



# Overview

---

This chapter provides an overview of Cisco Secure ACS Solution Engine.

This chapter contains the following topics:

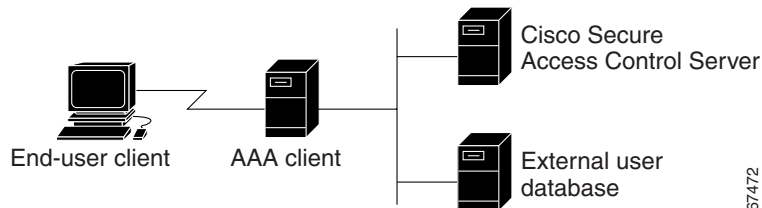
- [The Cisco Secure ACS Paradigm, page 1-2](#)
- [Cisco Secure ACS Specifications, page 1-3](#)
  - [System Performance Specifications, page 1-3](#)
  - [Cisco Secure ACS Services, page 1-4](#)
- [AAA Server Functions and Concepts, page 1-5](#)
  - [Cisco Secure ACS and the AAA Client, page 1-5](#)
  - [AAA Protocols—TACACS+ and RADIUS, page 1-6](#)
  - [Authentication, page 1-8](#)
  - [Authorization, page 1-16](#)
  - [Accounting, page 1-21](#)
  - [Administration, page 1-22](#)
  - [Posture Validation, page 1-27](#)
- [Cisco Secure ACS HTML Interface, page 1-28](#)
  - [About the Cisco Secure ACS HTML Interface, page 1-28](#)
  - [HTML Interface Layout, page 1-29](#)
  - [Uniform Resource Locator for the HTML Interface, page 1-32](#)
  - [Network Environments and Administrative Sessions, page 1-32](#)

- [Accessing the HTML Interface, page 1-34](#)
- [Logging Off the HTML Interface, page 1-35](#)
- [Online Help and Online Documentation, page 1-36](#)

## The Cisco Secure ACS Paradigm

Cisco Secure ACS provides authentication, authorization, and accounting (AAA—pronounced “triple A”) services to network devices that function as AAA clients, such as a network access server, PIX Firewall, or router. The AAA client in [Figure 1-1](#) represents any such device that provides AAA client functionality and uses one of the AAA protocols supported by Cisco Secure ACS.

**Figure 1-1 A Simple AAA Scenario**



Cisco Secure ACS centralizes access control and accounting, in addition to router and switch access management. With Cisco Secure ACS, network administrators can quickly administer accounts and globally change levels of service offerings for entire groups of users. Although the external user database shown in [Figure 1-1](#) is optional, support for many popular user repository implementations enables companies to put to use the working knowledge gained from and the investment already made in building their corporate user repositories.

Cisco Secure ACS supports Cisco AAA clients such as the Cisco 2509, 2511, 3620, 3640, AS5200 and AS5300, AS5800, the Cisco PIX Firewall, Cisco Aironet Access Point wireless networking devices, Cisco VPN 3000 Concentrators, and Cisco VPN 5000 Concentrators. It also supports third-party devices that can be configured with the Terminal Access Controller Access Control System (TACACS+) or the Remote Access Dial-In User Service (RADIUS) protocol. Cisco Secure ACS treats all such devices as AAA clients. Cisco Secure ACS uses the TACACS+ and RADIUS protocols to provide AAA

services that ensure a secure environment. For more information about support for TACACS+ and RADIUS in Cisco Secure ACS, see [AAA Protocols—TACACS+ and RADIUS](#), page 1-6.

# Cisco Secure ACS Specifications

This section provides information about Cisco Secure ACS performance specifications and the services that compose Cisco Secure ACS.

**Note**

---

For hardware specifications of the Cisco Secure ACS Solution Engine, see the *Installation and Setup Guide for Cisco Secure ACS Solution Engine*.

---

This section contains the following topics:

- [System Performance Specifications](#), page 1-3
- [Cisco Secure ACS Services](#), page 1-4

## System Performance Specifications

The performance capabilities of Cisco Secure ACS are heavily affected by your network topology and network management, the selection of user databases, and other factors. For example, Cisco Secure ACS can perform many more authentications per second if it is using its internal user database and is on a 1 GB Ethernet backbone than it can if it is using an external user database and is on a 10 MB LAN.

For more information about the expected performance of Cisco Secure ACS in your network setting, contact your Cisco sales representative. The following items are general answers to common system performance questions. The performance of Cisco Secure ACS in your network depends on your specific environment and AAA requirements.

- **Maximum users supported by the CiscoSecure user database**—There is no theoretical limit to the number of users the CiscoSecure user database can support. We have successfully tested Cisco Secure ACS with databases in excess of 100,000 users. The practical limit for a single Cisco Secure 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 Cisco Secure ACS.

- **Transactions per second per number of users**—Assuming 10,000 users in the CiscoSecure user database, Cisco Secure ACS provides 80 RADIUS full login cycles (authentication, accounting start, and accounting stop) per second and approximately 40 TACACS+ logins per second. As the database grows, this performance declines roughly proportionately.
- **Maximum number of AAA clients supported**—Cisco Secure ACS can support AAA services for approximately 5000 AAA client configurations. This limitation is primarily a limitation of the Cisco Secure ACS HTML interface. Performance of the HTML interface degrades when Cisco Secure ACS has more than approximately 5000 AAA client configurations. However, a AAA client configuration in Cisco Secure ACS can represent more than one physical network device, provided that the network devices use the same AAA protocol and use the same shared secret. If you make use of this ability, the number of actual AAA clients supported can be considerably higher than 5000.

## Cisco Secure ACS Services

Cisco Secure ACS operates as a set of services that provide the core of Cisco Secure ACS functionality. These services control the authentication, authorization, and accounting of users accessing networks. For a full discussion of each service, see [Chapter 1, “Overview”](#). The services on a Cisco Secure ACS Solution Engine include the following:

- **CSAdmin**—Provides the HTML interface for administration of Cisco Secure ACS.
- **CSAuth**—Provides authentication services.
- **CSDBSync**—Provides synchronization of the CiscoSecure user database with an external RDBMS application.
- **CSLog**—Provides logging services, both for accounting and system activity.
- **CSMon**—Provides monitoring, recording, and notification of Cisco Secure ACS performance, and includes automatic response to some scenarios.

- **CS Tacacs**—Provides communication between TACACS+ AAA clients and the CSAuth service.
- **CS Radius**—Provides communication between RADIUS AAA clients and the CSAuth service.

Each module can be started and stopped individually from the serial console or as a group from within the Cisco Secure ACS HTML interface or from the serial console for the appliance. For information about stopping and starting services using the HTML interface, see [Service Control, page 8-2](#). For information about stopping and starting services using the serial console, see *Installation and Setup Guide for Cisco Secure ACS Solution Engine*.

## AAA Server Functions and Concepts

Cisco Secure ACS is a AAA server, providing AAA services to network devices that can act as AAA clients.

As a AAA server, Cisco Secure ACS incorporates many technologies to render AAA services to AAA clients. Understanding Cisco Secure ACS requires knowledge of many of these technologies.

This section contains the following topics:

- [Cisco Secure ACS and the AAA Client, page 1-5](#)
- [AAA Protocols—TACACS+ and RADIUS, page 1-6](#)
- [Authentication, page 1-8](#)
- [Authorization, page 1-16](#)
- [Accounting, page 1-21](#)
- [Administration, page 1-22](#)
- [Posture Validation, page 1-27](#)

## Cisco Secure ACS and the AAA Client

A AAA client is software running on a network device that enables the network device to defer authentication, authorization, and logging (accounting) of user sessions to a AAA server. AAA clients must be configured to direct all end-user client access requests to Cisco Secure ACS for authentication of users and

authorization of service requests. Using the TACACS+ or RADIUS protocol, the AAA client sends authentication requests to Cisco Secure ACS. Cisco Secure ACS verifies the username and password using the user databases it is configured to query. Cisco Secure ACS returns a success or failure response to the AAA client, which permits or denies user access, based on the response it receives. When the user authenticates successfully, Cisco Secure ACS sends a set of authorization attributes to the AAA client. The AAA client then begins forwarding accounting information to Cisco Secure ACS.

When the user has successfully authenticated, a set of session attributes can be sent to the AAA client to provide additional security and control of privileges, otherwise known as authorization. These attributes might include the IP address pool, access control list, or type of connection (for example, IP, IPX, or Telnet). More recently, networking vendors are expanding the use of the attribute sets returned to cover an increasingly wider aspect of user session provisioning.

## AAA Protocols—TACACS+ and RADIUS

Cisco Secure ACS can use both 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
<b>Transmission Protocol</b>	TCP—connection-oriented transport layer protocol, reliable full-duplex data transmission	UDP—connectionless transport layer protocol, datagram exchange without acknowledgments or guaranteed delivery
<b>Ports Used</b>	49	Authentication and Authorization: 1645 and 1812 Accounting: 1646 and 1813
<b>Encryption</b>	Full packet encryption	Encrypts only passwords up to 16 bytes
<b>AAA Architecture</b>	Separate control of each service: authentication, authorization, and accounting	Authentication and authorization combined as one service
<b>Intended Purpose</b>	Device management	User access control

## TACACS+

Cisco Secure ACS conforms to the TACACS+ protocol as defined by Cisco Systems in draft 1.77. For more information, refer to the Cisco IOS software documentation or Cisco.com (<http://www.cisco.com>).

## RADIUS

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

- RFC 2138, Remote Authentication Dial In User Service
- RFC 2139, RADIUS Accounting
- 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 both the older and newer RFCs, Cisco Secure ACS accepts authentication requests on port 1645 and port 1812. For accounting, Cisco Secure ACS accepts accounting packets on port 1646 and 1813.

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

- Cisco IOS/PIX
- Cisco VPN 3000
- Cisco VPN 5000
- Ascend
- Juniper
- Microsoft
- Nortel

Cisco Secure 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 Cisco Secure ACS. In the Network Configuration section of the Cisco Secure ACS HTML interface, you can configure a AAA client to use a user-defined RADIUS VSA as its 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 9-28](#).

## Authentication

Authentication determines user identity and verifies the information. Traditional authentication uses a name and a fixed password. More modern and secure methods use technologies such as CHAP and one-time passwords (OTPs). Cisco Secure ACS supports a variety of these authentication methods.

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

This section contains the following topics:

- [Authentication Considerations, page 1-8](#)
- [Authentication and User Databases, page 1-9](#)
- [Authentication Protocol-Database Compatibility, page 1-10](#)
- [Passwords, page 1-11](#)
- [Other Authentication-Related Features, page 1-16](#)

## Authentication Considerations

Username and password is the most popular, simplest, and least expensive method used for authentication. No special equipment is required. This is a popular method for service providers because of its easy application by the client. 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.

To reduce the risk of password capturing on the network, use encryption. 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 the access control server. 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 or an ISDN line terminating at a network access server, or over a Telnet session between an end-user client and the hosting device.

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. Cisco Secure 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.

## Authentication and User Databases

Cisco Secure ACS supports a variety of user databases. It supports the CiscoSecure user database and several external user databases, including the following:

- Windows User Database
- Generic LDAP
- Novell NetWare Directory Services (NDS)
- RADIUS-compliant token servers



---

**Note**

For more information about token server support, see [Token Server User Databases, page 13-60](#).

---

## Authentication Protocol-Database Compatibility

The various password protocols supported by Cisco Secure ACS for authentication are supported unevenly by the various databases supported by Cisco Secure ACS. For more information about the password protocols supported by Cisco Secure ACS, see [Passwords, page 1-11](#).

[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
Cisco Secure ACS	Yes	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	No	Yes	Yes
Windows AD	Yes	No	No	Yes	Yes
LDAP	Yes	No	No	No	No
Novell NDS	Yes	No	No	No	No
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
Cisco Secure 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
Novell NDS	No	No	Yes	Yes	No	No	Yes

**Table 1-3 EAP Authentication Protocol and User Database Compatibility (Continued)**

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

## Passwords

Cisco Secure ACS supports many common password protocols:

- ASCII/PAP
- CHAP
- MS-CHAP
- LEAP
- EAP-MD5
- EAP-TLS
- PEAP(EAP-GTC)
- PEAP(EAP-MSCHAPv2)
- EAP-FAST
- ARAP

Passwords can be processed 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, Cisco Secure ACS acts as a client to the token server, using either its proprietary API or its RADIUS interface, depending on the token server. For more information, see [About Token Servers and Cisco Secure ACS, page 13-60](#).

Different levels of security can be concurrently used with Cisco Secure 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 CiscoSecure user database. ARAP support is included to support Apple clients.

## Comparing PAP, CHAP, and ARAP

PAP, CHAP, and ARAP are authentication protocols used to 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 MS-CHAP.
- **CHAP**—Uses a challenge-response mechanism with one-way encryption on the response. CHAP enables Cisco Secure ACS to negotiate downward from the most secure to the least secure encryption mechanism, and it protects passwords transmitted in the process. CHAP passwords are reusable. If you are using the CiscoSecure user database for authentication, you can use either 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

Cisco Secure ACS supports Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) for user authentication. Differences between MS-CHAP and standard CHAP are the following:

- 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 controlled by the authenticator.
- MS-CHAP provides additional failure codes in the Failure packet Message field.

For more information on MS-CHAP, refer to RFC draft-ietf-pppext-mschap-00.txt, RADIUS Attributes for MS-CHAP Support.

## EAP Support

The Extensible Authentication Protocol (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, go to [PPP Extensible Authentication Protocol \(EAP\) RFC 2284](#).

Cisco Secure 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-MSCHAPv2 protocols. For more information, see [PEAP Authentication, page 10-8](#).
- **EAP-FAST**—EAP Flexible Authentication via Secured Tunnel (EAP-FAST), a faster means of encrypting EAP authentication, supports EAP-GTC authentication. For more information, see [EAP-FAST Authentication, page 10-12](#).

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

## Basic Password Configurations

There are several basic password configurations:



### Note

---

These configurations are all classed as inbound authentication.

---

- **Single password for ASCII/PAP/CHAP/MS-CHAP/ARAP**—This is the most convenient method for both 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, there is the chance that the CHAP password can be compromised.

- **Separate passwords for ASCII/PAP and CHAP/MS-CHAP/ARAP**—For a higher level of security, users can be given 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 CiscoSecure user database. Instead, Cisco Secure ACS records which external user database it should query to authenticate the user.

## Advanced Password Configurations

Cisco Secure ACS supports the following advanced password configurations:

- **Inbound passwords**—Passwords used by most Cisco Secure ACS users. These are supported by both the TACACS+ and RADIUS protocols. They are held internally to the CiscoSecure user database and are not usually given up 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 a AAA client has to be authenticated by another AAA client and end-user client. Passwords from the CiscoSecure user database are then sent back 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 using the same OTP 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, *Fredpassword*) 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 either the single ASCII/PAP/ARAP or separate CHAP/ARAP password, depending on the configuration the user employs.

The TACACS+ SENDAUTH feature enables a AAA client to authenticate itself to another AAA client or an end-user client via outbound authentication. The outbound authentication can be PAP, CHAP, or ARAP. With outbound authentication, the Cisco Secure 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 the separate SENDAUTH password be configured for the user so that Cisco Secure 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 CiscoSecure user database with an outbound password that is different from the inbound password.

## Password Aging

With Cisco Secure ACS you can choose whether and how you want to employ password aging. Control for password aging may reside either in the CiscoSecure user database, or in a Windows user database. Each password aging mechanism differs as to requirements and setting configurations.

The password aging feature controlled by the CiscoSecure user database enables you force users to change their passwords under any of the following conditions:

- After a specified number of days.
- 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 controlled by the CiscoSecure user database, see [Enabling Password Aging for the CiscoSecure User Database, page 6-21](#).

The Windows-based password aging feature enables you 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 which Windows operating system you use and whether you employ Active Directory (AD) or Security Accounts Manager (SAM). For information on the requirements and configuration of the Windows-based password aging feature, see [Enabling Password Aging for Users in Windows Databases, page 6-26](#).

## User-Changeable Passwords

With Cisco Secure ACS, you can install a separate program that enables users to 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*.

## Other Authentication-Related Features

In addition to the authentication-related features discussed in this section, the following features are provided by Cisco Secure ACS:

- Authentication of unknown users with external user databases (see [About Unknown User Authentication, page 15-4](#)).
- Authentication of computers running Microsoft Windows (see [Machine Authentication, page 13-15](#)).
- Support for the Microsoft Windows Callback feature (see [Setting User Callback Option, page 7-8](#)).
- Ability to configure user accounts, including passwords, using an external data source (see [About RDBMS Synchronization, page 9-26](#)).
- Ability for external users to authenticate via an enable password (see [Setting TACACS+ Enable Password Options for a User, page 7-35](#)).
- Proxy of authentication requests to other AAA servers (see [Proxy in Distributed Systems, page 4-4](#)).
- Configurable character string stripping from proxied authentication requests (see [Stripping, page 4-6](#)).
- Self-signed server certificates (see [Using Self-Signed Certificates, page 10-47](#)).
- Certificate revocation list checking during EAP-TLS authentication (see [Managing Certificate Revocation Lists, page 10-40](#)).

## Authorization

Authorization determines what a user is allowed to do. Cisco Secure ACS can send user profile policies to a AAA client to determine the 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.

The Cisco Secure ACS access restrictions feature enables you 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 can be disabled on specified dates. This would make it possible for a service provider to offer a 30-day free trial. The same authorization could be used to create a temporary account for a consultant with login permission 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, AppleTalk Remote Access (ARA), Serial Line Internet Protocol (SLIP), or EXEC. After a service is selected, 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 being offered by service providers and adopted by corporations is a service authorization for Virtual Private Dial-Up Networks (VPDNs). Cisco Secure 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, Cisco Secure ACS can be used for each end of the VPDN.

This section contains the following topics:

- [MaxSessions Issues, page A-16](#)
- [Dynamic Usage Quotas, page 1-18](#)
- [Shared Profile Components, page 1-19](#)
- [Support for Cisco Device-Management Applications, page 1-19](#)
- [Other Authorization-Related Features, page 1-20](#)

## Max Sessions

Max Sessions is a useful feature for organizations that need to limit the number of concurrent sessions available to either 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, Cisco Secure ACS enables the administrator 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 5 sessions each. This way no single member of a group account would be able to use more than 5 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 6-12, and [Setting Max Sessions Options for a User](#), page 7-15.

## Dynamic Usage Quotas

Cisco Secure ACS enables you 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 either 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 allocated to the user.

For more information about usage quotas, see [Setting Usage Quotas for a User Group](#), page 6-14, and [Setting User Usage Quotas Options](#), page 7-17.

## Shared Profile Components

Cisco Secure 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 HTML interface, and then configure each group to use the network access restriction set you created.

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

## Support for Cisco Device-Management Applications

Cisco Secure 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. Support for command authorization for management application users is accomplished by using unique command authorization set types for each management application configured to use Cisco Secure ACS for authorization.

Cisco Secure ACS uses TACACS+ to communicate with management applications. For a management application to communicate with Cisco Secure ACS, the management application must be configured in Cisco Secure 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 Cisco Secure ACS, these requirements ensure the validity of the communication. For information about configuring a AAA client, see [AAA Client Configuration](#), page 4-11. For information about administrator accounts, see [Administrator Accounts](#), page 12-1.

Additionally, the administrator used by the management application must have the Create New Device Command Set Type privilege enabled. When a management application initially communicates with Cisco Secure ACS, it dictates to Cisco Secure ACS the creation of a device command set type, which appears in the Shared Profile Components section of the HTML interface. It also dictates a custom service to be authorized by TACACS+. The custom service appears on the

TACACS+ (Cisco IOS) page in the Interface Configuration section of the HTML 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 5-25](#).

After the management application has dictated the custom TACACS+ service and device command-authorization set type to Cisco Secure ACS, you can configure command-authorization sets for each role supported by the management application and apply those sets to user groups that contain network administrators or to individual users who are network administrators. For information about configuring a command-authorization set, see [Adding a Command Authorization Set, page 5-31](#). For information about applying a shared device command-authorization set to a user group, see [Configuring Device-Management Command Authorization for a User Group, page 6-37](#). For information about applying a shared device command-authorization set to a user, see [Configuring Device-Management Command Authorization for a User, page 7-30](#).

## Other Authorization-Related Features

In addition to the authorization-related features discussed in this section, the following features are provided by Cisco Secure ACS:

- Group administration of users, with support for 500 groups (see [Chapter 6, “User Group Management”](#)).
- Ability to map a user from an external user database to a specific Cisco Secure ACS group (see [Chapter 16, “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 7-19](#)).
- Ability to disable an account on a specific date (see [Setting Options for User Account Disablement, page 7-19](#)).
- Ability to disable groups of users (see [Group Disablement, page 6-4](#)).
- 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 6-8](#)).
- Downloadable ACLs for users or groups, enabling centralized, modular ACL management (see [Downloadable IP ACLs, page 5-7](#)).
- Network access filters, enabling you to apply different downloadable ACLs and NARs based upon a user's point of entry into your network (see [Network Access Filters, page 5-2](#)).
- IP pools for IP address assignment of end-user client hosts (see [Setting IP Address Assignment Method for a User Group, page 6-28](#)).
- Per-user and per-group TACACS+ or RADIUS attributes (see [Advanced Options, page 3-4](#)).
- Support for Voice-over-IP (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 provided by the RADIUS and TACACS+ protocols to communicate relevant data for each user session to the AAA server for recording. Cisco Secure ACS writes accounting records to comma-separated value (CSV) log files. 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. For example, `aaa-reports!` by Extraxi supports Cisco Secure ACS (<http://www.extraxi.com>).

Among the types of accounting logs you can generate are the following:

- **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.
- **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.
- **Administrative Accounting**—Lists commands entered on a network device with TACACS+ command authorization enabled.

For more information about Cisco Secure ACS logging capabilities, see [Chapter 1, “Overview”](#).

## Other Accounting-Related Features

In addition to the accounting-related features discussed in this section, the following features are provided by Cisco Secure ACS:

- Centralized logging, allowing several Cisco Secure ACS Solution Engines to forward their accounting data to a remote agent (see [Remote Logging, page 11-17](#)).
- Configurable supplementary user ID fields for capturing additional information in logs (see [User Data Configuration Options, page 3-3](#)).
- Configurable logs, allowing you to capture as much information as needed (see [Accounting Logs, page 11-6](#)).

## Administration

To configure, maintain, and protect its AAA functionality, Cisco Secure ACS provides a flexible administration scheme. You can perform nearly all administration of Cisco Secure ACS through its HTML interface. For more information about the HTML interface, including steps for accessing the HTML interface, see [Cisco Secure ACS HTML Interface, page 1-28](#).

This section contains the following topics:

- [HTTP Port Allocation for Administrative Sessions, page 1-22](#)
- [Network Device Groups, page 1-23](#)
- [Cisco Security Agent Integration, page 1-24](#)
- [Other Administration-Related Features, page 1-27](#)

## HTTP Port Allocation for Administrative Sessions

The HTTP port allocation feature allows you to configure the range of TCP ports used by Cisco Secure ACS for administrative HTTP sessions. Narrowing this range with the HTTP port allocation feature reduces the risk of unauthorized access to your network by a port open for administrative sessions.

We do not recommend that you administer Cisco Secure 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 Cisco Secure ACS uses. While narrowing this range reduces the risk of unauthorized access, a greater risk of attack remains if you allow administration of Cisco Secure ACS from outside a firewall. A firewall configured to permit HTTP traffic over the Cisco Secure ACS administrative port range must also permit HTTP traffic through port 2002, because this is the port a web browser must address 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. Cisco Secure ACS tracks the IP address 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 12-11](#).

## Network Device Groups

With a network device group (NDG), you can view and administer a collection of AAA clients and AAA servers as a single logical group. To simplify administration, you can assign each group a convenient name that can be used to refer to all devices within that group. This creates two levels of network devices within Cisco Secure ACS—discrete devices such as an individual router, access server, AAA server, or PIX Firewall, and NDGs, which are named collections of AAA clients and AAA servers.

A network device can belong to only one NDG at a time.

Using NDGs enables an organization with a large number of AAA clients spread across a large geographical area to logically organize its environment within Cisco Secure ACS to reflect the physical setup. For example, all routers in Europe could belong to a group named Europe; all routers in the United States could belong to a US group; and so on. This would be especially convenient if the AAA clients in each region were administered along the same divisions. Alternatively, the environment could be organized by some other attribute such as divisions, departments, business functions, and so on.

You can assign a group of users to an NDG. For more information on NDGs, see [Network Device Group Configuration, page 4-36](#).

## Cisco Security Agent Integration

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



### Note

---

The first appliance base image to incorporate CSA is 3.3.1.3. You can determine the base image of an appliance with the **show** console command or the Appliance Upgrade Status page in the System Configuration section.

---

This section contains the following topics:

- [CSA Service Management, page 1-24](#)
- [CSA Logging, page 1-25](#)
- [CSA Restrictions, page 1-25](#)
- [CSA Policies, page 1-25](#)

## 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 *Installation and Configuration Guide for Cisco Secure ACS Solution Engine*.

From the HTML interface, you can use the Appliance Configuration page in the System Configuration section to enable or disable CSAgent. For more information, see [Appliance Configuration, page 8-22](#).

## CSA Logging

CSA writes two logs to the appliance hard drive, CSALog and CSASecurityLog. Each log is limited to 1 MB. When a CSA log exceeds 1 MB, CSA begins a new log file. Cisco Secure 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 about using the console, see *Installation and Configuration Guide for Cisco Secure ACS Solution Engine*.

From the HTML interface, you can view the CSA logs using the links found on the View Diagnostic Logs page in the System Configuration section. For more information, see [Viewing or Downloading Diagnostic Logs, page 8-28](#).

## CSA Restrictions

The following restrictions are imposed by the protection that CSA provides the appliance when CSAgent is enabled:

- **Upgrade and Patch Restriction**—You cannot apply upgrades or patches using the Appliance Upgrade Status page in the System Configuration section or using the **upgrade** command at the appliance console. To upgrade Cisco Secure ACS or apply patches, you must first disable CSAgent.
- **ping Restriction**—CSA does not allow Cisco Secure 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 Cisco Secure ACS Solution Engine to respond to ping requests, be aware that no CSA protection is in place for as long as CSAgent is disabled.

For information about disabling CSAgent, see [CSA Service Management, page 1-24](#).

## CSA Policies

CSA on Cisco Secure ACS Solution Engine is configured with the following policies:

- **Application Control**—CSA permits execution of only those applications required for Cisco Secure 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 Cisco Secure ACS to operate correctly.
- **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 covert channels.
  - Blocks dangerous ICMP messages, including ping.
  - Prevents IP source routing.
  - Prevents trace routing.
- **Email Worm Protection**—CSA guards the appliance against email worms.
- **Registry Access Control**—CSA permits Registry access to only those applications requiring it 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.
  - Applications cannot download and execute ActiveX controls.
  - Applications cannot automatically execute downloaded programs.
  - Applications cannot directly access operating system password information.
  - Applications cannot write into memory owned by other processes.
  - Applications cannot monitor keystrokes while accessing the network.

## Other Administration-Related Features

In addition to the administration-related features discussed in this section, the following features are provided by Cisco Secure ACS:

- Ability to define different privileges per administrator (see [Administrator Accounts, page 12-1](#)).
- Ability to log administrator activities (see [Cisco Secure ACS System Logs, page 11-12](#)).
- Ability to view a list of logged-in users (see [Dynamic Administration Reports, page 11-7](#)).
- CSMonitor service, providing monitoring, notification, logging, and limited automated failure response (see [Cisco Secure ACS Active Service Management, page 8-17](#)).
- Ability to automate configuration of users, groups, network devices, and custom RADIUS VSAs (see [RDBMS Synchronization, page 9-25](#)).
- Replication of CiscoSecure user database components to other Cisco Secure ACSes (see [CiscoSecure Database Replication, page 9-1](#)).
- Scheduled and on-demand Cisco Secure ACS system backups (see [Cisco Secure ACS Backup, page 8-8](#)).
- Ability to restore Cisco Secure ACS configuration, user accounts, and group profiles from a backup file (see [Cisco Secure ACS System Restore, page 8-13](#)).

## Posture Validation

Cisco Secure ACS supports Network Admission Control (NAC) by providing posture validation services to NAC-compliant AAA clients and the NAC-client computers seeking network access using those AAA clients. NAC provides a powerful means to defend your network. The data with which you can configure Cisco Secure ACS to evaluate posture validation requests can include operating system patch level and anti-virus DAT file versions and dates.

Instead of establishing identity, posture validation determines the state of the NAC-client computer using data sent to Cisco Secure ACS by the NAC client. Cisco Secure ACS uses the result of evaluating the state of the computer to determine whether network access is to be granted from the computer and to determine the degree of that access.

For more information, see [Chapter 14, “Network Admission Control”](#).

## Cisco Secure ACS HTML Interface

This section discusses the Cisco Secure ACS HTML interface and provides procedures for using it.

This section contains the following topics:

- [About the Cisco Secure ACS HTML Interface, page 1-28](#)
- [HTML Interface Layout, page 1-29](#)
- [Uniform Resource Locator for the HTML Interface, page 1-32](#)
- [Network Environments and Administrative Sessions, page 1-32](#)
- [Accessing the HTML Interface, page 1-34](#)
- [Logging Off the HTML Interface, page 1-35](#)
- [Online Help and Online Documentation, page 1-36](#)

### About the Cisco Secure ACS HTML Interface

After installing Cisco Secure ACS, you configure and administer it through the HTML interface. The HTML interface enables you to easily modify Cisco Secure ACS configuration from any connection on your LAN or WAN.

The Cisco Secure ACS HTML interface is designed to be viewed using a web browser. The design primarily uses HTML, along with some Java functions, to enhance ease of use. This design keeps the interface responsive and straightforward. The inclusion of Java requires that the browser used for administrative sessions supports Java. For a list of supported browsers, see the Release Notes. The most recent revision to the Release Notes is posted on Cisco.com (<http://www.cisco.com>).

The HTML interface not only makes viewing and editing user and group information possible, it also enables you to restart services, add remote administrators, change AAA client information, back up the system, view reports from anywhere on the network, and more. The reports track connection activity, show which users are logged in, list failed authentication and authorization attempts, and show administrators' recent tasks.

## HTML Interface Security

Accessing the HTML 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 time out after a configurable length of idle time. Regardless, we recommend that you log out of the HTML interface after each session. For information about logging out of Cisco Secure ACS, see [Logging Off the HTML Interface, page 1-35](#). For information about configuring the idle timeout feature, see [Access Policy, page 12-11](#).

You can enable secure socket layer (SSL) for administrative sessions. This ensures that all communication between the web browser and Cisco Secure 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 SSL for HTML interface security, see [Access Policy, page 12-11](#).

## HTML Interface Layout

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

- **Navigation Bar**—The gray frame on the left of the browser window, the navigation bar contains the task buttons. Each button changes the configuration area (see below) to a unique section of the Cisco Secure 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 HTML 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 be configured. For more information about the Interface Configuration section, [Chapter 3, “Interface Configuration”](#).
- **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 15, “Unknown User Policy”](#). For information about user group mapping, see [Chapter 16, “User Group Mapping and Specification”](#).

- **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 1-36](#).
- **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, changes are not saved.

---

- **Display Area**—The frame on the right of the browser window, the display area shows one of the following options:
  - **Online Help**—Displays basic help about the page currently shown 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 1-36](#).
  - **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 is displayed in this section. The usernames are hyperlinks to the specific user configuration, so clicking the name enables you 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 you entered in the Password box does not match the information in the Confirm Password box in the User Setup section, Cisco Secure ACS displays an error message here. The incorrect information remains in the configuration area so that you can retype and resubmit the information correctly.

## Uniform Resource Locator for the HTML Interface

The HTML interface is available by web browser at one of the following uniform resource locators (URLs):

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

where *IP address* is the dotted decimal IP address of the Cisco Secure ACS Solution Engine and *hostname* is the hostname of the Cisco Secure ACS Solution Engine. 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 running the browser.

If Cisco Secure ACS is configured to use SSL to protect administrative sessions, you can also access the HTML interface by specifying the HTTPS protocol in the URLs:

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

If SSL is enabled and you do not specify HTTPS, Cisco Secure 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 12-11](#).

## Network Environments and Administrative Sessions

We recommend that administrative sessions take place without the use of an HTTP proxy server, without a firewall between the browser and Cisco Secure ACS, and without a NAT gateway between the browser and Cisco Secure ACS. Because these limitations are not always practical, this section discusses how various network environmental issues affect administrative sessions.

This section contains the following topics:

- [Administrative Sessions and HTTP Proxy, page 1-33](#)
- [Administrative Sessions through Firewalls, page 1-33](#)
- [Administrative Sessions through a NAT Gateway, page 1-34](#)

## Administrative Sessions and HTTP Proxy

Cisco Secure ACS does not support HTTP proxy for administrative sessions. If the browser used for an administrative session is configured to use a proxy server, Cisco Secure ACS sees the administrative session originating from the IP address of the proxy server rather than from the actual address of the computer. Administrative session tracking assumes each browser resides on a computer with a unique IP.

Also, IP filtering of proxied administrative sessions has to be based on the IP address of the proxy server rather than the IP address of the computer. This conflicts with administrative session communication that does use the actual IP address of the computer. For more information about IP filtering of administrative sessions, see [Access Policy, page 12-11](#).

For these reasons, we do not recommend performing administrative sessions using a web browser that is configured to use a proxy server. Administrative sessions using a proxy-enabled web browser is not tested. If your web browser is configured to use a proxy server, disable HTTP proxying when attempting Cisco Secure ACS administrative sessions.

## Administrative Sessions through Firewalls

In the case of firewalls that do not perform network address translation (NAT), administrative sessions conducted across the firewall can require additional configuration of Cisco Secure ACS and the firewall. This is because Cisco Secure ACS assigns a random HTTP port at the beginning of an administrative session.

To allow administrative sessions from browsers outside a firewall that protects Cisco Secure ACS, the firewall must permit HTTP traffic across the range of ports that Cisco Secure ACS is configured to use. You can control the HTTP port range using the HTTP port allocation feature. For more information about the HTTP port allocation feature, see [HTTP Port Allocation for Administrative Sessions, page 1-22](#).

While administering Cisco Secure ACS through a firewall that is not performing NAT is possible, we do not recommend that you administer Cisco Secure ACS through a firewall. For more information, see [HTTP Port Allocation for Administrative Sessions, page 1-22](#).

## Administrative Sessions through a NAT Gateway

We do not recommend conducting administrative sessions across a network device performing NAT. If the administrator runs a browser on a computer behind a NAT gateway, Cisco Secure ACS receives the HTTP requests from the public IP address of the NAT device, which conflicts with the computer private IP address, included in the content of the HTTP requests. Cisco Secure ACS does not permit this.

If Cisco Secure ACS is behind a NAT gateway and the URL used to access the HTML interface specifies Cisco Secure ACS by its hostname, administrative sessions operate correctly, provided that DNS is functioning correctly on your network or that computers used to access the HTML interface have a hosts file entry for Cisco Secure ACS.

If the URL used to access the HTML interface specifies Cisco Secure ACS by its IP address, you could configure the gateway to forward all connections to port 2002 to Cisco Secure ACS, using the same port. Additionally, all the ports allowed using the HTTP port allocation feature would have to be similarly mapped. We have not tested such a configuration and do not recommend implementing it.

## Accessing the HTML Interface

Administrative sessions always require that you login using a valid administrator name and password.

### Before You Begin

Determine whether a supported web browser is installed on the computer you want to use to access the HTML interface. If not, install a supported web browser or use a computer that already has a supported web browser installed. For a list of supported browsers, see the Release Notes. The latest revision to the Release Notes is posted on Cisco.com (<http://www.cisco.com>).

Because the HTML interface uses Java in a few places, the computer running the browser used to access the HTML interface must have a Java Virtual Machine available for the use of the browser.

To access the HTML interface, follow these steps:

- 
- Step 1** Open a web browser. For a list of supported web browsers, see the Release Notes for the version of Cisco Secure ACS you are accessing. The latest revision to the Release Notes is posted on Cisco.com (<http://www.cisco.com>).
- Step 2** In the Address or Location bar in the web browser, type the applicable URL. For a list of possible URLs, see [Uniform Resource Locator for the HTML Interface, page 1-32](#).
- Step 3** In the **Username** box, type a valid Cisco Secure ACS administrator name.
- Step 4** In the **Password** box, type the password for the administrator name you specified.
- Step 5** Click **Login**.
- The initial page appears.
- 

## Logging Off the HTML Interface

When you are finished using the HTML interface, we recommend that you log off. While Cisco Secure ACS can timeout unused administrative sessions, logging off prevents unauthorized access by someone using the browser after you or by unauthorized persons using the HTTP port left open to support the administrative session.

To log off the Cisco Secure ACS HTML interface, click the **Logoff** button.



### Note

---

The Logoff button appears in the upper right corner of the browser window, except on the initial page, where it appears in the upper left of the configuration area.

---

## Online Help and Online Documentation

We provide two sources of information in the HTML 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. At the top of each online help page is a list of topics covered by that page.

To jump from the top of the online help page to a particular topic, click the topic name in the list at the top of the page.

There are three icons that appear on many pages in Cisco Secure ACS:

- **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.
- **Section Information**—Many online help pages contain a Section Information icon at the bottom of the page. To view an applicable section of the online documentation, click the Section Information icon.
- **Back to Help**—Wherever you find a 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 Documentation

Online documentation is the user guide for Cisco Secure ACS. The user guide provides information about the configuration, operation, and concepts of Cisco Secure ACS. The information presented in the online documentation is as current as the release date of the Cisco Secure ACS version you are using. For the most up-to-date documentation about Cisco Secure ACS, please go to <http://www.cisco.com>.

**Tip**

---

Click **Section Information** on any online help page to view online documentation relevant to the section of the HTML interface you are using.

---

To access online documentation, follow these steps:

---

**Step 1** In the Cisco Secure ACS HTML interface, click **Online Documentation**.

**Tip**

---

To open the online documentation in a new browser window, right-click **Online Documentation**, and then click **Open Link in New Window** (for Microsoft Internet Explorer) or **Open in New Window** (for Netscape Navigator).

---

The table of contents opens in the configuration area.

**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, follow these steps:

a. Click [**Index**].

The index appears in the display area.

b. Scroll through the index to find an entry for the topic you are researching.

**Tip**

---

Use the lettered shortcut links to jump to a particular section of the index.

---

Entries appear with numbered links after them. The numbered links lead to separate instances of the entry topic.

c. Click an instance number for the desired topic.

The online documentation for the topic selected appears in the display area.

**Step 4** If you want to print the online documentation, click in the display area, and then click **Print** in the navigation bar of your browser.

---

