)

Authentication Considerations

Username and password is the most popular, simplest, and least-expensive method of authentication. The disadvantage is that this information can be told to someone else, guessed, or captured. Simple unencrypted username and password is not considered a strong authentication mechanism but can be sufficient for low authorization or privilege levels such as Internet access.

You should use encryption to reduce the risk of password capturing on the network. Client and server access-control protocols such as TACACS+ and RADIUS encrypt passwords to prevent them from being captured within a network. However, TACACS+ and RADIUS operate only between the AAA client and ACS. Before this point in the authentication process, unauthorized persons can obtain clear-text passwords, such as:

- The communication between an end-user client dialing up over a phone line
- An Integrated Services Digital Network (ISDN) line terminating at a network-access server
- Over a Telnet session between an end-user client and the hosting device

Authentication and User Databases

ACS supports a variety of user databases. It supports the ACS internal database and several external user databases, including:

- Windows User Database (for ACS Windows or for the Solution Engine remote agent)
- Generic LDAP
- Novell NetWare Directory Services (NDS) (only through Generic LDAP support)
- LEAP Proxy Remote Access Dial-In User Service (RADIUS) servers
- RADIUS-compliant token servers



Note For more information about token server support, see [Token Server User Databases, page 13-37](#).

Authentication Protocol-Database Compatibility

The various password protocols that ACS supports for authentication are supported unevenly by the various databases that ACS supports. For more information about the password protocols that ACS supports, see [Passwords, page 1-8](#).

[Table 1-2](#) specifies non-EAP authentication protocol support.

Table 1-2 Non-EAP Authentication Protocol and User Database Compatibility

Database	ASCII/PAP	CHAP	ARAP	MS-CHAP v.1	MS-CHAP v.2
ACS	Yes	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	No	Yes	Yes
Windows AD	Yes	No	No	Yes	Yes

Table 1-2 Non-EAP Authentication Protocol and User Database Compatibility (continued)

Database	ASCII/PAP	CHAP	ARAP	MS-CHAP v.1	MS-CHAP v.2
LDAP	Yes	No	No	No	No
ODBC	Yes	Yes	Yes	Yes	Yes
LEAP Proxy RADIUS Server	Yes	No	No	Yes	Yes
All Token Servers	Yes	No	No	No	No

Table 1-3 specifies EAP authentication protocol support.

Table 1-3 EAP Authentication Protocol and User Database Compatibility

Database	LEAP	EAP-MD5	EAP-TLS	PEAP (EAP-GTC)	PEAP (EAP-MS CHAPv2)	EAP-FAST Phase Zero	EAP-FAST Phase Two
ACS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	No	Yes	Yes	Yes	Yes
Windows AD	Yes	No	Yes	Yes	Yes	Yes	Yes
LDAP	No	No	Yes	Yes	No	No	Yes
ODBC	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LEAP Proxy RADIUS Server	Yes	No	No	Yes	Yes	Yes	Yes
All Token Servers	No	No	No	Yes	No	No	No

Passwords

ACS supports many common password protocols:

- ASCII/Password Authentication Protocol (ASCII/PAP)
- CHAP
- MS-CHAP
- Lightweight and Efficient Application Protocol (LEAP)
- AppleTalk Remote Access Protocol (ARAP)

Passwords can be processed by using these password-authentication protocols based on the version and type of security-control protocol used (for example, RADIUS or TACACS+), and the configuration of the AAA client and end-user client. The following sections outline the different conditions and functions of password handling.

In the case of token servers, ACS acts as a client to the token server by using its proprietary API or its RADIUS interface, depending on the token server. For more information, see [About Token Servers and ACS, page 13-38](#).

Different levels of security can be concurrently used with ACS for different requirements. The basic user-to-network security level is PAP. Although it represents the unencrypted security, PAP does offer convenience and simplicity for the client. PAP allows authentication against the Windows database. With

this configuration, users need to log in only once. CHAP allows a higher level of security for encrypting passwords when communicating from an end-user client to the AAA client. You can use CHAP with the ACS internal database. ARAP support is included to support Apple clients.

Comparing PAP, CHAP, and ARAP

PAP, CHAP, and ARAP are authentication protocols that encrypt passwords. However, each protocol provides a different level of security.

- **PAP**—Uses clear-text passwords (that is, unencrypted passwords) and is the least sophisticated authentication protocol. If you are using the Windows user database to authenticate users, you must use PAP password encryption or Microsoft-Challenge Authentication Handshake Protocol (MS-CHAP).
- **CHAP**—Uses a challenge-response mechanism with one-way encryption on the response. CHAP enables ACS to negotiate downward from the most secure to the least secure encryption mechanism, and it protects passwords that are transmitted in the process. CHAP passwords are reusable. If you are using the ACS internal database for authentication, you can use PAP or CHAP. CHAP does not work with the Windows user database.
- **ARAP**—Uses a two-way challenge-response mechanism. The AAA client challenges the end-user client to authenticate itself, and the end-user client challenges the AAA client to authenticate itself.

MS-CHAP

ACS supports MS-CHAP for user authentication. Differences between MS-CHAP and standard CHAP are:

- The MS-CHAP Response packet is in a format compatible with Microsoft Windows and LAN Manager 2.x. The MS-CHAP format does not require the authenticator to store a clear-text or reversibly encrypted password.
- MS-CHAP provides an authentication-retry mechanism that the authenticator controls.
- MS-CHAP provides additional failure codes in the Failure packet Message field.

For more information on MS-CHAP, refer to RFC 2433 [Microsoft PPP CHAP Extensions](#) for RADIUS Attributes for MS-CHAP Support.

Basic Password Configurations

Several basic password configurations are available:



Note

These configurations are all classed as inbound authentication.

- **Single password for ASCII/PAP/CHAP/MS-CHAP/ARAP**—The most convenient method for the administrator when setting up accounts and the user when obtaining authentication. However, because the CHAP password is the same as the PAP password, and the PAP password is transmitted in clear text during an ASCII/PAP login, the CHAP password could be compromised.
- **Separate passwords for ASCII/PAP and CHAP/MS-CHAP/ARAP**—For a higher level of security, users can have two separate passwords. If the ASCII/PAP password is compromised, the CHAP/ARAP password can remain secure.
- **External user database authentication**—For authentication by an external user database, the user does not need a password stored in the ACS internal database. Instead, ACS records which external user database it should query to authenticate the user.

Advanced Password Configurations

ACS supports the following advanced password configurations:

- **Inbound passwords**—Passwords used by most ACS users. The TACACS+ and RADIUS protocols support these passwords. The passwords held in the ACS internal database and are not usually provided to an external source if an outbound password has been configured.
- **Outbound passwords**—The TACACS+ protocol supports outbound passwords that can be used, for example, when another AAA client and end-user client authenticate a AAA client. Passwords from the ACS internal database are then sent to the second AAA client and end-user client.
- **Token caching**—When token caching is enabled, ISDN users can connect (for a limited time) a second B Channel by using the same OTP that was entered during original authentication. For greater security, the B-Channel authentication request from the AAA client should include the OTP in the username value (for example, Fred`password`) while the password value contains an ASCII/PAP/ARAP password. The TACACS+ and RADIUS servers then verify that the token is still cached and validate the incoming password against the single ASCII/PAP/ARAP or separate CHAP/ARAP password, depending on the configuration that the user employs.

The TACACS+ SENDAUTH feature enables AAA clients to authenticate themselves to other AAA clients or an end-user clients via outbound authentication. The outbound authentication can be PAP, CHAP, or ARAP. With outbound authentication, the ACS password is given out. By default, ASCII/PAP or CHAP/ARAP password is used, depending on how this has been configured; however, we recommend that you configure the separate SENDAUTH password for the user so that ACS inbound passwords are never compromised.

If you want to use outbound passwords and maintain the highest level of security, we recommend that you configure users in the ACS internal user database with an outbound password that is different from the inbound password.

Password Aging

With ACS you can choose whether and how to employ password aging. Control for password aging may reside in the ACS internal database, or in an external Windows user database. Each password-aging mechanism differs as to requirements and setting configurations.

You use the password aging feature the ACS internal database controls to force users to change their passwords under any of the following conditions:

- Date exceeds: value (a date).
- After a specified number of logins.
- The first time a new user logs in.

For information on the requirements and configuration of the password aging feature that the ACS internal database controls, see [Enabling Password Aging for the ACS Internal Database, page 6-15](#).

You use the Windows-based password aging feature to control the following password aging parameters:

- Maximum password age in days.
- Minimum password age in days.

The methods and functionality of Windows password aging differ according to the Windows operating system release. For information on the requirements and configuration of the Windows-based password aging feature, see [Enabling Password Aging for Users in Windows Databases, page 6-19](#), and refer to your Windows system documentation.

User-Changeable Passwords

With ACS, you can install a separate program so that users can change their passwords by using a web-based utility. For more information about installing user-changeable passwords, see the *Installation and User Guide for Cisco Secure ACS User-Changeable Passwords* on <http://www.cisco.com>.

EAP Support

The EAP, based on IETF 802.1x, is an end-to-end framework that allows the creation of authentication types without changing AAA client configurations. For more information about EAP, see RFC 2284, [PPP Extensible Authentication Protocol \(EAP\)](#).

ACS supports the following varieties of EAP:

- **EAP-MD5**—An EAP protocol that does not support mutual authentication.
- **EAP-TLS**—EAP incorporating Transport Layer Security. For more information, see [EAP-TLS Deployment Guide for Wireless LAN Networks](#) and [EAP-TLS Authentication, page 10-2](#).
- **LEAP**—An EAP protocol used by Cisco Aironet wireless equipment; it supports mutual authentication.
- **PEAP**—Protected EAP, which is implemented with EAP-Generic Token Card (GTC) and EAP-MS-CHAPv2 protocols. For more information, see [PEAP Authentication, page 10-5](#).
- **EAP-FAST**—A faster means of encrypting EAP authentication, supports EAP-GTC authentication. For more information, see [EAP-FAST Authentication, page 10-8](#).

The architecture of ACS is extensible with regard to EAP; additional varieties of EAP will be supported as those protocols mature.

Other Authentication-Related Features

In addition to the authentication-related features discussed in this section, ACS provides additional features:

- Authentication of unknown users with external user databases. (See [About Unknown User Authentication, page 16-3](#).)
- Authentication of computers running Microsoft Windows. (See [Machine Authentication, page 13-10](#).)
- Support for the Microsoft Windows Callback feature. (See [Setting the User Callback Option, page 7-6](#).)
- Ability to configure user accounts, including passwords, by using an external data source. (See [About RDBMS Synchronization, page 9-17](#).)
- Ability for external users to authenticate via an enable password. (See [Setting TACACS+ Enable Password Options for a User, page 7-23](#).)
- Proxy of authentication requests to other AAA servers. (See [Proxy in Distributed Systems, page 4-3](#).)
- Configurable character string stripping from proxied authentication requests. (See [Stripping, page 4-4](#).)
- Self-signed server certificates. (See [Using Self-Signed Certificates, page 10-34](#).)
- Certificate revocation list checking during EAP-TLS authentication. (See [Managing Certificate Revocation Lists, page 10-30](#).)

Authorization

Authorization determines what a user is allowed to do. ACS can send user profile policies to AAA clients to determine which network services the user can access. You can configure authorization to give different users and groups different levels of service. For example, standard dial-up users might not have the same access privileges as premium customers and users. You can also differentiate by levels of security, access times, and services.

You can use the ACS access restrictions feature to permit or deny logins based on time-of-day and day-of-week. For example, you could create a group for temporary accounts that you can disable on specified dates. A service provider could then offer a 30-day free trial. You could use the same authorization to create a temporary account for a consultant with login permission that is limited to Monday through Friday, 9 A.M. to 5 P.M.

You can restrict users to a service or combination of services such as PPP, ARAP, Serial Line Internet Protocol (SLIP), or EXEC. After a user selects a service, you can restrict Layer 2 and Layer 3 protocols, such as IP and IPX, and you can apply individual access lists. Access lists on a per-user or per-group basis can restrict users from reaching parts of the network where critical information is stored or prevent them from using certain services, such as File Transfer Protocol (FTP) or Simple Network Management Protocol (SNMP).

One fast-growing service that providers offer and corporations adopt is a service authorization for Virtual Private Dial-Up Networks (VPDNs). ACS can provide information to the network device for a specific user to configure a secure tunnel through a public network, such as the Internet. The information can be for the access server (such as the home gateway for that user) or for the home gateway router to validate the user at the customer premises. In either case, ACS can be used for each end of the VPDN.

This section contains the following topics:

- [Max Sessions, page 1-12](#)
- [Dynamic Usage Quotas, page 1-13](#)
- [Shared Profile Components, page 1-13](#)
- [Support for Cisco Device-Management Applications, page 1-13](#)
- [Other Authorization-Related Features, page 1-14](#)

Max Sessions

Max Sessions is a useful feature for organizations that need to limit the number of concurrent sessions that are available to a user or a group:

- **User Max Sessions**—For example, an Internet service provider can limit each account holder to a single session.
- **Group Max Sessions**—For example, an enterprise administrator can allow the remote access infrastructure to be shared equally among several departments and limit the maximum number of concurrent sessions for all users in any one department.

In addition to enabling simple User and Group Max Sessions control, as an administrator you can use ACS to specify a Group Max Sessions value and a group-based User Max Sessions value; that is, a User Max Sessions value based on the group membership of the user. For example, an administrator can allocate a Group Max Sessions value of 50 to the group *Sales* and also limit each member of the *Sales* group to five sessions each. Therefore, no single member of a group account would be able to use more than five sessions at any one time, but the group could still have up to 50 active sessions.

For more information about the Max Sessions feature, see [Setting Max Sessions for a User Group, page 6-9](#) and [Setting Max Sessions Options for a User, page 7-11](#).

Dynamic Usage Quotas

You can use ACS to define network usage quotas for users. Using quotas, you can limit the network access of each user in a group or of individual users. You define quotas by duration of sessions or the total number of sessions. Quotas can be absolute; or based on daily, weekly, or monthly periods. To grant access to users who have exceeded their quotas, you can reset session quota counters as needed.

To support time-based quotas, we recommend enabling accounting update packets on all AAA clients. If update packets are not enabled, the quota is updated only when the user logs off and the accounting stop packet is received from the AAA client. If the AAA client through which the user is accessing your network fails, the session information is not updated. In the case of multiple sessions, such as with ISDN, the quota would not be updated until all sessions terminate, which means that a second channel will be accepted; even if the first channel has exhausted the quota that is allocated to the user.

For more information about usage quotas, see [Setting Usage Quotas for a User Group, page 6-10](#) and [Options for Setting User Usage Quotas, page 7-12](#).

Shared Profile Components

ACS provides a means for specifying authorization profile components that you can apply to multiple user groups and users. For example, you may have multiple user groups that have identical network-access restrictions. Rather than configuring the network-access restrictions several times, once per group, you can configure a network-access restriction set in the Shared Profile Components section of the web interface, and then configure each group to use the network-access restriction set that you created.

For information about the types of shared-profile components that ACS supports, see [About Shared Profile Components, page 5-1](#).

Support for Cisco Device-Management Applications

ACS supports Cisco device-management applications, such as by providing command authorization for network users who are using the management application to configure managed network devices. You provide support for command authorization for management application users by using unique command-authorization set types for each management application that is configured to use ACS for authorization.

ACS uses TACACS+ to communicate with management applications. For a management application to communicate with ACS, you must configure the management application in ACS as a AAA client that uses TACACS+. Also, you must provide the device-management application with a valid administrator name and password. When a management application initially communicates with ACS, these requirements ensure the validity of the communication.

Additionally, the administrator that the management application uses must have the Create New Device Command Set Type privilege enabled. When a management application initially communicates with ACS, it dictates to ACS the creation of a device command set type, which appears in the Shared Profile Components section of the web interface. It also dictates a custom service for TACACS+ to authorize. The custom service appears on the TACACS+ (Cisco IOS) page in the Interface Configuration section of the web interface. For information about enabling TACACS+ services, see [Protocol Configuration Options for TACACS+, page 3-7](#). For information about device command-authorization sets for management applications, see [Command Authorization Sets, page 5-24](#).

After the management application has dictated the custom TACACS+ service and device command-authorization set type to ACS, you can configure command-authorization sets for each role that the management application supports and apply those sets to user groups that contain network administrators or to individual users who are network administrators.

Other Authorization-Related Features

In addition to the authorization-related features discussed in this section, ACS provides these additional features:

- Group administration of users. (See [Chapter 6, “User Group Management.”](#))
- Ability to map a user from an external user database to a specific ACS group. (See [Chapter 17, “User Group Mapping and Specification.”](#))
- Ability to disable an account after a number of failed attempts, specified by the administrator. (See [Setting Options for User Account Disablement, page 7-13.](#))
- Ability to disable an account on a specific date. (See [Setting Options for User Account Disablement, page 7-13.](#))
- Ability to disable groups of users. (See [Group Disablement, page 6-3.](#))
- Ability to restrict time-of-day and day-of-week access. (See [Setting Default Time-of-Day Access for a User Group, page 6-5.](#))
- Network access restrictions (NARs) based on remote address caller line identification (CLID) and dialed number identification service (DNIS.) (See [Setting Network Access Restrictions for a User Group, page 6-6.](#))
- Downloadable ACLs for users or groups, enabling centralized, modular ACL management. (See [Downloadable IP ACLs, page 5-13.](#))
- Network access filters, which apply different downloadable ACLs and NARs based on a user’s point of entry into your network. (See [Network Access Filters, page 5-2.](#))
- Ability to enable or disable users based on the Network Access Profile configuration. (See [Configuring Authorization Policies, page 15-43.](#))
- IP pools for IP address assignment of end-user client hosts. (See [Setting IP Address Assignment Method for a User Group, page 6-21.](#))
- Per-user and per-group TACACS+ or RADIUS attributes. (See [Advanced Options, page 3-5.](#))
- Support for VoIP, including configurable logging of accounting data. (See [Enabling VoIP Support for a User Group, page 6-4.](#))

Accounting

AAA clients use the accounting functions that the RADIUS and TACACS+ protocols provide to communicate relevant data for each user session to the AAA server for recording. ACS writes accounting records according to the ACS product type for:

- ACS Windows, ACS writes accounting records to a comma-separated value (CSV) log file or ODBC database, depending on your configuration.
- The ACS Solution Engine, ACS writes accounting records to local CSV log files or to the remote logging agent.

You can easily import these logs into popular database and spreadsheet applications for billing, security audits, and report generation. You can also use a third-party reporting tool to manage accounting data.

The types of accounting logs that you can generate include:

- **TACACS+ Accounting**—Lists when sessions start and stop; records AAA client messages with username; provides caller line identification information; records the duration of each session.
- **TACACS+ Administration**—Lists commands entered on a network device with TACACS+ command authorization enabled.
- **RADIUS Accounting**—Lists when sessions stop and start; records AAA client messages with username; provides caller line identification information; records the duration of each session.
- **VoIP Accounting**—Lists VoIP session stop and start times, AAA client messages with usernames, caller line identification (CLID) information, and VoIP session duration.
- **Failed Attempts**—Lists authentication and authorization failures with an indication of the cause.
- **Passed Authentications**—Lists successful authentication requests.

For more information about ACS logging capabilities, see [Chapter 11, “Logs and Reports.”](#)

Other Accounting-Related Features

In addition to the accounting-related features in this section, ACS provides these additional features:

- Centralized logging for:
 - ACS Windows, allow several ACS installations to forward their accounting data to a remote ACS.
 - The ACS Solution Engine, uses the remote agent for centralized logging.

For more information, see [Remote Logging, page 11-13](#).

- Configurable supplementary user ID fields for capturing additional information in logs. (See [User Data Configuration Options, page 3-4](#).)
- Configurable logs, allowing you to capture as much information as needed. (See [Accounting Logs, page 11-4](#).)

Managing and Administrating ACS

ACS provides a flexible administration scheme to configure, maintain, and protect its AAA functionality. You can perform nearly all ACS administration tasks through the ACS web interface. You use the web interface to easily modify the ACS configuration from any connection on your LAN or WAN, and view it by using a web browser. For a list of supported browsers, see the latest version of the *Release Notes for Cisco Secure ACS Solution Engine 4.0* on <http://www.cisco.com>.

The web interface not only makes viewing and editing user and group information possible, you use it to restart services, add remote administrators, change AAA client information, back up the system, view reports from anywhere on the network, and more.

This section describes the ACS web interface and provides information about the following topics:

- [Web Interface Security, page 1-16](#)
- [Cisco Security Agent Integration, page 1-16](#)
- [HTTP Port Allocation for Administrative Sessions, page 1-18](#)

- [Web Interface Layout, page 1-18](#)
- [Uniform Resource Locator for the Web Interface, page 1-20](#)
- [Online Help and Online Documentation, page 1-20](#)

Web Interface Security

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

Administrative sessions time out after a configurable length of idle time. Regardless, we recommend that you log out of the web interface after each session. For information about configuring the idle timeout feature, see [Access Policy, page 12-8](#).

You can enable a secure socket layer (SSL) for administrative sessions. This method ensures that all communication between the web browser and ACS is encrypted. Your browser must support SSL. You can enable this feature on the Access Policy Setup page in the Administration Control section. For more information about enabling the SSL for web interface security, see [Access Policy, page 12-8](#).

Cisco Security Agent Integration

Cisco Security Agent (CSA) protects the ACS Solution Engine. Whether you have applied a CSA update to ACS or you are using an appliance base image that incorporates CSA, CSA helps to protect ACS from viruses, worms, and attacks. On the ACS Solution Engine, CSA operates in standalone mode, which Cisco has configured to permit ACS to normally operate while providing protection.



Note

The first appliance base image version that incorporates CSA is 3.3.1.3. You can determine the base image version of an appliance by using the **show** console command or the Appliance Upgrade Status page in the System Configuration section of the web interface.

This section contains the following topics:

- [CSA Service Management, page 1-16](#)
- [CSA Logging, page 1-17](#)
- [CSA Restrictions, page 1-17](#)
- [CSA Policies, page 1-17](#)

CSA Service Management

CSA runs on the appliance as an additional service, named **CSAgent**.

From the appliance console, you can use the **start**, **stop**, and **restart** commands to manage **CSAgent**. For more information about these commands, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine*.

From the HTML interface, you can use the Appliance Configuration page in the System Configuration section of the web interface to enable or disable **CSAgent**. For more information, see [Appliance Configuration, page 8-16](#).

CSA Logging

CSA writes two logs to the appliance hard drive, *CSALog* and *CSASecurityLog*. The size of each log is limited to 1 MB. When a CSA log exceeds 1 MB, CSA begins a new log file. ACS retains the three most recent files for each CSA log.

From the appliance console, you can use the **exportlogs** command to retrieve the CSA logs. For more information about the **exportlogs** command or using the console, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine*.

From the web interface, you can view the CSA logs by clicking the links on the View Diagnostic Logs page in the System Configuration section.

CSA Restrictions

The protection that CSA provides to the appliance imposes the following restrictions when **CSAgent** is enabled:

- **Upgrade and Patch Restriction**—You cannot apply upgrades or patches by using the Appliance Upgrade Status page in the System Configuration section or the **upgrade** command at the appliance console. To upgrade ACS or apply patches, you must first disable **CSAgent**.
- **ping Restriction**—CSA does not allow the ACS Solution Engine to respond to **ping** requests that it receives from other computers. CSA does not affect the use of the **ping** command at the appliance console. If you disable **CSAgent** to permit the ACS Solution Engine to respond to **ping** requests, no CSA protection is in place for as long as **CSAgent** is disabled.

For information about disabling CSAgent, see [CSA Service Management, page 1-16](#).

CSA Policies

CSA is configured with the following policies:

- **Application Control**—CSA permits execution of only those applications required for ACS to operate correctly. Because of this protection, you must disable CSA before applying an upgrade or patch.
- **File Access Control**—CSA permits file system access for only those applications required for ACS to correctly operate.
- **IP and Transport Control**—CSA provides the following protections:
 - Discards invalid IP headers.
 - Discards invalid transport headers.
 - Detects TCP/UDP port scans.
 - Cloaks the appliance to prevent port scans.
 - Prevents TCP blind session spoofing.
 - Prevents TCP SYN floods.
 - Blocks ICMP convert channels.
 - Blocks dangerous ICMP messages, including **ping**.
 - Prevents IP source routing.
 - Prevents trace routing.
- **E-mail Worm Protection**—CSA guards the appliance against e-mail worms.

- **Registry Access Control**—CSA permits registry access to only those applications requiring access for proper operation of the appliance.
- **Kernel Protection**—CSA does not allow kernel modules to be loaded after system startup is complete.
- **Trojan and Malicious Application Protection**—CSA provides the following protections. Applications cannot:
 - Write code to space owned by other applications.
 - Download and execute ActiveX controls.
 - Automatically execute downloaded programs.
 - Directly access operating system password information.
 - Write into memory owned by other processes.
 - Monitor keystrokes while accessing the network.

HTTP Port Allocation for Administrative Sessions

You use the HTTP port allocation feature to configure the range of TCP ports that ACS uses for administrative HTTP sessions. Narrowing this range with the HTTP port allocation feature reduces the risk of unauthorized access to your network through a port that is open for administrative sessions.

We do not recommend that you administer ACS through a firewall. Doing so requires that you configure the firewall to permit HTTP traffic over the range of HTTP administrative session ports that ACS uses. While narrowing this range reduces the risk of unauthorized access, a greater risk of attack remains if you allow administration of ACS from outside a firewall. A firewall that is configured to permit HTTP traffic over the ACS administrative port range must also permit HTTP traffic through port 2002, because a web browser must address this port to initiate an administrative session.



Note

A broad HTTP port range could create a security risk. To prevent accidental discovery of an active administrative port by unauthorized users, keep the HTTP port range as narrow as possible. ACS tracks the IP address that is associated with each administrative session. An unauthorized user would have to impersonate, or “spoof,” the IP address of the legitimate remote host to make use of the active administrative session HTTP port.

For information about configuring the HTTP port allocation feature, see [Access Policy, page 12-8](#).

Web Interface Layout

The web interface has three vertical partitions, known as frames:

- **Navigation Bar**—The gray frame on the left side of the browser window, the navigation bar contains the task buttons. Each button changes the configuration area to a unique section of the ACS application, such as the User Setup section or the Interface Configuration section. This frame does not change; it always contains the following buttons:
 - **User Setup**—Add and edit user profiles. For more information about the User Setup section, see [Chapter 7, “User Management.”](#)
 - **Group Setup**—Configure network services and protocols for groups of users. For more information about the Group Setup section, see [Chapter 6, “User Group Management.”](#)

- **Shared Profile Components**—Add and edit network-access restriction and command-authorization sets, to be applied to users and groups. For more information about the Shared Profile Components section, see [Chapter 5, “Shared Profile Components.”](#)
 - **Network Configuration**—Add and edit network-access devices and configure distributed systems. For more information about the Network Configuration section, see [Chapter 4, “Network Configuration.”](#)
 - **System Configuration**—Configure system-level features. Four chapters address this large section of the web interface. For information about fundamental features such as backup scheduling and service controls, see [Chapter 8, “System Configuration: Basic.”](#) For information about advanced features such as database replication, see [Chapter 9, “System Configuration: Advanced.”](#) For information about configuring authentication protocols and certificate-related features, see [Chapter 10, “System Configuration: Authentication and Certificates.”](#) For information about configuring logs and reports, see [Chapter 11, “Logs and Reports.”](#)
 - **Interface Configuration**—Display or hide product features and options to configure. For more information about the Interface Configuration section, [Chapter 3, “Using the Web Interface.”](#)
 - **Administration Control**—Define and configure access policies. For more information about the Administration Control section, [Chapter 12, “Administrators and Administrative Policy.”](#)
 - **External User Databases**—Configure databases, the Unknown User Policy, and user group mapping. For information about configuring databases, see [Chapter 13, “User Databases.”](#) For information about the Unknown User Policy, see [Chapter 16, “Unknown User Policy.”](#) For information about user group mapping, see [Chapter 17, “User Group Mapping and Specification.”](#)
 - **Posture Validation**—Control the degree of access that is permitted from computers that access your network through AAA clients that are configured to enforce NAC. For more information on posture validation, see [Chapter 14, “Posture Validation.”](#)
 - **Network Access Profiles**—Set up the conditions that allow a user to connect to the network and identify the way requests to access the network are applied. For more information on setting up Network Access Profiles and Profile-based Policies, see [Chapter 15, “Network Access Profiles.”](#)
 - **Reports and Activity**—Display accounting and logging information. For information about viewing reports, see [Chapter 11, “Logs and Reports.”](#)
 - **Online Documentation**—View the user guide. For information about using the online documentation, see [Online Help and Online Documentation, page 1-20.](#)
- **Configuration Area**—The frame in the middle of the browser window, the configuration area displays web pages that belong to one of the sections represented by the buttons in the navigation bar. The configuration area is where you add, edit, or delete information. For example, you configure user information in this frame on the User Setup Edit page.



Note Most pages have a Submit button at the bottom. Click **Submit** to confirm your changes. If you do not click Submit, the changes are not saved.

- **Display Area**—The pane on the right side of the browser window, the display area shows one of the following options:
 - **Online Help**—Displays basic help about the page that currently appears in the configuration area. This help does not offer in-depth information, rather it gives some basic information about what can be accomplished in the middle frame. For more information about online help, see [Using Online Help, page 1-20.](#)

- **Reports or Lists**—Displays lists or reports, including accounting reports. For example, in User Setup you can show all usernames that start with a specific letter. The list of usernames beginning with a specified letter appears in this section. The usernames are hyperlinks to the specific user configuration, so you click the name to edit that user.
- **System Messages**—Displays messages after you click Submit if you have typed in incorrect or incomplete data. For example, if the information that you entered in the Password box does not match the information in the Confirm Password box in the User Setup section, ACS displays an error message here. The incorrect information remains in the configuration area so that you can retype the information correctly and resubmit it.

Uniform Resource Locator for the Web Interface

You can access the ACS web interface by using one of the following uniform resource locators (URLs):

- `http://IP address:2002`
- `http://hostname:2002`

where *IP address* is the dotted decimal IP address and *hostname* is the hostname of the server that is running ACS. If you use the hostname, DNS must be functioning properly on your network or the hostname must be listed in the local hosts file of the computer that is running the browser.

If ACS is configured to use SSL to protect administrative sessions, you must specify the HTTPS protocol in the URLs:

- `https://IP address:2002`
- `https://hostname:2002`

If SSL is enabled and you do not specify HTTPS, ACS redirects the initial request to HTTPS for you. Using SSL to access the login page protects administrator credentials. For more information about enabling SSL to protect administrative sessions, see [Access Policy, page 12-8](#).

From the computer that is running ACS, you can also use the following URLs:

- `http://127.0.0.1:2002`
- `http://localhost:2002`

If SSL is enabled, you can specify the HTTP protocol in the URLs:

- `https://127.0.0.1:2002`
- `https://localhost:2002`

Online Help and Online Documentation

We provide two sources of information in the web interface:

- **Online Help**—Contains basic information about the page shown in the configuration area.
- **Online Documentation**—Contains the entire user guide.

Using Online Help

Online help is the default content in the display area. For every page that appears in the configuration area, there is a corresponding online help page. Each online help page contains a list of topics covered on that page.


The two help icons that appear on pages in ACS are:

- **Question Mark**—Many subsections of the pages in the configuration area contain an icon with a question mark (?). To jump to the applicable topic in an online help page, click the question mark (?) icon.
- **Back to Help**—Wherever you find an online help page with a Section Information icon, the corresponding page in the configuration area contains a Back to Help icon. If you have accessed the online documentation by clicking a Section Information icon and want to view the online help page again, click the Back to Help icon.

Using the Online User Guide

The user guide provides information about the configuration, operation, and concepts of ACS. The information in the online documentation is as current as the release date of the ACS version that you are using. For the latest documentation about ACS, click <http://www.cisco.com>.

To access online documentation:

-
- Step 1** In the ACS web interface, click **Online Documentation**.
- Step 2** If you want to select a topic from the table of contents, scroll through the table of contents and click the applicable topic.
- The online documentation for the topic selected appears in the display area.
- Step 3** If you want to select a topic from the index, click **Index** and scroll through the index to find an entry for the topic that you want.
-  **Tip** Use the lettered shortcut links to jump to a particular section of the index.
-
- Step 4** If you want to search for a specific string or topic in the online documentation, click **Search**, and then enter the string that you want.
- Step 5** If you want to access the entire user guide in PDF format, click, **View PDF**.
-

ACS Specifications



Note

For the hardware, operating system, third-party software, and network requirements, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine* at:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_soft/csacsapp/csapp40/install/index.htm.

This section contains the following topics:

- [System Performance Specifications, page 1-22](#)
- [ACS Windows Services, page 1-22](#)

System Performance Specifications

The performance capabilities of ACS are depend mostly on the Windows server it is installed on, your network topology and network management, the selection of user databases, and other factors. For example, ACS can perform many more authentications per second if it is using its internal user database and running on a computer that is using the fastest processor and network interface card available than if it is using external user databases and running on a computer that complies with the minimum system requirements. (See the *Installation and Setup Guide for Cisco Secure ACS Solution Engine*.)

The following items are general answers to common system-performance questions. The performance of ACS in your network depends on your specific environment and AAA requirements.

- **Maximum users supported by the ACS internal database**—There is no theoretical limit to the number of users the ACS internal database can support. We have successfully tested ACS with databases in excess of 100,000 users. The practical limit for a single ACS authenticating against all its databases, internal and external, is 300,000 to 500,000 users. This number increases significantly if the authentication load is spread across a number of replicated ACS instances.
- **Transactions per second**—Authentication and authorization transactions per second depend on many factors, most of which are external to ACS. For example, high network latency in communication with an external user database lowers the number of transactions per second that ACS can achieve.
- **Maximum number of AAA clients supported**—ACS has been tested to support AAA services for approximately 50,000 AAA client configurations. This limitation is primarily a limitation of the ACS memory.

If your network comprises tens of thousands of AAA clients, we recommend using multiple ACSs and assigning a manageable number of AAA clients to each ACS. For example, if you have 80,000 AAA clients, you could use four ACS servers and divide the AAA client load among them so that no single ACS manages more than 40,000 AAA client configurations. Then you can have overlapping AAA client support for backup AAA servers and not exceed the 50,000 AAA client limit. If you use replication to propagate configuration data among ACSs, limit replication of AAA client data to ACSs that serve the same set of AAA clients.

ACS Windows Services

ACS operates as a set of Microsoft Windows services. When you install ACS, the installation adds these Windows services to the server. These services provide the core of ACS functionality.

The ACS services on the computer running ACS include:

- **CSAdmin**—Provides the web interface for administration of ACS.
- **CSAuth**—Provides authentication services.
- **CSDBSync**—Provides synchronization of the ACS internal database with an external RDBMS application.
- **CSLog**—Provides logging services, for accounting and system activity.
- **CSMon**—Provides monitoring, recording, and notification of ACS performance, and behavior.
- **CS Tacacs**—Provides communication between TACACS+ AAA clients and the CSAuth service.
- **CSRADIUS**—Provides communication between RADIUS AAA clients and the CSAuth service.

For a full description of each service, see [Appendix F, “Internal Architecture.”](#)

You can start and stop each module individually from within the serial console and Microsoft Windows Service Control Panel or as a group from within the serial console or the ACS web interface. For information about stopping and starting ACS services by using the web interface, see [Service Control, page 8-1](#). For information about stopping and starting ACS services by using the serial console, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine*. For information on service logs and gathering data for troubleshooting, see [Service Logs, page 11-19](#).

Network administrators who offer increased levels of security services and corporations that want to lessen the chance of intruder access resulting from password capturing can use an OTP. ACS supports several types of OTP solutions, including PAP for Point-to-Point Protocol (PPP) remote-node login. Token cards are considered one of the strongest OTP authentication mechanisms.

