Installation and Setup Guide for Cisco Secure ACS Appliance

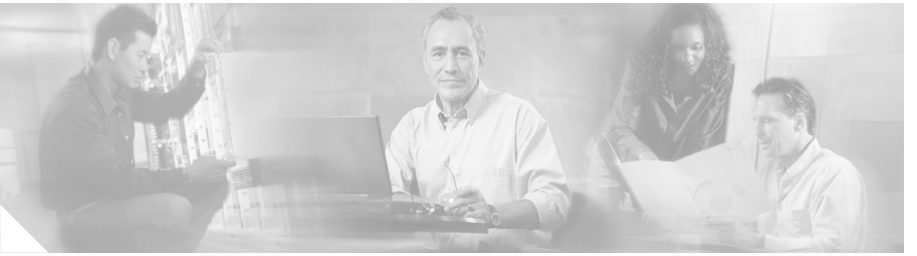
Version 3.2

License, Warranty, and Installation Instructions

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number: DOC-7814573=
Text Part Number: 78-14573-02

Installation and Setup Guide for Cisco Secure ACS Appliance



Cisco 90-Day Limited Hardware Warranty Terms

There are special terms applicable to your hardware warranty and various services that you can use during the warranty period. Your formal Warranty Statement, including the warranties and license agreements applicable to Cisco software, is available on Cisco.com. Follow these steps to access and download the *Cisco Information Packet* and your warranty and license agreements from Cisco.com.

1. Launch your browser, and go to this URL:

   http://www.cisco.com/univercd/cc/td/doc/es_inpck/cetrans.htm

   The Warranties and License Agreements page appears.

2. To read the *Cisco Information Packet*, follow these steps:

   a. Click the **Information Packet Number** field, and make sure that the part number 78-5235-03A0 is highlighted.

   b. Select the language in which you would like to read the document.

   c. Click **Go**.

      The Cisco Limited Warranty and Software License page from the Information Packet appears.

   d. Read the document online, or click the **PDF** icon to download and print the document in Adobe Portable Document Format (PDF).

Note You must have Adobe Acrobat Reader to view and print PDF files. You can download the reader from Adobe's website: http://www.adobe.com

3. To read translated and localized warranty information about your product, follow these steps:
   a. Enter this part number in the Warranty Document Number field:

      78-5236-01C0

   b. Select the language in which you would like to read the document.
   c. Click **Go**.

      The Cisco warranty page appears.

   d. Review the document online, or click the **PDF** icon to download and print the document in Adobe Portable Document Format (PDF).

You can also contact the Cisco service and support website for assistance:

http://www.cisco.com/public/Support_root.shtml.

Duration of Hardware Warranty

Ninety (90) days.

Replacement, Repair, or Refund Policy for Hardware

Cisco or its service center will use commercially reasonable efforts to ship a replacement part within ten (10) working days after receipt of a Return Materials Authorization (RMA) request. Actual delivery times can vary, depending on the customer location.

Cisco reserves the right to refund the purchase price as its exclusive warranty remedy.

To Receive a Return Materials Authorization (RMA) Number

Contact the company from whom you purchased the product. If you purchased the product directly from Cisco, contact your Cisco Sales and Service Representative.

Complete the information below, and keep it for reference:

Company product purchased from	
Company telephone number	
Product model number	
Product serial number	
Maintenance contract number	

Preface

This guide describes how to install and initially configure the Cisco Secure ACS Appliance version 3.2. It also details administrative functions that can be performed from the command line interface.

Audience

This guide is intended primarily for system administrators who install and configure internetworking equipment and who are familiar with Cisco IOS software.

Warning **Only trained and qualified personnel should install, replace, or service this equipment.**

Organization

This guide consists of the following chapters and appendixes:

- Preface
- Chapter 1, “Cisco Secure ACS Appliance Overview”
- Chapter 2, “Preparing for Installation”
- Chapter 3, “Installing and Configuring the Cisco Secure ACS Appliance”
- Chapter 4, “Administering the Cisco Secure ACS Appliance”

- Appendix A, “Technical Specifications”
- Appendix B, “Windows Service Advisement”
- Appendix C, “Command Reference”

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** `font`
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Selecting a menu item	**Option > Network Preferences**

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning Definition

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the translated safety warnings that accompanied this device.

Note: SAVE THESE INSTRUCTIONS

Note: This documentation is to be used in conjunction with the specific product installation guide that shipped with the product. Please refer to the Installation Guide, Configuration Guide, or other enclosed additional documentation for further details.

Waarschuwing **BELANGRIJKE VEILIGHEIDSINSTRUCTIES**

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Voor een vertaling van de waarschuwingen die in deze publicatie verschijnen, dient u de vertaalde veiligheidswaarschuwingen te raadplegen die bij dit apparaat worden geleverd.

Opmerking BEWAAR DEZE INSTRUCTIES.

Opmerking Deze documentatie dient gebruikt te worden in combinatie met de installatiehandleiding voor het specifieke product die bij het product wordt geleverd. Raadpleeg de installatiehandleiding, configuratiehandleiding of andere verdere ingesloten documentatie voor meer informatie.

Varoitus **TÄRKEITÄ TURVALLISUUTEEN LIITTYVIÄ OHJEITA**

Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. Tässä asiakirjassa esitettyjen varoitusten käännökset löydät laitteen mukana toimitetuista ohjeista.

Huomautus SÄILYTÄ NÄMÄ OHJEET

Huomautus Tämä asiakirja on tarkoitettu käytettäväksi yhdessä tuotteen mukana tulleen asennusoppaan kanssa. Katso lisätietoja asennusoppaasta, kokoonpano-oppaasta ja muista mukana toimitetuista asiakirjoista.

Attention **IMPORTANTES INFORMATIONS DE SÉCURITÉ**

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant causer des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions d'avertissements figurant dans cette publication, consultez les consignes de sécurité traduites qui accompagnent cet appareil.

Remarque CONSERVEZ CES INFORMATIONS

Remarque Cette documentation doit être utilisée avec le guide spécifique d'installation du produit qui accompagne ce dernier. Veuillez vous reporter au Guide d'installation, au Guide de configuration, ou à toute autre documentation jointe pour de plus amples renseignements.

Warnung **WICHTIGE SICHERHEITSANWEISUNGEN**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewusst. Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise sind im Lieferumfang des Geräts enthalten.

Hinweis BEWAHREN SIE DIESE SICHERHEITSANWEISUNGEN AUF

Hinweis Dieses Handbuch ist zum Gebrauch in Verbindung mit dem Installationshandbuch für Ihr Gerät bestimmt, das dem Gerät beiliegt. Entnehmen Sie bitte alle weiteren Informationen dem Handbuch (Installations- oder Konfigurationshandbuch o. Ä.) für Ihr spezifisches Gerät.

Figyelem! **FONTOS BIZTONSÁGI ELÕÍRÁSOK**

Ez a figyelmezetõ jel veszélyre utal. Sérülésveszélyt rejtõ helyzetben van. Mielõtt bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplõ figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található.

Megjegyzés ÕRIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Megjegyzés Ezt a dokumentációt a készülékhez mellékelt üzembe helyezési útmutatóval együtt kell használni. További tudnivalók a mellékelt Üzembe helyezési útmutatóban (Installation Guide), Konfigurációs útmutatóban (Configuration Guide) vagy más dokumentumban találhatók.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Per le traduzioni delle avvertenze riportate in questo documento, vedere le avvertenze di sicurezza che accompagnano questo dispositivo.

Nota CONSERVARE QUESTE ISTRUZIONI

Nota La presente documentazione va usata congiuntamente alla guida di installazione specifica spedita con il prodotto. Per maggiori informazioni, consultare la Guida all'installazione, la Guida alla configurazione o altra documentazione acclusa.

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette varselssymbolet betyr fare. Du befinner deg i en situasjon som kan forårsake personskade. Før du utfører arbeid med utstyret, bør du være oppmerksom på farene som er forbundet med elektriske kretssystemer, og du bør være kjent med vanlig praksis for å unngå ulykker. For å se oversettelser av advarslene i denne publikasjonen, se de oversatte sikkerhetsvarslene som følger med denne enheten.

Merk TA VARE PÅ DISSE INSTRUKSJONENE

Merk Denne dokumentasjonen skal brukes i forbindelse med den spesifikke installasjonsveiledningen som fulgte med produktet. Vennligst se installasjonsveiledningen, konfigureringsveiledningen eller annen vedlagt tilleggsdokumentasjon for detaljer.

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. O utilizador encontra-se numa situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha em atenção os perigos envolvidos no manuseamento de circuitos eléctricos e familiarize-se com as práticas habituais de prevenção de acidentes. Para ver traduções dos avisos incluídos nesta publicação, consulte os avisos de segurança traduzidos que acompanham este dispositivo.

Nota GUARDE ESTAS INSTRUÇÕES

Nota Esta documentação destina-se a ser utilizada em conjunto com o manual de instalação incluído com o produto específico. Consulte o manual de instalação, o manual de configuração ou outra documentação adicional inclusa, para obter mais informações.

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Vea las traducciones de las advertencias que acompañan a este dispositivo.

Nota GUARDE ESTAS INSTRUCCIONES

Nota Esta documentación está pensada para ser utilizada con la guía de instalación del producto que lo acompaña. Si necesita más detalles, consulte la Guía de instalación, la Guía de configuración o cualquier documentación adicional adjunta.

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Se översättningarna av de varningsmeddelanden som finns i denna publikation, och se de översatta säkerhetsvarningarna som medföljer denna anordning.

OBS! SPARA DESSA ANVISNINGAR

OBS! Denna dokumentation ska användas i samband med den specifika produktinstallationshandbok som medföljde produkten. Se installationshandboken, konfigurationshandboken eller annan bifogad ytterligare dokumentation för närmare detaljer.

Предупреждение ВАЖНЫЕ СВЕДЕНИЯ ПО БЕЗОПАСНОСТИ

Этот символ предупреждает о наличии опасности. При неправильных действиях возможно получение травм. Перед началом работы с любым оборудованием необходимо ознакомиться с ситуациями, в которых возможно поражение электротоком, и со стандартными действиями для предотвращения несчастных случаев. Переведенный текст предупреждений содержится в соответствующем документе, поставляемом вместе с устройством.

Примечание СОХРАНЯЙТЕ ЭТУ ИНСТРУКЦИЮ
Примечание Эта инструкция должна использоваться вместе с руководством по установке конкретного изделия, входящим в комплект поставки. Дополнительные сведения см. в руководстве по установке, руководстве по настройке и другой документации, поставляемой с изделием.

警告　有关安全的重要说明

这个警告符号指有危险。您所处的环境可能使身体受伤。操作设备前必须意识到电流的危险性，务必熟悉操作标准，以防发生事故。如果需要了解本说明中出现的警告符号的译文，请参阅本装置所附之安全警告译文。

注意　保存这些说明
注意　本文件应与本产品附带的具体安装说明一并阅读。如欲了解详情，请参阅《安装说明》、《配置说明》或所附的其他文件。

警告　安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。このマニュアルに記載されている警告の各国語版は、装置に付属の「Translated Safety Warnings」を参照してください。

注　これらの注意事項を保管しておいてください。
注　この資料は、製品に付属のインストレーション ガイドと併用してください。詳細は、インストレーション ガイド、コンフィギュレーション ガイド、または添付されているその他のマニュアルを参照してください。

Related Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

The following documentation is also available:

Paper Documentation

- *Release Notes for Cisco Secure ACS Appliance Version 3.1. (*While a printed copy of this document comes with the product, check http://www.cisco.com for the most recent version.)
- *Regulatory Compliance and Safety Information for the Cisco Secure ACS Appliance.*

Online Documentation

- Online Help—Contains information for each associated page in the Cisco Secure ACS Appliance HTML interface.
- Online Documentation—A complete copy of the following documents are located online:
  - *User Guide for Cisco Secure ACS Appliance*
- PDF documentation—The following documents can be found in PDF form on the CD-ROM included with the Cisco Secure ACS Appliance:
  - *Installation and Setup Guide for Cisco Secure ACS Appliance* .
  - *Regulatory Compliance and Safety Information for the Cisco Secure ACS Appliance.*
  - User Guide for Cisco Secure ACS Appliance
  - *Installation and Configuration Guide for Cisco Secure Remote Agents*
  - *Release Notes for Cisco Secure ACS Appliance Version 3.1. (*Check http://www.cisco.com for the latest version.)

Note Adobe Acrobat Reader 4.0, or later, is required to view PDF documents.

- You can find other product literature, including white papers, data sheets, and product bulletins, at: http://www.cisco.com/warp/public/cc/pd/sqsw/sq/prodlit/index.shtml.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

http://www.cisco.com/tac/caseopen

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/index.html

Cisco Secure ACS Appliance Overview

System Description

Cisco Secure ACS Appliance version 3.2 is a highly scalable, rack-mounted, dedicated platform that serves as a high performance access control server supporting centralized Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS+). The Cisco Secure ACS Appliance controls the authentication, authorization, and accounting (AAA) of users accessing corporate resources through the network.

The Cisco Secure ACS Appliance allows you to control who can access the network, to authorize what types of network services are available for particular users or groups of users, and to keep an accounting record of all user actions in the network. The appliance supports access control and accounting for dial-up access servers, firewalls and VPNs, Voice-over-IP solutions, content networking, and switched and wireless local area networks (LANs and WLANs). In addition, the same AAA framework can be used, via TACACS+, to manage administrative roles and groups and to control how network administrators can change, access, and configure the network internally.

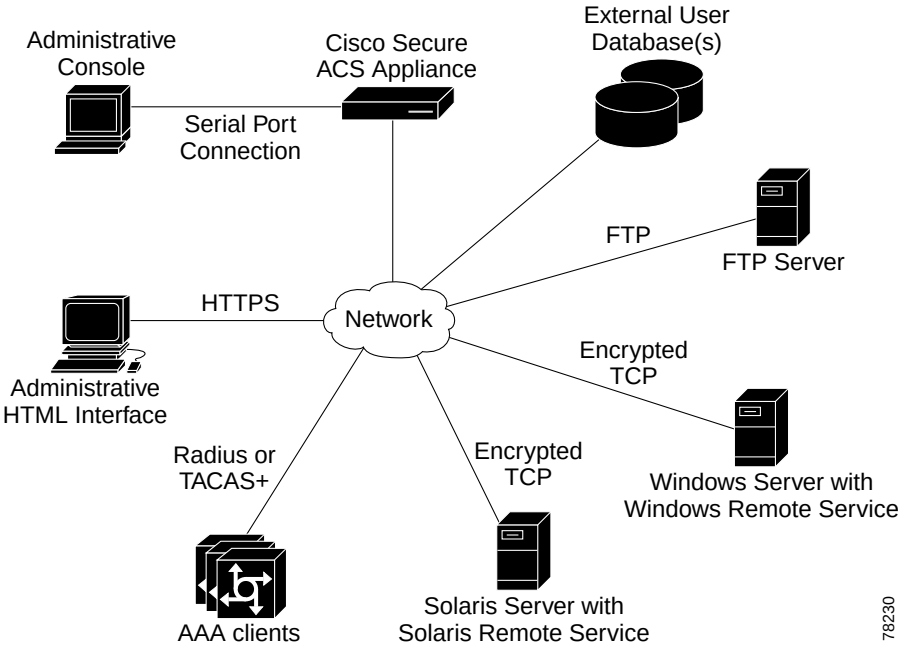
The Cisco Secure ACS Appliance provides, as nearly as possible, the exact same features and functions of the Cisco Secure ACS for Windows Server (the software product) in a dedicated, security hardened, application-specific, appliance packaging. The appliance includes additional features specific to operating and managing the Cisco Secure ACS Appliance.

To ensure a highly secure posture, Cisco Secure ACS Appliance:

- Runs only the necessary services of the underlying hardened Windows operating system. (See Appendix B, "Windows Service Advisement," for details on the hardening.)
- Does not support a keyboard or monitor.
- Does not provide access to its file system.
- Does not allow running arbitrary applications on it.
- Allows TCP/IP connections only via the ports necessary to its own operations.

Figure 1-1 shows the Cisco Secure ACS Appliance operating context.

Figure 1-1 Cisco Secure ACS Appliance Context Diagram



The administrative console shown in the context diagram represents any data terminal equipment (DTE) capable of supporting administrative connection via a serial port connection and is generally referred to as a console in this guide.

For more detailed information on Cisco Secure ACS Appliance features and capabilities, see the *User Guide for Cisco Secure ACS Appliance* and the *Release Notes for Cisco Secure ACS Appliance Version 3.2*.

Cisco Secure ACS Appliance Hardware Description

The Cisco Secure ACS Appliance is a rack-mountable 1U box with the following configuration:

- Intel 3.06 GHz Pentium 4 processor with a 512-KB level 2 ECC cache
- Two built-in NC7760 PCI gigabit server adapters
- 40-GB ATA hard drive
- Floppy drive
- CD-ROM drive
- Serial port

The parallel port, video, keyboard, and mouse controllers are not used.

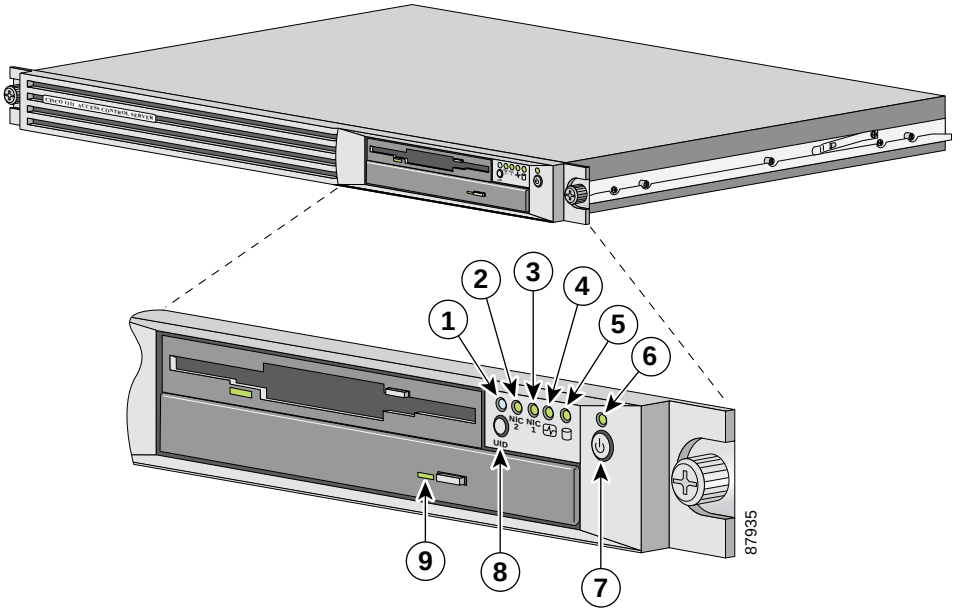
Technical specifications are detailed in Appendix A, "Technical Specifications."

This section contains the following sections and subsections:

Front Panel Features

The Cisco Secure ACS Appliance front panel contains switches, indicators, and the CD-ROM drive. Figure 1-2 shows the front panel switches and LED indicators. The functions of the switches and LED indicators are described in below the illustration.

Figure 1-2 Front Panel Switches and Indicators



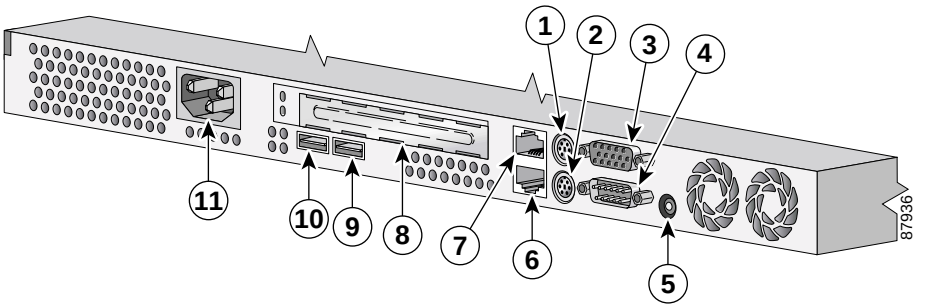
No.	Switch or LED Indicator	Description
1	Front unit identification LED	Glows blue when unit ID switch has been pressed.
2	NIC 2 link/activity LED	On = Link Off = No Link Blinking = Activity
3	NIC 1 link/activity LED	On = Link Off = No Link Blinking = Activity
4	System health LED	Green = Good Amber = Degraded Red = Critical Error
5	Hard drive activity LED	On = Activity Off = No Activity

No.	Switch or LED Indicator	Description
6	Power On/Off LED	Green = Power On Amber = Standby Mode Off = Power Off
7	Power On/Off	Toggles power on and off.
8	Front unit identification switch	Toggles to illuminate the blue unit ID LEDs on the front and back panels. (Used to mark a particular unit in a rack full of similar equipment.)
9	CD-ROM drive activity LED	On = Activity Off = No Activity

Back Panel Features

The back panel contains the AC power receptacle, Ethernet connectors, indicator LEDs, and a serial port. Figure 1-3 shows the back-panel features.

Figure 1-3 Back Panel Features



1	Mouse connector (not supported)	7	RJ-45 Fast Ethernet connector with 10/100/1000-Mbit/s operation for NIC 2
2	Keyboard connector (not supported)	8	64-bit expansion slot (not supported)
3	Serial connector (see Figure 1-4)	9	USB connector 1 (not supported)

4	Video connector (not supported)	**10**	USB connector 2 (not supported)
5	Back unit identification LED switch	**11**	AC power receptacle
6	RJ-45 Fast Ethernet connector with 10/100/1000-Mbit/s operation for NIC 1		

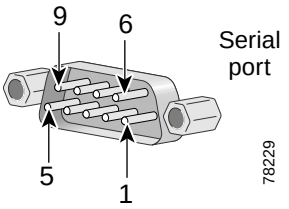
Serial Port

The integrated serial port on the back panel of the appliance uses a 9-pin D-subminiature connector.

Serial Port Connector

If you reconfigure your hardware, you may need information regarding the pin number and signal for the serial port connector. Figure 1-4 illustrates the pin numbers for the serial port connector and defines the pin assignments and interface signals for the serial port connector. (Pin numbering proceeds bottom to top and right to left, as illustrated.)

Figure 1-4 Pin Numbers for the Serial Port Connector



Pin	Signal	I/O	Definition
1	DCD	I	Data carrier detect
2	SIN	I	Serial input
3	SOUT	O	Serial output
4	DTR	O	Data terminal ready
5	GND	N/A	Signal ground
6	DSR	I	Data set ready
7	RTS	O	Request to send

Pin	Signal	I/O	Definition
8	CTS	I	Clear to send
9	RI	I	Ring indicator
Shell	N/A	N/A	Chassis ground

Ethernet Connectors

Your system has two integrated 10/100/1000–megabit-per-second (Mbps) Ethernet connectors. Cisco Secure ACS Appliance supports the operation of either Ethernet connector, but not both connectors. Each Ethernet connector provides all the functions of a network expansion card and supports the 10BASE-T, 100BASE-TX, and 1000BASE-TX Ethernet standards.

Each NIC is configured to automatically detect the speed and duplex mode of the network.

Note The Cisco Secure ACS Appliance supports the operation of only one Ethernet connector at a time. Concurrent operation of both Ethernet connectors is not supported.

Network Cable Requirements

Warning **To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.**

The Ethernet connectors are designed for attaching an unshielded twisted pair (UTP) Ethernet cable equipped with standard RJ-45 compatible plugs. Press one end of the UTP cable into the Ethernet connector until the plug snaps securely into place. Connect the other end of the cable to an RJ-45 port on a hub or other device, depending on your network configuration. Observe the following cabling restrictions for 10BASE-T, 100BASE-TX, and 1000BASE-TX networks:

- For 10BASE-T networks, use Category 3 or greater wiring and connectors.
- For 100BASE-TX and 1000BASE-TX networks, use Category 5 or greater wiring and connectors.
- The maximum cable run length is 328 feet (ft) or 100 meters (m).

Preparing for Installation

This chapter describes the safety instructions and site requirements for installing Cisco Secure ACS Appliance 3.2, and guides you through installation preparation. It contains the following sections:

Safety

This section provides safety information for installing this product.

Warnings and Cautions

Read the installation instructions in this document before you connect the system to its power source. Failure to read and follow these guidelines could lead to an unsuccessful installation and possibly damage the system and components.

You should observe the following safety guidelines when working with any equipment that connects to electrical power or telephone wiring. They can help you avoid injuring yourself or damaging the Cisco Secure ACS Appliance.

The following warnings and cautions are provided to help you prevent injury to yourself or damage to the devices:

Warning **IMPORTANT SAFETY INSTRUCTIONS**
This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translations of the warnings that appear in this publication, refer to the translated safety warnings that accompanied this device.

Note: SAVE THESE INSTRUCTIONS
Note: This documentation is to be used in conjunction with the specific product installation guide that shipped with the product. Please refer to the Installation Guide, Configuration Guide, or other enclosed additional documentation for further details.

Warning **The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.**

Warning **Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.**

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.**

Warning **Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages.**

Warning **Only trained and qualified personnel should install, replace, or service this equipment.**

Warning **This unit might have more than one power cord. To reduce the risk of electrical shock, disconnect all power supply cords before servicing the unit.**

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Make sure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. and 240 VAC, 10A international are used on the phase conductors (all current-carrying conductors).**

Warning **This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.**

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place**

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.**

Warning **Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals.**

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.**

Warning **Before working on a system that has an On/Off switch, turn OFF the power and unplug the power cord.**

Warning **Read the installation instructions before you connect the system to its power source.**

Warning **The ports labeled “10BaseT”, “100BaseTX,” and “1000BaseTX” are safety extra-low voltage (SELV) circuits. SELV circuits should only be connected to other SELV circuits. Avoid connecting these circuits to telephone network voltage (TNV) circuits.**

Warning **There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer’s instructions.**

General Precautions

Observe the following general precautions when using and working with your system:

- Keep your system components away from radiators and heat sources, and do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the computer gets wet, see the appropriate chapter in your troubleshooting guide or contact the Cisco Technical Assistance Center. For instructions on contacting the Technical Assistance Center, see Obtaining Technical Assistance, page xxiv, in the Preface.

- Do not push any objects into the openings of your system components. Doing so can cause fire or electric shock by shorting out interior components.
- Position system cables and power cables carefully; route system cables and the power cable and plug so that they cannot be stepped on or tripped over. Be sure that nothing rests on your system components' cables or power cable.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.
- To help avoid possible damage to the system board, wait 5 seconds after turning off the system before removing a component from the system board or disconnecting a peripheral device from the computer.

Maintaining Safety with Electricity

Follow these guidelines when working on equipment powered by electricity:

- If any of the following conditions occur contact the Cisco Technical Assistance Center:
  - The power cable or plug is damaged.
  - An object has fallen into the product.
  - The product has been exposed to water.
  - The product has been dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Use the correct external power source. Operate the product only from the type of power source indicated on the electrical ratings label. If you are not sure of the type of power source required, consult the Cisco Technical Assistance Center or a local power company.
- Use only approved power cable(s). You have been provided with a power cable for your Cisco Secure ACS Appliance that is intended for your system (approved for use in your country, based on the shipping location). Should you have to purchase a power cable, ensure that it is rated for the product and for the voltage and current marked on the product's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the product.

- To help prevent electric shock, plug the Cisco Secure ACS Appliance, components, and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable.
- To help protect your system and components from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptable power supply (UPS).
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local and national wiring rules.

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside your computer. To prevent static damage, discharge static electricity from your body before you touch any of your computer's electronic components, such as the microprocessor. You can do so by touching an unpainted metal surface on the computer chassis.

As you continue to work inside the computer, periodically touch an unpainted metal surface to remove any static charge your body may have accumulated.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

- When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your computer. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
- When transporting a sensitive component, first place it in an antistatic container or packaging.
- Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads and workbench pads.

Preventing EMI

When you run wires for any significant distance in an electromagnetic field, electromagnetic interference (EMI) can occur between the field and the signals on the wires.

Note that:

- Bad plant wiring can result in radio frequency interference (RFI).
- Strong EMI, especially when it is caused by lightning or radio transmitters, can destroy the signal drivers and receivers in the system, and can even create an electrical hazard by conducting power surges through lines and into the system.

To predict and remedy strong EMI, consult RFI experts.

Preparing Your Site for Installation

This section describes the requirements your site must meet for safe installation and operation of your Cisco Secure ACS Appliance. Ensure that your site is properly prepared before beginning installation.

Environmental

When planning your site layout and equipment locations, keep in mind the precautions described in this section to help avoid equipment failures and reduce the possibility of environmentally caused shutdowns. If you are experiencing shutdowns or unusually high errors with your existing equipment, these precautions will help you isolate the cause of failures and prevent future problems.

Use the following precautions when planning the operating environment for your Cisco Secure ACS Appliance.

- Always follow the ESD-prevention procedures described in Preventing EMI, page 27, to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.
- Make sure that the chassis cover is secure. The chassis allows cooling air to flow effectively within it. An open chassis allows air leaks, which could interrupt and redirect the flow of cooling air from internal components.
- Electrical equipment generates heat. Ambient air temperature might not be adequate to cool equipment to acceptable operating temperatures without adequate circulation. Make sure that the room in which you operate has adequate air circulation.

Choosing a Site for Installation

Warning **This unit is intended for installation in restricted access areas. A restricted access area is where access can only be gained by service personnel through the use of a special tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.**

- Choose a site with a dry, clean, well-ventilated and air-conditioned area.
- Choose a site that maintains an ambient temperature of 10° to 35°C (50° to 95°F).

Grounding the System

Warning **Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.**

Creating a Safe Environment

Follow these guidelines to create a safe operating environment:

- Keep tools and chassis components off the floor and away from foot traffic.
- Clear the area of possible hazards, such as moist floors, ungrounded power extension cables, and missing safety grounds.
- Keep the area around the chassis free from dust and foreign conductive material (such as metal flakes from nearby construction activity).

AC Power

Ensure that the plug-socket combination is accessible at all times, because it serves as the main disconnecting device. For the Cisco Secure ACS Appliance power requirements, see Appendix A, "Technical Specifications.".

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Make sure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. and 240 VAC, 10A international are used on the phase conductors (all current-carrying conductors).**

Cabling

Use the cables in the accessory kit to connect the Cisco Secure ACS Appliance console port to a console or computer that is running a console program. In addition to using the console cable, use the provided standard Ethernet cable to connect the Cisco Secure ACS Appliance to your network. For information detailing cable requirements, see Network Cable Requirements, page 1-7.

Precautions for Rack-Mounting

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

Observe the following precautions for rack stability and safety. Also refer to the rack installation documentation accompanying the rack for specific warning and caution statements and procedures.

Note Component refers to any server, storage system, or appliance, and to various peripherals or supporting hardware.

- Do not move large racks by yourself. Due to the height and weight of the rack, a minimum of two people are needed to accomplish this task.
- Ensure that the rack is level and stable before extending a component from the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80% of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.
- Do not step or stand on any system or component when servicing other systems and components in a rack.
- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.
- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Required Tools and Equipment

You need the following tools and equipment to install the Cisco Secure ACS Appliance:

- RJ-45 console cable (provided)
- Power cord (provided)
- Number 2 Phillips screwdriver
- Tape measure and level
- Antistatic mat or antistatic foam
- ESD grounding strap
- Ethernet cable
- Rack-mount kit (provided)
  - Two chassis-support rails
  - Cable support bracket (optional)
  - Cable tray clamp (optional)
- Eight screws sized to attach chassis-support rails to your particular rack (1/4-20 or M6 thread size suggested)

Installing and Configuring the Cisco Secure ACS Appliance

This chapter describes how to install and configure Cisco Secure ACS Appliance 3.2. It contains the following sections:

Quick Reference

Table 3-1 provides a high-level overview of the installation process.

Table 3-1 Quick Reference

Task	Steps	References
Install rack rails.	1. Adjust length of rack rails. 2. Attach rack rails to rack.	Installing the Cisco Secure ACS Appliance in a Rack, page 3-6
Attach the fixed cable tray to the back rail post.	Insert fixed cable tray post into rail slot.	Installing the Cisco Secure ACS Appliance in a Rack, page 3-6
Attach the cable support bracket to the chassis.	1. Remove access panel. 2. Hook cable support bracket to the chassis. 3. Fasten cable support bracket thumbnut to the chassis. 4. Replace access panel.	Accessing Internal Components, page 3-5 and Installing the Cisco Secure ACS Appliance in a Rack, page 3-6
Insert the Cisco Secure ACS Appliancechassis into the rack.	1. Slide chassis into rack. 2. Secure front panel thumbnuts. 3. Secure fixed cable tray to cable support bracket. 4. Fasten cable tray thumbnut to rail.	Installing the Cisco Secure ACS Appliance in a Rack, page 3-6
Route and connect cables.	1. Plug the network connection into the Ethernet NIC 1 port. 2. Connect a terminal to the console serial port.	Connecting Cables, page 3-11
Connect to a power source.	Connect to an AC power source.	Connecting to Power Source, page 3-13
Power on the Cisco Secure ACS Appliance	Press the power switch.	Powering On the Cisco Secure ACS Appliance, page 3-13

Table 3-1 Quick Reference (continued)

Task	Steps	References
Configure the Cisco Secure ACS Appliance	1. Boot the Cisco Secure ACS Appliance and log in from a serial console. 2. Configure the initial Cisco Secure ACS Appliance connectivity by responding to the prompts.	Configuring the Cisco Secure ACS Appliance, page 3-15
Verify the initial configuration.	1. Reboot the Cisco Secure ACS Appliance. 2. Log in from the system console. 3. Verify Cisco Secure ACS Appliance initial configuration.	Verifying the Initial Configuration, page 3-20
Perform full Cisco Secure ACS Appliance configuration.	The second phase of Cisco Secure ACS Appliance configuration is performed via the HTML interface and is beyond the scope of this guide.	Next Steps, page 3-21, and the *User Guide for Cisco Secure ACS Appliance*

Installing the Cisco Secure ACS Appliance

This section provides instructions for installing the Cisco Secure ACS Appliance in a rack. The rack must be properly secured to the floor, to the ceiling, or to an upper wall, and where applicable, to adjacent racks. The rack should be secured using floor and wall fasteners and bracing specified or approved by the rack manufacturer or by industry standards. Refer to the installation documentation from the rack manufacturer for precautionary warnings and information before you install the Cisco Secure ACS Appliance.

Before you install the Cisco Secure ACS Appliance in a rack, read Preparing Your Site for Installation, page 2-7, to familiarize yourself with proper site and environmental conditions. Failure to read and follow these guidelines could lead

to an unsuccessful installation and possibly damage the system and components or injury to yourself. Follow these guidelines when installing and servicing the Cisco Secure ACS Appliance:

Warning **Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.**

Warning **Do not touch the power supply when the power cord is connected. For systems with a power switch, line voltages are present within the power supply even when the power switch is off and the power cord is connected. For systems without a power switch, line voltages are present within the power supply when the power cord is connected.**

- Disconnect all power and external cables before installing the system.
- Install the system in compliance with your local and national electrical codes:
  - United States: National Fire Protection Association (NFPA) 70; United States National Electrical Code.
  - Canada: Canadian Electrical Code, Part, I, CSA C22.1.
  - Other countries: If local and national electrical codes are not available, refer to IEC 364, Part 1 through Part 7.
- Do not work alone under potentially hazardous conditions.
- Do not perform any action that creates a potential hazard to people or makes the equipment unsafe.
- Do not attempt to install the Cisco Secure ACS Appliance in a rack that has not been securely anchored in place. Damage to the system and personal injury may result.

See Chapter 2, “Preparing for Installation,” for additional safety information regarding installing the Cisco Secure ACS Appliance.

This section contains the following subsections:

- Connecting to Power Source, page 3-13
- Powering On the Cisco Secure ACS Appliance, page 3-13

Accessing Internal Components

The Cisco Secure ACS Appliance access panel can be removed to gain access to internal components or to allow clearance for attaching the optional cable support bracket.

Warning **Before working on a system that has an on/off switch, turn OFF the power and unplug the power cord.**

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units.**

Warning **Before opening the chassis, disconnect the telephone-network cables to avoid contact with telephone-network voltages**

Warning **The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.**

Caution Electrostatic discharge can damage electronic components. Be sure you are properly grounded if you may come in contact with components.

To remove the Cisco Secure ACS Appliance access panel, follow these steps:

Step 1 Ensure that the Cisco Secure ACS Appliance is powered down and disconnected from the electrical outlet.

Step 2 Disconnect from network cabling.

Step 3 Hold down the two latches on the top of the access panel while sliding it toward the rear of the unit (about half an inch).

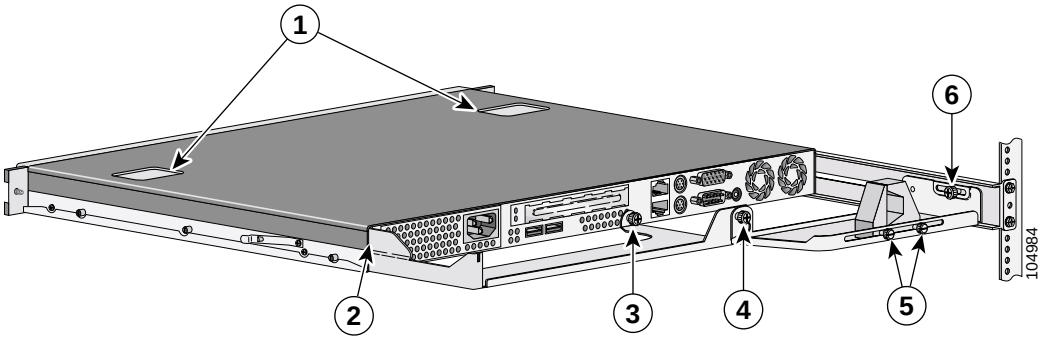
Step 4 Lift and remove the access panel.

Tip Reverse this procedure to reattach the access panel.

Installing the Cisco Secure ACS Appliance in a Rack

Cisco Secure ACS Appliance rack installation entails attaching rack rails, two different cable tray assembly components, and the unit itself to your existing equipment rack. See Figure 3-1 for a view of the final installation configuration from the rear and for the names of the parts.

Figure 3-1 Installation Overview - Rear View



1	Latches on chassis access panel	**4**	Fixed cable tray support bracket thumbnut
2	Hook on support bracket	**5**	Cable clamp thumbnuts
3	Cable support bracket thumbnut	**6**	Fixed cable tray rail thumbnut

To install the Cisco Secure ACS Appliance in a rack, follow these steps:

Step 1 Attach the rack rails to the rack:

a. Loosen the thumbnuts on each of the two rack rails provided.

b. Adjust the length of the rack rails so that the endplates fit outside the rack posts both in front and in the rear.

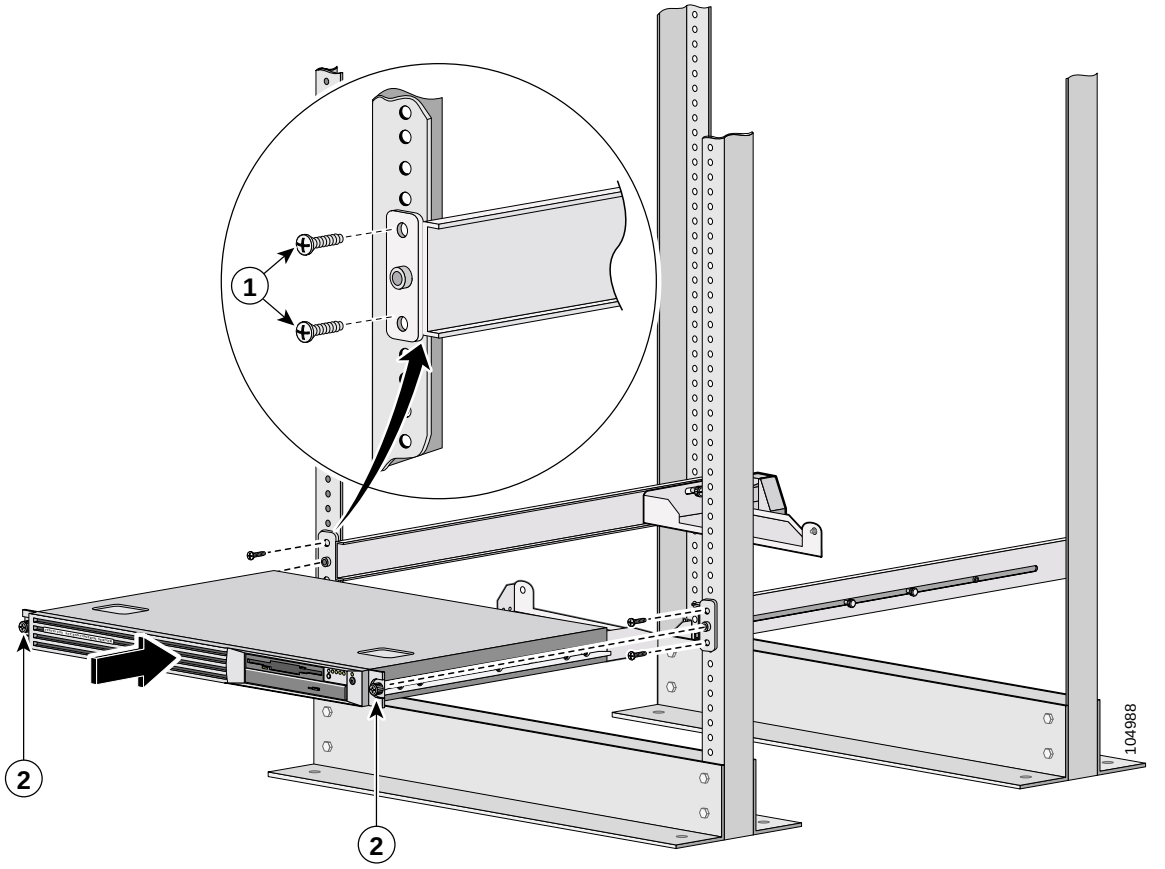
See Figure 3-2 for proper positioning of rack rails and endplates.

Note Ensure that the rack rails are positioned so that they are level, the thumbnuts and endplates are facing out, and the rails are to the inside of the rack posts.

c. Using 8 screws that you provide, appropriate to the size of your rack (1/4-20 or M6 thread size suggested), fasten the front and back endplates of each rack rail to the front and back of the rack.

d. Tighten the thumbnuts on both rack rails.

Figure 3-2 Rail and Chassis Installation



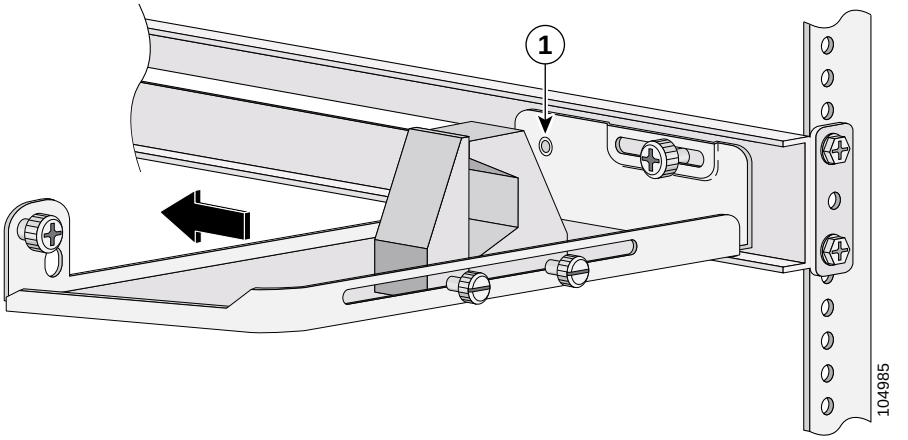
1	Screws sized to rack (not included)	**2**	Front panel thumbnuts

Step 2 Attach the fixed cable tray to the back rail post:

a. Insert the fixed cable tray post into the slot on the back of the rack rail and slide it toward the front of the rail to secure the post within the slot.

See Figure 3-3 for proper positioning of the fixed cable tray to the rack rail.

Figure 3-3 Fixed Cable Tray Installation



1	Fixed cable tray post		

Step 3 Attach the cable support bracket:

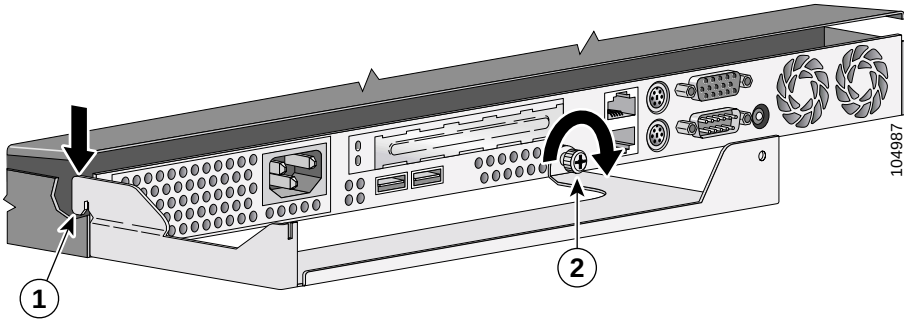
a. Remove the access panel. (See Accessing Internal Components, page 3-5).

b. On the left side of the back panel, hook the cable support bracket to the chassis. See Figure 3-4.

c. Use the cable support bracket thumbnut to fasten the cable support bracket to the back of the chassis.

d. Replace the access panel.

Figure 3-4 Cable Support Bracket Installation



1	Hook on support bracket	**2**	Cable support bracket thumbnut

Step 4 Insert the chassis into the rack:

a. Align the rear of the chassis with the front of the rack rails.

b. Slide the chassis into the rack; ensure that the fixed rails on the chassis slide inside the rack rails.

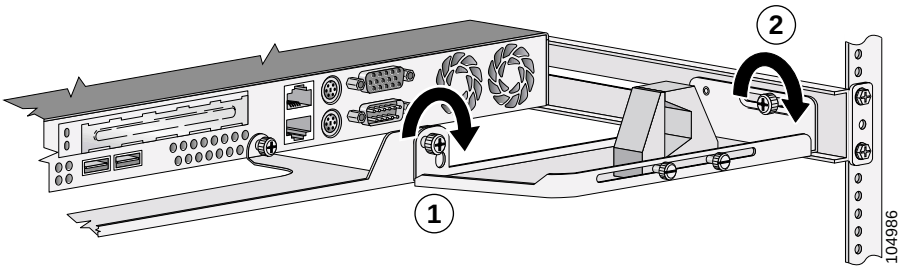
Caution The rack-mount kit is not intended for use as a slide rail system. You must complete installation by securely fastening the chassis into the rack.

c. Secure the chassis to the rack by tightening the two thumbnuts on the front panel of the chassis. (See Figure 3-2.)

d. At the rear of the rack, tighten the fixed cable tray support bracket thumbnut to secure the tray to the cable support bracket. (See Figure 3-5.)

e. Also at the rear of the rack, slide the fixed cable tray rail thumbnut to align with one of the screwholes on the rack rail. Tighten the thumbnut.

Figure 3-5 Chassis Attachment to Cable Tray



Connecting Cables

Use unshielded twisted pair (UTP) copper wire Ethernet cable, with standard RJ-45 compatible plugs, to connect Cisco Secure ACS Appliance to the network.

To connect the cables, follow these steps:

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.**

Step 1 Plug the network connection into the Ethernet port for NIC 1. For the location of the Ethernet port, see Figure 1-3 on page 1-5. The NIC is configured to automatically detect the speed and duplex mode of the network.

Tip The Ethernet port for NIC 1 is the lower of the two Ethernet ports. Only one Ethernet port can be used at one time.

Step 2 Loosen the cable clamp thumbnuts to open the cable clamp jaws and then tighten the thumbnuts to secure the jaws in the open position.

Step 3 Route the Ethernet cable through the cable clamp jaws.

Step 4 Connect a console to the serial port on the back panel. To connect the console to the terminal port:

a. Attach a DB-9 to RJ-45 adapter (provided) to the serial port on the console.

b. Attach a DB-9 to RJ-45 adapter (provided) to the console serial port on the back panel of the Cisco Secure ACS Appliance.

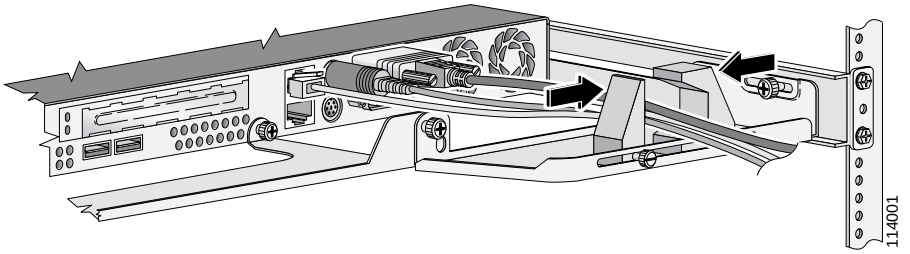
c. Connect the console to the Cisco Secure ACS Appliance using an RJ-45 cable (provided).

d. Route the RJ45 cable through the cable clamp.

Note The console terminal must be set to the VT 100 mode with 115200 baud, 8 bits, no parity, stops 1, and no flow control.

Step 5 When you have finished routing cables through the open cable clamp, loosen the cable clamp thumbnuts, slide the jaws of the cable clamp together, and retighten the cable clamp thumbnuts to secure the cables. See Figure 3-6.

Figure 3-6 Cable Clamp



Connecting to Power Source

Warning **Never defeat the ground conductor or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.**

Warning **Before working on equipment that is connected to power lines, remove jewelry (including rings, necklaces, and watches). Metal objects will heat up when connected to power and ground and can cause serious burns or weld the metal object to the terminals. (43)**

Step 1 Connect the power cable (provided) to the power connector on the back panel of the chassis.

Step 2 Route the power cable from the back of the chassis through the cable clamp.

Step 3 Close the cable clamp by sliding the two sides together and then tighten the thumbnuts on the clamp to secure the clamp closed.

Step 4 Connect the AC power receptacle to the AC power source with the provided power cable.

Powering On the Cisco Secure ACS Appliance

To power on the Cisco Secure ACS Appliance, press the power switch. (For location of the power switch, see Figure 1-2 on page 1-4.

To turn power off, press and hold the power switch. The power switch is located on the front panel, see Figure 1-2 on page 1-4. The power ON/OFF LED indicator is located directly above the power switch.

The system begins booting and sends messages to the console window. When the `login:` prompt appears, you can configure the system.

Initial Configuration

There are essentially four parts to configuring the Cisco Secure ACS Appliance. The first three steps are documented in this manual:

- Establishing a Serial Console Connection, page 3-14
- Configuring the Cisco Secure ACS Appliance, page 3-15
- Verifying the Initial Configuration, page 3-20

Note The fourth and final part of the configuration, which includes establishing administrative and user accounts and configuring network connections, is performed via the HTML interface and is detailed in the *User Guide for Cisco Secure ACS Appliance*.

Establishing a Serial Console Connection

Before you can perform the initial configuration of Cisco Secure ACS Appliance, you must establish a serial console connection to it. This requires a PC, two DB-9 to RJ-45 adapters (provided), an RJ-45 cable (provided), and Telnet communications software (Hyper Terminal or equivalent).

To establish a serial console connection, follow these steps:

Note If you performed the procedure in Connecting Cables, page 3-11, you can skip to Step 2.

Step 1 Connect a console to the serial console port on the back panel:

a. Attach a DB-9 to RJ-45 adapter (provided) to the serial port of the console.

b. Attach a DB-9 to RJ-45 adapter (provided) to the serial port of the Cisco Secure ACS Appliance. For the location of the serial port, see Figure 1-3 on page 1-5.

c. Use an RJ-45 cable (provided) to connect the console to the Cisco Secure ACS Appliance.

Tip You may also use a serial concentrator connection, if desired.

Step 2 Power on Cisco Secure ACS Appliance and the console, and open your Telnet communications software on the console.

Note Serial console service starts when Cisco Secure ACS Appliance boots up.

Step 3 Set your Telnet software to operate with the following settings:

- Baud = 115200
- Databits = 8
- Parity = N
- Stops = 1
- Flow control = None

Result*:* The `login:` prompt appears.

Configuring the Cisco Secure ACS Appliance

You must configure the Cisco Secure ACS Appliance when you boot the system for the first time, and whenever you re-image the system.

Before you begin to configure the appliance, you should have the following information at hand:

- Network hostname of the appliance.
- DNS domain name.
- Administrator name and password.
- Whether or not you will enable DCHP (enabling DCHP is not recommended).
- IP, netmask, and gateway addresses you will assign to the Cisco Secure ACS Appliance.
- Whether you will be using NTP synchronization and, if yes, the address of the NTP server.

To configure the Cisco Secure ACS Appliance, follow these steps:

Step 1 Establish a serial console connection to the Cisco Secure ACS Appliance; for details see Establishing a Serial Console Connection, page 3-14.

Note If the Cisco Secure ACS Appliance is not configured (that is, it is new or has been re-imaged) the system displays the system information—including the software version.

Step 2 Confirm that the following information is displayed above the `login:` prompt:

```
Cisco Secure ACS: [version number]
Appliance Management Software: [version number]
Appliance Base Image: [version number]
Status: Appliance is functioning properly
The ACS Appliance has not been configured.
Logon as “Administrator” with password “setup” to configure
appliance.
```

Step 3 At the `login:` prompt, type **Administrator** and then press **Enter**.

Note When you boot the system for the first time, it is not configured. Logging in as Administrator allows you to configure the system.

Result: The system displays the `password:` prompt.

Step 4 At the `password:` prompt, type **setup** and press **Enter**.

Note The password is case sensitive.

Result: The system displays the following message on the console:

```
Initialize Appliance.
Machine will be rebooted after initialization.
Entering Ctrl-C before setting appliance name will shutdown the
appliance
```

Step 5 At the `ACS Appliance name [deliverance1]:` prompt, type the name you intend to use for your Cisco Secure ACS Appliance, and then press **Enter**.

Tip The name can contain up to 15 letters and numbers, but no spaces.

Result*:* The system displays the following message on the console:

```
ACS Appliance name is set to xxx.
```

Step 6 At the `DNS domain [ ]:` prompt, type the domain name. Then press **Enter**.

Result*:* The system displays the following message on the console:

```
DNS name is set to xxx.com.
You need to set the administrator account name and password.
```

Step 7 At the `Enter new account name:` prompt, type the Cisco Secure ACS Appliance administrator account name, and then press **Enter**.

Tip There is only one Cisco Secure ACS Appliance administrator account at a given time. The account's credentials can be changed. For more information see Chapter 4, "Resetting the Appliance Administrator Password."

Step 8 At the `Enter new password:` prompt, type the new Cisco Secure ACS Appliance password and press **Enter**.

Note The new password must contain a minimum of 6 characters, and it must include a mix of at least three character types (uppercase letters, lowercase letters, digits, and special characters). Each of the following examples is acceptable: 1PaSsWoRd, *password44, Pass*word. The password cannot contain the account name.

Step 9 At the `Enter new password again:` prompt, type the new Cisco Secure ACS Appliance password, and then press **Enter**.

Result*:* The system displays the following message on the console:

```
Password is set successfully.
Administrator name is set to xxx.
```

Step 10 At the `Use Static IP Address [Yes]:` prompt, type **Y** for yes or **N** for No, and then press **Enter**.

Note To set or change the IP address of your Cisco Secure ACS Appliance, it must be connected to a working Ethernet connection.

Note A static IP address must be assigned to your Cisco Secure ACS Appliance. You can set the IP address directly by answering **Y** to this step and performing the substeps detailed in Step 11. Alternatively, you may use a DHCP server if it assigns a single IP address that does not change.

Step 11 The following prompts appear only if you set a static IP address manually. Otherwise the following message appears:

```
No change to the configuration.
Accept network setting [Yes]
```

a. To specify the Cisco Secure ACS Appliance IP address, at the `IP Address [xx.xx.xx.xx]:` prompt, type the IP address, and then press **Enter**.

b. At the `Subnet Mask [xx.xx.xx.xx]:` prompt, type the subnet mask value, and then press **Enter**.

c. At the `Default Gateway [xx.xx.xx.xx]:` prompt, type the default gateway value, and then press **Enter**.

d. At the `DNS Servers [xx.xx.xx.xx]:` prompt, type the address of any DNS servers you intend to use (separate each by a single space), and then press **Enter**.

Note If you do not intend to use a DNS server, enter the IP address of the Cisco Secure ACS Appliance at the `DNS Servers [xx.xx.xx.xx]:` prompt. If you do not configure the Cisco Secure ACS Appliance to use a DNS server, you must respond to all prompts for "`hostname or IP address`" only with an IP address.

Result*:* The system displays the new configuration information followed by the following message:

```
IP Address is reconfigured.
```

e. At the prompt, `Confirm the changes? [Yes]:` type **Y**, and then press **Enter**.

Result*:* The system displays the following message:

```
New ip address is set.
Default gateway is set to xx.xx.xx.xx
DNS servers are set to: xx.xx.xx.xx xx.xx.xx.xx.
```

f. At the prompt, `Test network connectivity [Yes]:`, type **Y**, and then press **Enter**.

Tip This step is essentially executing a **ping** command to ensure the connectivity of the Cisco Secure ACS Appliance.

g. At the prompt, `Enter hostname or IP address:`, type the IP address or hostname of a device connected to the Cisco Secure ACS Appliance, and then press **Enter**.

Result*:* If successful, the system displays the ping statistics. The system displays the prompt: `Test network connectivity [Yes]:`.

h. If network connectivity is proven okay in the previous two steps, at the prompt, `Test network connectivity [Yes]:`, type **N**, and then press **Enter**.

Tip The system continues to provide you with the opportunity to test network connectivity until you answer no. This gives you an opportunity, if required, to correct network connections or retype the IP address.

Step 12 If the settings have been correctly displayed, at the prompt, `Accept network setting [Yes]:`, type **Y**, and then press **Enter**.

Result*:* The system displays the following message on the console:

```
Current Date Time Setting:
Time Zone: (GMT -xx:xx) XXX Time
Date and Time: mm/dd/yyyy
NTP Server(s): NTP Synchronization Disabled.
```

Step 13 To set the time and date of the Cisco Secure ACS Appliance, at the `Change Date & Time Setting [N]:` prompt, type **Y**, and then press **Enter**.

Result*:* The system displays a numbered list of time zones.

Step 14 At the `Enter desired time zone index (0 for more choices):` prompt, type the index number of the time zone you want set, and then press **Enter**.

Result*:* The system displays the new time zone.

Step 15 At the `Synchronize with NTP server? [N]:` prompt, do one of the following:

- To set the time manually, type **N**, and then press **Enter**.
- To use an NTP server for setting time, type **Y**, and when prompted enter the IP address of the NTP server you want to use.

Result*:* The system displays a confirmation message reflecting your choice.

Step 16 At the `Enter date [mm/dd/yyyy]:` prompt, type the date in the given format, and then press **Enter**.

Step 17 At the `Enter time [hh:mm:ss]:` prompt, type the current time in the given format, and then press **Enter**.

Result*:* The system displays the following message on the console:

```
Initial configuration is successful. Appliance will now reboot.
```

The system reboots.

Verifying the Initial Configuration

To verify that you have correctly completed the Cisco Secure ACS Appliance initial configuration, follow these steps:

Before You Begin

Establish a serial console connection to the Cisco Secure ACS Appliance. For details see Establishing a Serial Console Connection, page 3-14.

Step 1 Reboot the Cisco Secure ACS Appliance. For more information, see Rebooting the Appliance via Serial Console, page 4-4.

Result: When the systems finish booting, a `login:` prompt appears on the console.

Step 2 At the `login:` prompt, type the new administrator name, press **Enter**, and then at the `password:` prompt, enter the password you created during initial configuration.

Result: The system prompt appears.

Step 3 At the system prompt, type **show**, and then press **Enter**.

Result: The system displays status information.

Step 4 Verify the information displayed.

Next Steps

After you have successfully performed the procedures in this guide, your Cisco Secure ACS Appliance is installed and initially configured. The next step is to use a browser and the HTML interface to fully configure your Cisco Secure ACS Appliance to provide the AAA services you want from this installation. The HTML address is in the following format: HTTP//[*ip address*]:2002, where *ip address* is the address you assign during configuration.

For information on setting up user, group, network, and other parameters, see the *User Guide for Cisco Secure ACS Appliance*.

Administering the Cisco Secure ACS Appliance

This section describes the major Cisco Secure ACS Appliance 3.2 system administration tasks that you can perform via the serial console connection command line interface (CLI). For all other Cisco Secure ACS Appliance configuration and administration tasks, that is, those performed from the ACS HTML interface, see the *User Guide for Cisco Secure ACS Appliance*.

Serial console service starts automatically when the Cisco Secure ACS Appliance boots and prompts the user to log in. Successful login launches a command line application (shell) that operates the CLI.

This section contains the following topics:

Basic Command Line Administration Tasks

This section details basic administrative tasks performed using a serial console connected the Cisco Secure ACS Appliance. This section contains the following procedures:

Logging On to the Appliance via Serial Console

To log on to the Cisco Secure ACS Appliance via a serial console, follow these steps:

Step 1 Establish a serial console connection to the Cisco Secure ACS Appliance. For details, see Establishing a Serial Console Connection, page 3-14.

Step 2 At the `login:` prompt, enter the Cisco Secure ACS Appliance administrator name.

Step 3 At the `password:` prompt, enter the Cisco Secure ACS Appliance password.

Result: The system prompt appears in the following form:

`Cisco Secure ACS Appliance name`

Note There is only one set of Cisco Secure ACS Appliance login credentials (administrator name and password) that have the serial connection privilege.

Shutting Down the Appliance via Serial Console

Caution Powering off the Cisco Secure ACS Appliance by using the Power button may cause the loss or corruption of data. Use this procedure to shut down the Cisco Secure ACS Appliance.

To use the serial console to shut down the Cisco Secure ACS Appliance, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 At the system prompt, type **shutdown**, and then press **Enter.**

Step 3 At the `Are you sure you want to shut down? (Y/N)` prompt, type **Y** for yes and then press **Enter**.

Result: The Cisco Secure ACS Appliance displays the following message:

```
Shutting down the system (This may take several minutes)
```

The Cisco Secure ACS Appliance then ends operations and powers OFF.

Logging Off the Appliance via Serial Console

To log off the Cisco Secure ACS Appliance via the serial console, follow these steps:

Step 1 At the system prompt, type **exit**.

Step 2 Press **Enter.**

Result: The serial console connection closes, and the `login:` prompt reappears.

Rebooting the Appliance via Serial Console

To reboot the Cisco Secure ACS Appliance via the serial console, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 At the system prompt, type **reboot**, and then press **Enter**.

Result: The Cisco Secure ACS Appliance displays the following message:

```
Are you sure you want to reboot? (Y/N)
```

Step 3 Type **Y** for yes and then press **Enter**.

Result: The Cisco Secure ACS Appliance reboots. When the reboot is finished, the `login:` prompt reappears.

Determining the Status of Appliance System and Services via Serial Console

You can use the serial console connection to obtain system and service status information.

Note Status determination is typically performed from within the Cisco Secure ACS Appliance HTML user interface. For more information, see "Determining the Status of Cisco Secure ACS Services" in the *User Guide for Cisco Secure ACS Appliance*.

To determine the status of the Cisco Secure ACS Appliance and the Cisco Secure ACS Services, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 At the system prompt, type **show**, and then press **Enter**.

Result: The system displays the following status information:

```
Cisco Secure ACS Appliance Name
Cisco Secure ACS Appliance Version

Appliance Management Software Version
Appliance Base Image Version
Session Timeout (in minutes)
Current Date & Time
Time Zone
NTP Server(s)
CPU Load (percentage)
Free Disk (amount of hard drive space available)
Free Physical Memory
Appliance IP Configuration
    DHCP Enabled (Yes/No)
    IP Address
    Subnet Mask
    Default Gateway
    DNS Servers
ACS Services (running/stopped)
    CSAdmin
    CSAuth
    CSDbSync
    CSLog
    CSMon
    CSRadius
    CSTacacs
```

Tracing Routes

If you are unfamiliar with the **trace route** command or want information on the command's optional arguments, see the Command Reference entry tracert, page C-21.

To trace the network route taken by the Cisco Secure ACS Appliance to a given destination, follow these steps:

Step 1 At the system prompt, type **tracert**, followed by zero or more optional arguments and then the IP address of the target destination.

Step 2 Press **Enter.**

Result: The system displays the route tracing information followed by the message:

```
Trace complete
```

Stopping Appliance Services via Serial Console

Note Stopping appliance services is a procedure that is typically performed from within the HTML interface.

You can stop any of the Cisco Secure ACS Appliance services from the serial console. The Cisco Secure ACS Appliance services include the following:

- CSAdmin
- CSAuth
- CSDbSync
- CSLog
- CSMon
- CSRadius
- CSTacacs

Tip To list the services and their status, you can use the **show** command. For more information, see Determining the Status of Appliance System and Services via Serial Console, page 4-4.

To stop a service on the Cisco Secure ACS Appliance, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 Type **stop** followed by a single space and the name of the ACS service you want to stop.

Tip You can list more than one service to stop; type a single space between each.

Step 3 Press **Enter**.

Result: The system immediately shows the message:

```
[service name] is stopping. . .
```

Followed by the message:

```
[service name] is not running
```

Starting Appliance Services via Serial Console

Note Starting appliance services is typically performed from within the HTML user interface.

You can start any of the ACS services from the serial console. The Cisco Secure ACS Appliance services include the following:

- CSAdmin
- CSAuth

- CSDbSync
- CSLog
- CSMon
- CSRadius
- CSTacacs

Tip To list the services and their status, you can use the **show** command. For more information, see Determining the Status of Appliance System and Services via Serial Console, page 4-4.

To start an ACS service, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 Type **start** followed by a single space and the name of the ACS service you want to start.

Tip You can list more than one service to start; type a single space between each.

Step 3 Press **Enter**.

Result: The system immediately shows the message:

```
[service name] is starting. . .
```

Followed by the message

```
[service name] is running
```

Restarting Appliance Services via Serial Console

Note Restarting appliance services is a procedure that is typically performed from within the HTML interface.

You can restart any Cisco Secure ACS Appliance service from the serial console. Cisco Secure ACS Appliance services include the following:

- CSAdmin
- CSAuth
- CSDbSync
- CSLog
- CSMon
- CSRadius
- CSTacacs

Tip To list the services and their status, you can use the **show** command. For more information, see Determining the Status of Appliance System and Services via Serial Console, page 4-4.

To restart an ACS service, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 Type **restart** followed by a single space and the name of the ACS service you want to restart.

Tip You can list more than one service to restart; type a single space between each.

Step 3 Press **Enter**.

Result: The system immediately shows the message:

```
service name is stopping. . .
```

Followed by the messages

```
service name is not running
service name is starting
service name is running
```

Getting Command Help via Serial Console

To obtain a list and description of commands on the Cisco Secure ACS Appliance via the serial console, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 At the system prompt, type **help**, and then press **Enter**.

Tip Press **Enter** again to scroll through the list of commands, as necessary.

Result: The Cisco Secure ACS Appliance displays the following list of commands and their descriptions:

```
?               List commands

backup          Backup Appliance

dbcompact       Database Compact

download        Download ACS Install Package

exit            Log off

exportgroups    Export group information to an FTP server
```

```
exportlogs      Export appliance diagnostic logs to FTP server
exportusers     Export user information to an FTP server
help            List commands
ping            Verify connections to remote computers
reboot          Soft reboot appliance
restart         Restart ACS services
restore         Restore Appliance
rollback        Rollback patched package
set admin       Set administrator's name
set domain      Set DNS domain
set hostname    Set appliance's hostname
set ip          Set IP configuration
set password    Set administrator's password
set time        Set timezone, enable NTP synch, or set date and time
set timeout     Set the timeout for serial console with no activity
show            Show appliance status
shutdown        Shutdown appliance
start           Start ACS services
stop            Stop ACS services
support         Collect logs, registry, and other useful information
tracert         Determine the route take to a destination
upgrade         Upgrade appliance (stage II)
```

For more information on Cisco Secure ACS Appliance commands, see Appendix C, "Command Reference."

Working with System Data

This section details basic data manipulation tasks performed from a serial console connected to the Cisco Secure ACS Appliance. This section contains the following procedures:

Obtaining Support Logs via the Serial Console

This section details the procedure for running the support tool. The support tool first collects logs, system Registry information, and other ancillary data, and then compresses the collected information into a single file with the extension .cab. This file can then be sent to support personnel for analysis.

Caution Performing this procedure stops and restarts all services and will interrupt use of the Cisco Secure ACS Appliance.

Note This procedure is typically performed from within the Cisco Secure ACS Appliance HTML interface.

This procedure uses the **support** command. For more information on this command, see support, page C-20, of Appendix C, "Command Reference." The arguments for the **support** command include the following:.

`-d n`	`collect the previous n days logs.`
`-u`	`collect user database information`
`server`	`the hostname for the ftp server to which the file is to be sent`
`filepath`	`the location under the ftp root for the server into which the package.cab is to be sent`
`username`	`the account used to authenticate the ftp session`

To generate a .cab file of log and system Registry information, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 Type **support** and the arguments necessary to your purpose.

Step 3 Press **Enter**.

Step 4 To collect user database information, at the `Collect User Data?` prompt, type **Y** and then press **Enter**.

Step 5 At the `Collect Previous days logs?` prompt, type the number of days for which you want to collect information (from 1 to 9999) and press **Enter**.

Step 6 At the `Enter FTP Server Hostname` prompt, enter your FTP server hostname or IP address and press **Enter**.

Step 7 At the `Enter FTP Server Filepath` prompt, enter the filepath to the location on your FTP server that you want to send the file to and then press **Enter**.

Step 8 At the `Enter FTP Server Username` prompt, enter your FTP server user account name and press **Enter**.

Caution Performing this next step begins the procedure that stops and restarts all services and will, therefore, interrupt use of the Cisco Secure ACS Appliance.

Step 9 At the `Enter FTP Server Password` prompt, enter your FTP server password and press **Enter**.

Result: The Cisco Secure ACS Appliance displays a series of messages detailing the writing and dumping of the files and the stopping and starting of services. At file transfer conclusion the system displays the following messages:

```
Transferring 'Package.cab' completed
Press any key to finish.
```

This indicates the Cisco Secure ACS Appliance has packaged and transferred the .cab file as specified and restarts services.

Step 10 Press **Enter.**

Result: The system returns to the system prompt.

Exporting Logs

This section details the procedure for exporting Cisco Secure ACS Appliance log files to an FTP server for further examination and processing. Using the **exportlogs** command, you can either enter the name of the log or logs to exported or select log names from a list.

Before you begin

You must have the FTP server address and filepath, as well as the proper credentials for writing to the FTP server (username and password).

Caution Performing this procedure stops and restarts all services and will interrupt use of the Cisco Secure ACS Appliance.

To export log files to an FTP server, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 Type **exportlogs** ***logname***.

Tip You can enter more than one log name separating each with a space. If you enter no log name, after you press **Enter,** the system displays the names of the log files available for export.

Caution Performing this procedure stops and restarts all services and will interrupt use of the Cisco Secure ACS Appliance.

Step 3 Press **Enter**.

Step 4 At the prompt, enter the IP address or hostname of the FTP server and press **Enter**.

Step 5 At the prompt, enter your FTP server username and press **Enter**.

Step 6 At the prompt, enter your FTP server password and press **Enter**.

Step 7 At the prompt, enter the FTP server directory filepath and press **Enter**.

Result: The Cisco Secure ACS Appliance exports the specified files to the specified location.

Exporting a List of Groups

This section details the procedure for exporting a list of Cisco Secure ACS Appliance user groups to an FTP server for further examination and processing.

Before you begin

You must have the FTP server address and filepath, as well as the proper credentials for writing to the FTP server (username and password).

Caution Performing this procedure stops and restarts the csauth service and will interrupt use of the Cisco Secure ACS Appliance.

To export a user group list to an FTP server, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 Type **exportgroups**.

Tip You can enter the following parameters following the command or in response to subsequent prompts: [server] [username] [filepath]

Step 3 Press **Enter**.

Result: The system displays the following message:

```
Command with restart CSAuth. Are you sure you want to continue?
```

Caution Performing this procedure stops and restarts the csauth service and will interrupt use of the Cisco Secure ACS Appliance.

Step 4 To proceed, type **Y** and press **Enter**.

Step 5 At the `Enter IP Address or hostname of the FTP Server` prompt, enter the FTP server IP address or hostname and press **Enter**.

Step 6 At the `Login:` prompt, enter your FTP server username and press **Enter**.

Step 7 At the `Password:` prompt, enter your FTP server password and press **Enter**.

Step 8 At the `Directory:` prompt, enter the FTP server filepath and press **Enter**.

Result: The Cisco Secure ACS Appliance exports the group list file to the specified location. When done the system displays following message:

```
Transferring ‘groups.txt’ completed
```

The system prompt returns.

Exporting a List of Users

This section details the procedure for exporting a list of Cisco Secure ACS Appliance users to an FTP server for further examination and processing.

Before you begin

You must have the FTP server address and filepath, as well as the proper credentials for writing to the FTP server (username and password).

Caution Performing this procedure stops and restarts the csauth service and will interrupt use of the Cisco Secure ACS Appliance.

To export a list of users to an FTP server, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 Type **exportusers**.

Tip You can enter the following parameters following the command or in response to subsequent prompts: [server] [username] [filepath]

Step 3 Press **Enter**.

Result: The system displays the following message:

```
Command with restart CSAuth. Are you sure you want to continue?
```

Caution Performing this procedure stops and restarts the csauth service and will interrupt use of the Cisco Secure ACS Appliance.

Step 4 To proceed, type **Y** and press **Enter**.

Step 5 At the `Enter IP Address or hostname of the FTP Server` prompt, enter the FTP server IP address or hostname and press **Enter**.

Step 6 At the `Login:` prompt, enter your FTP server username and press **Enter**.

Step 7 At the `Password:` prompt, enter your FTP server password and press **Enter**.

Step 8 At the `Directory:` prompt, enter the FTP server filepath and press **Enter**.

Result: The Cisco Secure ACS Appliance exports the list of users file to the specified location. When done the system displays following message:

```
Transferring 'users.txt' completed
```

The system prompt returns.

Backing Up ACS Data via the Serial Console

This section details how to use the serial console to backup Cisco Secure ACS Appliance data to an FTP server.

Note This procedure is typically performed from within the HTML interface.

During backup, AAA services are interrupted and Cisco Secure ACS Appliance data is packaged and sent in a file to an FTP server. You may choose to encrypt this file package. For information on how to restore the backup data to the system, see Restoring ACS Data via the Serial Console, page 4-20.

Before you begin

You must have the FTP server address and filepath, as well as the proper credentials for writing to the FTP server (username and password).

Caution This procedure interrupts the use of the Cisco Secure ACS Appliance for AAA services.

To export Cisco Secure ACS Appliance data to an FTP server, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 Type **backup**.

Tip You can enter the following parameters following the command or in response to subsequent prompts: [server] [username] [filepath]

Step 3 Press **Enter**.

Step 4 At the `Enter FTP Server Hostname or IP Address:` prompt, enter the FTP server IP address or hostname and press **Enter**.

Step 5 At the `Enter FTP Server Directory:` prompt, enter the FTP server filepath and press **Enter**.

Step 6 At the `Enter FTP Server Username:` prompt, enter your FTP server username and press **Enter**.

Step 7 At the `Enter FTP Server Password:` prompt, enter your FTP server password and press **Enter**.

Step 8 At the `File:` prompt, enter the name you want to give the backup file and then press **Enter**.

Step 9 At the `Encrypt Backup File? (Y or N)` prompt, type **Y** to encrypt the backup file or **N** not to encrypt it, and then press **Enter**.

Caution This procedure interrupts the use of the Cisco Secure ACS Appliance for AAA services.

Step 10 If you previously chose to encrypt the backup file, at the `Encryption Enter FTP Server Password:` prompt, type a password and then press **Enter**.

Result: The Cisco Secure ACS Appliance displays the following messages:

```
Backing up now . . .
All running services will be stopped and restarted automatically.
Are you sure you want to proceed? (y/Y = proceed)
```

Step 11 To proceed, type **Y** and press **Enter**.

Result: The Cisco Secure ACS Appliance exports the backup file to the specified location and displays messages regarding the progress of the backup. Before returning to the system prompt, the following message signifies the completion of the backup process:

```
Transferring xxx completed.
```

Restoring ACS Data via the Serial Console

This section details how use the serial console to restore Cisco Secure ACS Appliance data from an FTP server after having performed a backup. For more information on backing up Cisco Secure ACS Appliance data, see Backing Up ACS Data via the Serial Console, page 4-18.

Note This procedure is typically performed from within the HTML interface.

Before you begin

You must have the FTP server address and filepath, as well as the proper credentials for writing to the FTP server (username and password). You also need the name of the backup file and, if the backup was encrypted, the decryption password.

Caution This procedure interrupts the use of the Cisco Secure ACS Appliance for AAA services.

Caution This procedure overwrites current system data and replaces it with the backup data.

To restore Cisco Secure ACS Appliance data from an FTP server, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 Type **restore**.

Tip You can enter the following parameters following the command or in response to subsequent prompts: [server] [username] [filepath]

Step 3 Press **Enter**.

Step 4 At the `Enter FTP Server Hostname or IP Address:` prompt, enter the FTP server IP address or hostname and press **Enter**.

Step 5 At the `Enter FTP Server Directory:` prompt, enter the FTP server filepath and press **Enter**.

Step 6 At the `Enter FTP Server Username:` prompt, enter your FTP server username and press **Enter**.

Step 7 At the `Enter FTP Server Password:` prompt, enter your FTP server password and press **Enter**.

Step 8 At the `File:` prompt, enter the name of the backup file and then press **Enter**.

Step 9 At the `Select Components to Restore: User and Group Database:` prompt, to restore the user and group database type **Y** and then press **Enter**.

Step 10 At the `CiscoSecure ACS System Configuration: (Y or N)` prompt, to restore the system configuration data type **Y** and then press **Enter**.

Step 11 At the `Decrypt Backup file? (Y or N)` prompt, if you previously encrypted the backup file, type **Y** and then press **Enter**.

Step 12 At the `Encryption Password:` prompt, type the FTP password**,** and then press **Enter**.

Note The system displays a warning message:

```
Reloading a system backup will overwrite ALL current configuration
information. All services will be stopped and started automatically
```

Step 13 At the `Are you sure you want to proceed? (Y or N)` prompt, type **Y** and then press **Enter**.

Result: The Cisco Secure ACS Appliance receives the backup file from the specified location and displays messages regarding the restoration. You may see warnings about components not included in the backup file. For example, if Cisco Secure ACS Appliance has no shared profile components configured, you see a message about DCS (device command sets) not on the backup. This is normal.

When completed the system displays the message:

```
Done
```

Compacting the ACS Appliance Database

This section details the procedure you perform to compact the Cisco Secure ACS Appliance user database. Like many relational databases, the Cisco Secure ACS Appliance user database handles the deletion of records by marking deleted records as deleted but not removing the record from the database. Over time, your Cisco Secure ACS Appliance user database may be substantially larger than is required by the number of users it contains. To reduce the CiscoSecure user database size, you can compact it periodically.

Database compaction includes three basic operations that take place automatically when you issue the **dbcompact** command:

- A database dump occurs.
- The database is initialized, thus removing deleted records.
- The dumped data is loaded back to the database.

Performing this procedure can reduce the amount of space that the database takes up and improve the database response time.

Caution Compacting the CiscoSecure user database requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

Note This procedure is typically performed from within the Cisco Secure ACS Appliance HTML user interface.

To compact the Cisco Secure ACS Appliance use database, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 Type **dbcompact**.

Result: The system displays the following message:

```
Command will restart CSAuth. Are you sure you want to continue? (Y/N):
```

Caution Compacting the CiscoSecure user database requires that you stop the CSAuth service. While CSAuth is stopped, no users are authenticated.

Step 3 Type **Y**, and then press **Enter**.

Result: The system displays a series of messages similar to the following:

```
Stopping service: CSAuth
Done
Initializing database . . .
Loading database from dump.txt . . .
Done
Starting service: CSAuth
```

Finally, the system returns to displaying the system prompt.

Reconfiguring Appliance System Parameters

This section details basic reconfiguration tasks performed from a serial console connected the Cisco Secure ACS Appliance. This section contains the following procedures:

- Resetting the Appliance Administrator Password, page 4-24
- Resetting the Appliance Administrator Name, page 4-25

Resetting the Appliance Administrator Password

There is always a single set of Cisco Secure ACS Appliance administrator credentials consisting of administrator name and password. Unlike other ACS administrative accounts, this unique administrative account is granted all privileges, cannot be deleted, and is not listed in the Administrators table of the Administrative Control page in the Cisco Secure ACS HTML user interface.

You can reset the Cisco Secure ACS Appliance administrator name, the administrator password, or both. This procedure details how to reset the password after having logged on with the existing credentials. To reset the administrator name see Resetting the Appliance Administrator Name, page 4-25.

If you do not have the existing Cisco Secure ACS Appliance administrator login credentials with which to log on, you must have the recovery CD ROM to reset these credentials. For information on resetting the administrator login and password without first logging on, see Recovering from Loss of Administrator Credentials, page 4-38.

To reset the Cisco Secure ACS Appliance administrator login credentials, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 At the system prompt, type **set password** and then press **Enter.**

Result: The Cisco Secure ACS Appliance displays the following prompt:

```
Set administrator's password
```

Step 3 Type the new password, and then press **Enter**.

Note The new password must not contain the administrator account name, must contain a minimum of 6 characters, and it must include a mix of at least 3 character types (numerals, special characters, upper case letters, and lowercase letters). Each of the following examples is acceptable: 1PaSsWoRd, *password44, Pass*word.

Step 4 At the *`Set password again`* prompt, type the password again and then press **Enter**.

Result: The system displays the following message on the console:

`Password is set successfully.`

Resetting the Appliance Administrator Name

There is always a single set of Cisco Secure ACS Appliance administrator credentials consisting of administrator name and password. Unlike other ACS administrative accounts, this unique administrative account is granted all privileges, cannot be deleted, and is not listed in the Administrators table of the Administrative Control page in the Cisco Secure ACS HTML user interface.

You can reset the Cisco Secure ACS Appliance administrator name, the administrator password, or both. This procedure details how to reset the administrator name after having logged on with the existing credentials. To reset the password, see Resetting the Appliance Administrator Password, page 4-24.

If you do not have the existing Cisco Secure ACS Appliance administrator login credentials with which to log on, you must have the recovery CD ROM to reset these credentials. For information on resetting the administrator login and password without first logging on, see Recovering from Loss of Administrator Credentials, page 4-38.

To reset the Cisco Secure ACS Appliance administrator name, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 At the system prompt, type **set admin**, and then press **Enter.**

Result: The Cisco Secure ACS Appliance displays the *`Set administrator's name`* prompt.

Step 3 Type the new administrator name, and then press **Enter**.

Step 4 At the *`Set administrator name again`* prompt, type the administrator name again and then press **Enter**.

Result*:* The system displays the following message on the console:

`Administrator name is set successfully.`

Reconfiguring the Appliance IP Address

Typically, you configure the IP address only once, during initial configuration. See Configuring the Cisco Secure ACS Appliance, page 3-15.

Caution Reconfiguring the IP address may cause other network devices to fail to recognize the Cisco Secure ACS Appliance.

Caution Reconfiguring the IP address causes services to restart. AAA services to users will be interrupted.

Note To set or change the IP address of your Cisco Secure ACS Appliance, it must be connected to a working Ethernet connection.

To reconfigure the IP address, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 Type **set ip**, and then press **Enter**.

Step 3 At the `Use Static IP Address [Y]:` prompt, type **Y** for yes or **N** for No, and then press **Enter**.

Step 4 If you answered **No** to using a static IP address, the system displays a confirmation of DHCP and the message `IP Address is reconfigured`. Continue the procedure with Step 5.

If you responded **Yes** in the previous step to use a static IP address, do the following:

a. To specify the Cisco Secure ACS Appliance IP address, at the `IP Address [xx.xx.xx.xx]:` prompt, type the IP address, and then press **Enter**.

b. At the `Subnet Mask [xx.xx.xx.xx]:` prompt, type the subnet mask, and then press **Enter**.

c. At the `Default Gateway [xx.xx.xx.xx]:` prompt, type the default gateway, and then press **Enter**.

d. At the `DNS Servers [xx.xx.xx.xx]:` prompt, type the address of any DNS servers you intend to use (separate each by a single space), and then press **Enter**.

Result*:* The system displays the new configuration information and the following message:

```
IP Address is reconfigured.
```

Step 5 Review the information presented and, at the `Confirm the changes? [Y]:` prompt, press **Enter**.

Result*:* The Cisco Secure ACS Appliance restarts. The system displays the following message:

```
New ip address is set.
```

Step 6 At the prompt, `Test network connectivity [Yes]:`, type **Y**, and then press **Enter**.

Tip This step executes a **ping** command to ensure the connectivity of the Cisco Secure ACS Appliance.

Step 7 At the prompt, `Enter hostname or IP address:`, type the IP address or hostname of a device connected to the Cisco Secure ACS Appliance and then press **Enter**.

Result: If successful, the system displays the ping statistics. Once again the system displays the prompt: `Test network connectivity [Yes]:`.

Step 8 If network connectivity is proven okay in the previous two steps, at the prompt, `Test network connectivity [Yes]:`, type **N**, and then press **Enter**.

Tip The system will continue to provide you with the opportunity to test network connectivity until you answer no. This gives you an opportunity, if required, to correct network connections or retype the IP address.

Result: The Cisco Secure ACS Appliance restarts services, after which, it displays the system prompt.

Setting the System Time and Date Manually

You can set and maintain the system date and time using either of two methods:

- Set the time and date manually.
- Assign a network time protocol (NTP) server with which the system synchronizes its date and time.

To set the Cisco Secure ACS Appliance system time and date using an NTP, see Setting the System Time and Date with NTP, page 4-29.

To set the Cisco Secure ACS Appliance system time and date manually, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 At the system prompt, type **set time**, and then press **Enter**.

Result*:* The system displays the following message on the console:

```
Current Date Time Setting:
    Time Zone: (GMT -xx:xx) XXX Time
    Date and Time: mm/dd/yyyy hh/mm/ss

NTP Servers: (“Ntp Synchronization Disabled” - or -a list of NTP
servers)
Change Date & Time Setting? [N]
```

Step 3 To set the time zone, time, or date type **Y**, and then press **Enter**.

Result*:* The system displays a list of indexed time zones and the following message:

```
[xx] (GMT -xx:xx) XXX Time.
Enter desired time zone index (0 for more choices) [x]:
```

Step 4 Enter the desired time zone index number from the time zone setting list, and then press **Enter**.

Tip You can also type **0** (zero) and press **Enter** to see more time zone index numbers.

Result*:* The system displays the new time zone.

Step 5 At the `Synchronize with NTP Server?` prompt, type **N**, and then press **Enter**.

Step 6 At the `Enter date [mm/dd/yyyy]:` prompt, type the date, and then press **Enter**.

Step 7 At the `Enter time [hh:mm:ss]:` prompt, type the current time, and then press **Enter**.

Result*:* The system time is reset.

Setting the System Time and Date with NTP

You can set and maintain the system date and time using either of two methods:

- Set the time and date manually.
- Assign a network time protocol (NTP) server with which the system synchronizes its date and time.

To set the Cisco Secure ACS Appliance system time and date manually, see Setting the System Time and Date Manually, page 4-28.

To set the Cisco Secure ACS Appliance system time and date with NTP, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 At the system prompt, type **set time**, and then press **Enter**.

Result: The system displays the following message on the console:

```
Current Date Time Setting:
    Time Zone: (GMT -xx:xx) XXX Time
    Date and Time: mm/dd/yyyy hh/mm/ss
    NTP Servers: (“Ntp Synchronization Disabled” - or - List of NTP
    servers)
Change Date & Time Setting? [N]
```

Step 3 To set the time zone, time, or date type **Y**, and then press **Enter**.

Result: The system lists indexed time zones and the following message:

```
[xx] (GMT -xx:xx) XXX Time.
Enter desired time zone index (0 for more choices) [x]:
```

Step 4 Enter the desired time zone index number from the time zone setting list, and then press **Enter**.

Tip You can also type **0** (zero) and press **Enter** to see more time zone index numbers; or simply press **Enter** to accept the existing time zone.

Result: The system displays the time zone setting.

Step 5 At the `Synchronize with NTP Server?` prompt, type **Y**, and then press **Enter**.

Step 6 At the `Enter NTP Server IP Address:` prompt, enter the IP address of the NTP server you want to use, and then press **Enter**.

Result*:* The system displays the following message on the console:

```
Successfully synchronized with NTP server
Current Date/Time Setting:
        Time Zone: XXX
    Date & Time:
    NTP servers:
```

Setting the System Timeout

You can set a system timeout. This is the number of minutes with no activity on the serial console that can pass before the console login times out. To set the Cisco Secure ACS Appliance system timeout, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 At the system prompt, type **set timeout** followed by a single space and the timeout period in minutes.

Step 3 Press **Enter**.

Result*:* The system sets the new timeout period.

Setting the Appliance System Domain

You can set the system DNS domain from the serial console. To set the Cisco Secure ACS Appliance system domain, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 At the system prompt, type **set domain** followed by a single space and the domain name.

Step 3 Press **Enter**.

Result: The system displays the following confirmation message:

```
You should reboot appliance for the change to take effect.
```

Setting the Appliance System Hostname

Caution Performing this procedure stops and restarts all services and will interrupt use of the Cisco Secure ACS Appliance.

You can set the system hostname. To set the Cisco Secure ACS Appliance system hostname, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 2 At the system prompt, type **set hostname** followed by a single space and the hostname.

Tip You can use up to 15 letters and numbers but no spaces.

Step 3 Press **Enter**.

Result: The system restarts all services and the hostname is reset.

Upgrading the Appliance

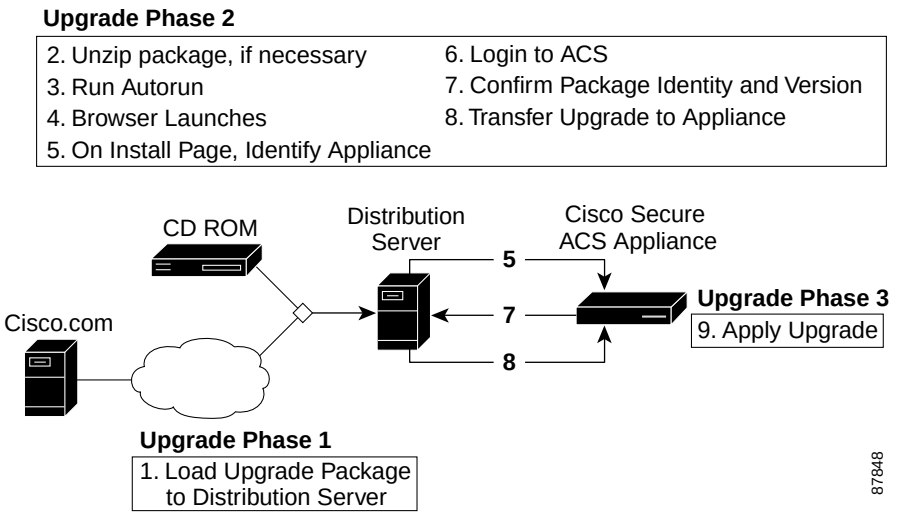
This section describes how to load and install a Cisco Secure ACS Appliance upgrade image from the command line interface of the serial console.

Upgrading the Cisco Secure ACS Appliance typically involves the following three steps:

1. Obtain the upgrade package from Cisco Systems and load it onto a distribution server in your network. This can be done either by employing an upgrade CD or downloading the upgrade package from Cisco.com.
2. Load the upgrade image onto the Cisco Secure ACS Appliance from the distribution server on your network. You can do this either from within the HTML interface, or from the serial console. The Cisco Secure ACS Appliance verifies the files transferred to ensure that they have not been corrupted. For more information on performing this step from the HTML interface, see the *User Guide for Cisco Secure ACS Appliance*. To load the upgrade image using the command line interface, use the following procedure: Upgrading the Appliance, page 4-32.
3. Finally, apply the Cisco Secure ACS Appliance system upgrade. You can do this either from within the HTML interface, or from the serial console. For more information, see Applying an Appliance System Upgrade, page 4-35.

This process is shown in Figure 4-1.

Figure 4-1 Appliance Upgrade Process



Transferring an Upgrade Package to the Appliance via Serial Console

Use this procedure to transfer an upgrade package from a distribution server to a Cisco Secure ACS Appliance.

Before you begin

You must have acquired the upgrade package and selected a distribution server. For more information, see Upgrading the Appliance, page 4-32.

Note This procedure is typically performed from within the HTML interface. For more information, see the *User Guide for Cisco Secure ACS Appliance*.

To transfer an upgrade to your Cisco Secure ACS appliance, follow these steps:

Step 1 If the distribution server uses Microsoft Windows, follow these steps:

a. If you have acquired the upgrade package on CD, insert the CD in a CD ROM drive on the distribution server.

Tip You can also use a shared CD drive on a different computer. If you do so and autorun is enabled on the shared CD drive, the HTTP server included in the upgrade package runs on the other computer, not the distribution server.

b. If either of the following conditions are true:

- You have acquired the upgrade package as a compressed file.
- Autorun is not enabled on the CD ROM drive.

locate the autorun.bat file on the CD or in the directory that you extracted the compressed upgrade package in and run it.

Result: The HTTP server starts.

Step 2 If the distribution server uses Sun Solaris, follow these steps:

a. If you have acquired the upgrade package on CD, insert the CD in a CD ROM drive on the distribution server.

b. Locate the autorun.sh file on the CD or in the directory that you extracted the compressed upgrade package in.

c. Run **autorun.sh**.

Result: The HTTP server starts. Messages from autorun.sh appear in a console window. Two web browser windows appear. The browser window titled Appliance Upgrade contains the Enter appliance hostname or IP address box. The browser window titled New Desktop contains buttons labeled Install Next and Stop Distribution Server. You can use the New Desktop window to start transfers to other appliances.

Step 3 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Step 4 At the system prompt, type **download** followed by the IP address of the distribution server.

Step 5 Press **Enter**.

Result: The system displays a number of messages including, finally, the following confirmation message:

```
Successfully downloaded the package. Run upgrade command to install
the package.
```

Applying an Appliance System Upgrade

You use this procedure to install upgrades on the Cisco Secure ACS Appliance. Upgrades may include the installation of a full software revision or simply the installation of a software patch.

Before you begin

You must have an upgrade to install. For information on checking the availability of and obtaining an upgrade, see the *User Guide for Cisco Secure ACS Appliance*. For information on how to load the upgrade package onto the Cisco Secure ACS Appliance see, Transferring an Upgrade Package to the Appliance via Serial Console, page 4-34.

Also, because the Cisco Secure ACS Appliance is non-operational during the upgrade process, you may want to schedule the upgrade for a time when its absence online will have the least impact.

To apply a Cisco Secure ACS Appliance system upgrade, follow these steps:

Step 1 Log on to the Cisco Secure ACS Appliance. For more information, see Logging On to the Appliance via Serial Console, page 4-2.

Caution The Cisco Secure ACS Appliance will be non-operational during the upgrade process.

Step 2 At the system prompt, type **upgrade**.

Step 3 Press **Enter**.

Result: The system displays a series of messages that include:

```
---Extracting---
---Verifying . . .---
```

Tip If there is no upgrade package loaded on the Cisco Secure ACS Appliance, you will see a message that requests that you download an upgrade package.

Step 4 Depending on your certification authority settings, you may see a warning message similar to the following:

```
Upgrade package was not verified
Applying this upgrade package may corrupt the appliance
Continue at your own risk!
Continue ---y(yes), n(no)
```

If you do see this prompt, type **y** to continue.

Result: The system displays a series of messages that may include:

```
Installing Cisco Secure ACS Version: x.x.x
Upgrading . . .

ACS Installation was successful
Successfully upgraded Cisco Secure ACS Version x.x.x
Completed upgrade and system will be rebooted.
```

Note During this installation of the upgrade, the system reboots twice. Therefore, when the system displays the following message:

```
Reboot will occur in a few minutes.

Login:
```

Continue to wait until you see the final message:

```
Status: Appliance is functioning normally.
```

This message indicates that the upgrade is complete.

Tip To obtain system information, including the current version, see Determining the Status of Appliance System and Services via Serial Console, page 4-4.

Patch Rollback

Removing Installed Patches

Use this procedure to uninstall one or more patches and to roll back the Cisco Secure ACS Appliance to the version that existed before the patch installation.

To roll back a Cisco Secure ACS Appliance system patch, follow these steps:

Step 1 Connect a console to the Cisco Secure ACS Appliance console port. For the location of the console port, see Figure 1-3 on page 1-5.

Step 2 Type **rollback** and the name of the patch application that you want rolled back. Then press **Enter**.

Tip If you do not include the specific patch application name as a parameter following the **rollback** command, the system displays the list of patches that can be rolled back. Use this list to identify the patch application name, type **rollback** followed by the patch application name, and then press **Enter**.

Result: The system displays a series of messages that include:

```
Rolling patch back
Rollback process initiated successfully
Successfully rolled back '[patch name]' to 0.
```

Tip To obtain system information, including the current version, see Determining the Status of Appliance System and Services via Serial Console, page 4-4.

Recovery Management

Cisco Secure ACS Appliance functionality includes two procedures that the administrator can perform using the Cisco Secure ACS Appliance Recovery CD ROM. These procedures, detailed in this section, include the following:

- Recovering from Loss of Administrator Credentials, page 4-38
- Re-Imaging the Appliance Hard Drive, page 4-40

Recovering from Loss of Administrator Credentials

If you cannot log on to the system because you have lost the account name or password for the Cisco Secure ACS Appliance administrator account, perform this procedure. In this procedure you use the Cisco Secure ACS Appliance Recovery CD ROM to access the system via the serial console and reset the administrator login credentials.

You should understand the following regarding the Cisco Secure ACS Appliance administrator login credentials:

- There is only one set of administrator login credentials at one time.
- Administrator login credentials are set (that is, changed from the default) during initial configuration.
- Administrator login credentials may be reset. For more information, see Resetting the Appliance Administrator Password, page 4-24.
- This recovery procedure entails replacing the administrator login credentials with a new account name and password.

To reset the administrator login credentials, follow these steps:

Step 1 Connect a console to the Cisco Secure ACS Appliance console port. For the location of the console port, see Figure 1-3 on page 1-5.

Step 2 Power on the console.

Step 3 Place the Cisco Secure ACS Appliance Recovery CD ROM into the appliance CD ROM drive.

Step 4 Power on the Cisco Secure ACS Appliance. (Or if already running, reboot the appliance. For more information, see Rebooting the Appliance via Serial Console, page 4-4.)

Result: The system displays the following message on the console:

```
ACS Appliance Recovery Options
[1] Reset administrator account
[2] Restore hard disk image from CD
[3] Exit and reboot
Enter menu item number: [ ]
```

Step 5 Type **1**.

Result: The system displays the following prompt:

```
Hit the Return key to log in.
```

Step 6 Type **Y**.

Result: The system displays the following prompt:

```
Please remove this recovery CD from the drive,
then hit RETURN to restart the system:
```

Step 7 Remove the recovery CD from the drive, and then press **Enter**.

Result: The system reboots, and then displays the system version information followed by:

```
Status: The appliance is functioning properly
Login:
```

Step 8 Type **Administrator**, and then press **Enter**.

Note The password is case sensitive.

Step 9 At the `password` prompt, type **setup**, and then press **Enter**.

Result: The system displays the system prompt.

Step 10 At the `Enter new account name:` prompt, type the name of the Cisco Secure ACS Appliance administrator, and then press **Enter**.

Step 11 At the `Enter new password:` prompt, type the new Cisco Secure ACS Appliance password, and then press **Enter**.

Note The new password must contain a minimum of 6 characters, and it must include a mix of at least 3 character types (numerals, special characters, upper case letters, and lower case letters). Each of the following examples is acceptable: 1PaSsWoRd, *password44, Pass*word.

Step 12 At the `Enter new password again:` prompt, type the new Cisco Secure ACS Appliance password, and then press **Enter**.

Result: The system displays the following message on the console:

```
Password is set successfully.
```

Re-Imaging the Appliance Hard Drive

Use the Cisco Secure ACS Appliance Recovery CD ROM to re-image the Cisco Secure ACS Appliance if necessary. This will destroy all data and install a new image.

To re-image your Cisco Secure ACS Appliance, follow these steps:

Caution Performing this procedure destroys all data stored on the Cisco Secure ACS Appliance.

Step 1 Connect a console to the Cisco Secure ACS Appliance console port. For the location of the console port, see Figure 1-3 on page 1-5.

Step 2 Put the Recovery CD in the Cisco Secure ACS Appliance CD-ROM drive. For the location of the CD-ROM drive, see Figure 1-2 on page 1-4.

Step 3 Power on the Cisco Secure ACS Appliance. (Or if the appliance is already running, reboot it. For more information, see Rebooting the Appliance via Serial Console, page 4-4.

Result: The Cisco Secure ACS Appliance displays the following message on the console:

```
ACS Appliance Recovery Options
[1] Reset administrator account
[2] Restore hard disk image from CD
[3] Exit and reboot
Enter menu item number: [ ]
```

Step 4 Type **2**, and then press **Enter**.

Result: The Cisco Secure ACS Appliance displays the following message on the console:

```
This operation will completely erase the hard drive. Press 'Y' to
confirm, any other key to cancel: __
```

Caution The next step erases the Cisco Secure ACS Appliance hard drive. You will permanently lose all system data that you have not backed up.

Step 5 Type **Y**.

Result: The Cisco Secure ACS Appliance processes the new image (this may take more than 2 minutes) while displaying odd characters and then displays the following message on the console:

```
The system has been reimaged successfully. Please remove this recovery
CD from the drive, then hit RETURN to restart the system:
```

Step 6 Remove the Recovery CD from the Cisco Secure ACS Appliance.

Step 7 Press **Enter** to restart the Cisco Secure ACS Appliance.

Result: The Cisco Secure ACS Appliance reboots, performs some configurations, and reboots again. The configurations that occur after the first reboot take a significant amount of time, during which there is no feedback; this is normal system behavior.

Note After re-imaging the appliance hard drive, you must once again perform initial configuration of the Cisco Secure ACS Appliance. For detailed instructions, see Configuring the Cisco Secure ACS Appliance, page 3-15.

Technical Specifications

Table A-1 provides the technical specifications of the Cisco Secure ACS Appliance 3.2.

Table A-1 Cisco Secure ACS Appliance Technical Specifications

Component	Specifications
Height	4.19 cm (1.65 inches)
Width	42.55 cm (16.75 inches)
Depth	65.45 cm (25.75 inches)
Weight	10 kg (26 lb) maximum
Rated input voltage	100 VAC to 240 VAC
Rated input frequency	50 Hz to 60 Hz
Rated input current	2.8 A (110 V) to 1.4 A (220 V)
Rated input power	307 W
BTUs per hour	1048
Power supply output: steady state	180 W
Power supply output: maximum peak power	200 W
Operating temperature range (see note*)	10°C to 35°C (50°F to 95°F)

Table A-1 Cisco Secure ACS Appliance Technical Specifications (continued)

Component	Specifications
Shipping temperature range (see note*)	-40° to 70°C (-40° to 158°F)
Operating relative humidity	10% to 90% (noncondensing)
Non-operating relative humidity	5% to 95% (noncondensing)
Maximum wet bulb temperature	28°C (82.4°F)
Processor	Intel Pentium 4 - 3.06-GHz
Cache Memory	512-KB level 2 ECC cache
Memory	Two 512-MB DIMMs (PC2100 Registered ECC DDR SDRAM)
Network Controller	Two - 10/100/1000 NC7760 Ethernet NICs. (Only one operational at a given time.)
Storage Controller	Integrated dual channel ultra ATA/100 adapter with integrated ATA RAID 0, 1
Hard Drive	40-GB ATA/100 7,200 rpm
System battery	HP 540-milliampere-hour lithium 3V
Chipset	ServerWorks GC-SL chipset with 533-MHz Front side bus
CD-ROM	24x IDE (ATAPI)

*Operating temperature has an altitude derating of 1°C per 304.8 M (1,000 ft). No direct sunlight. Storage maximum humidity of 95% is based on a maximum temperature of 45°C. Altitude minimum for storage is 70 KPa.

Windows Service Advisement

The operating system for the Cisco Secure ACS Appliance v3.2 is a customized and minimized version of the Windows 2000 operating system. The Cisco Secure ACS Appliance removes all extraneous services, blocks all unused ports, and otherwise prevents all other access to the Cisco Secure ACS server system, thereby dramatically increasing the security posture of Cisco Secure ACS.

The following sections present details regarding the minimization of the operating system's services:

Services that are Run, page B-1

Services that Are Not Run, page B-3

Services that are Run

Table B-1 lists the services that are run on the Cisco Secure ACS Appliance.

Table B-1 Operating System Services Automatically Run by Cisco Secure ACS Appliance

Service Name	Description
COM+ Event System	Provides automatic distribution of events to subscribing COM components.
DHCP Client	Manages network configuration by registering and updating IP addresses and DNS names.

Table B-1 Operating System Services Automatically Run by Cisco Secure ACS Appliance (continued)

Service Name	Description
DNS Client	Resolves and caches Domain Name System (DNS) names.
Event Log	Logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in Event Viewer.
IPSEC Policy Agent	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.
License Logging Service	Tracks Client Access License usage for a server product.
Logical Disk Manager	Performs the Logical Disk Manager Watchdog Service.
Network Connections	Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.
Plug and Play	Manages device installation and configuration and notifies programs of device changes.
Protected Storage	Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes, or users.
Remote Procedure Call (RPC)	Provides the endpoint mapper and other miscellaneous RPC services.
Removable Storage	Manages removable media, drives, and libraries.
RunAs Service	Enables starting processes under alternate credentials.

Table B-1 Operating System Services Automatically Run by Cisco Secure ACS Appliance (continued)

Service Name	Description
Security Accounts Manager	Stores security information for local user accounts.
Server	Provides RPC support and file, print, and named pipe sharing.
System Event Notification	Tracks system events such as Windows logon, network, and power events. Notifies COM+ Event System subscribers of these events.
Telnet	Allows a remote user to log on to the system and run console programs using the command line.
Windows Management Instrumentation	Provides system management information.
Windows Management Instrumentation Driver Extensions	Provides systems management information to and from drivers.

Services that Are Not Run

Table B-2 lists the operating system services that are not run on the Cisco Secure ACS Appliance.

Table B-2 Disabled Operating System Services in Cisco Secure ACS Appliance

Service Name	Description
Alerter	Notifies selected users and computers of administrative alerts.
Application Management	Provides software installation services such as Assign, Publish, and Remove.

Table B-2 Disabled Operating System Services in Cisco Secure ACS Appliance (continued)

Service Name	Description
Automatic Updates	Enables the download and installation of critical Windows updates. If the service is disabled, the operating system can be manually updated at the Windows Update Web site.
Background Intelligent Transfer Service	Transfers files in the background using idle network bandwidth. If the service is stopped, features such as Windows Update, and MSN Explorer will be unable to automatically download programs and other information. If this service is disabled, any services
ClipBook	Supports ClipBook Viewer, which allows pages to be seen by remote ClipBooks.
Computer Browser	Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.
Distributed File System	Manages logical volumes distributed across a local or wide area network.
Distributed Link Tracking Client	Sends notifications of files moving between NTFS volumes in a network domain.
Distributed Link Tracking Server	Stores information so that files moved between volumes can be tracked for each volume in the domain.
Distributed Transaction Coordinator	Coordinates transactions that are distributed across two or more databases, message queues, file systems, or other transaction protected resource managers.
Fax Service	Helps you send and receive faxes.

Table B-2 Disabled Operating System Services in Cisco Secure ACS Appliance (continued)

Service Name	Description
File Replication	Maintains file synchronization of file directory contents among multiple servers.
Indexing Service	Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.
Internet Connection Sharing	Provides network address translation, addressing, and name resolution services for all computers on your home network through a dial-up connection.
Intersite Messaging	Allows sending and receiving messages between Windows Advanced Server sites.
Kerberos Key Distribution Center	Generates session keys and grants service tickets for mutual client/server authentication.
Logical Disk Manager Administrative Service	Performs administrative service for disk management requests.
Messenger	Sends and receives messages transmitted by administrators or by the Alerter service.
Net Logon	Supports pass-through authentication of account logon events for computers in a domain.
NetMeeting Remote Desktop Sharing	Allows authorized people to remotely access your Windows desktop using NetMeeting.
Network DDE	Provides network transport and security for dynamic data exchange (DDE).
Network DDE DSDM	Manages shared dynamic data exchange and is used by Network DDE

Table B-2 Disabled Operating System Services in Cisco Secure ACS Appliance (continued)

Service Name	Description
NT LM Security Support Provider	Provides security to remote procedure call (RPC) programs that use transports other than named pipes.
Performance Logs and Alerts	Configures performance logs and alerts.
Print Spooler	Loads files to memory for later printing.
QoS RSVP	Provides network signaling and local traffic control setup functionality for QoS-aware programs and control applets.
Remote Access Auto Connection Manager	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.
Remote Access Connection Manager	Creates a network connection.
Remote Procedure Call (RPC) Locator	Manages the RPC name service database.
Remote Registry Service	Allows remote Registry manipulation.
Routing and Remote Access	Offers routing services to businesses in local area and wide area network environments.
Smart Card	Manages and controls access to a smart card inserted into a smart card reader attached to the computer.
Smart Card Helper	Provides support for legacy smart card readers attached to the computer.
Task Scheduler	Enables a program to run at a designated time.
TCP/IP NetBIOS Helper Service	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.

Table B-2 Disabled Operating System Services in Cisco Secure ACS Appliance (continued)

Service Name	Description
Telephony API (TAPI)	Provides Telephony API (TAPI) support for programs that control telephony devices and IP-based voice connections on the local computer and, through the LAN, on servers that are also running the service.
Terminal Services	Provides a multi-session environment that allows client devices to access a virtual Windows 2000 Professional desktop session and Windows-based programs running on the server.
Uninterruptible Power Supply	Manages an uninterruptible power supply (UPS) connected to the computer.
Utility Manager	Starts and configures accessibility tools from one window
WMDM PMSP Service	—
Workstation	Provides network connections and communications.
Windows Installer	Installs, repairs and removes software according to instructions contained in .MSI files.
Windows Time	Sets the computer clock.

Command Reference

This appendix summarizes the command line interface (CLI) commands of the Cisco Secure ACS Appliance 3.2.

This appendix contains the following sections:

CLI Conventions

The command-line interface (CLI) uses the following conventions:

- The key combination **^c**, or **Ctrl-c**, means hold down the **Ctrl** key while you press the **c** key.
- A string is defined as a nonquoted set of characters.

Do not confuse the Cisco Secure ACS Appliance CLI with the IOS CLI. Though they are similar, they are not identical.

Command Privileges

Access to CLI commands on the Cisco Secure ACS Appliance is limited to those who physically connect via the console port and who possess the proper administrative credentials.

For more information about establishing the console connection, see Establishing a Serial Console Connection, page 3-14.

Checking Command Syntax

The serial console interface provides several types of responses to incorrect command entries:

- If you enter a command line that does not contain any valid commands, the system displays `Command not found.`
- If you enter a valid command but omit required options, the system displays `Incomplete command.`
- If you enter a valid command but provide invalid options or parameters, the system displays `Invalid input.`

In addition, some commands have command-specific error messages that notify you that a command is valid, but that it cannot run correctly.

System Help

You can obtain help using the following methods:

- For a list of all commands and their syntax, enter **help**, and then press **Enter**.
- For help on a specific command, type the command name, a space, and a question mark, and then press **Enter**, for example, **show?**. The help contains command usage information and syntax.

Command Summary

Table C-1 summarizes all commands available on the Cisco Secure ACS Appliance. Refer to the full description of commands that you are not familiar with before using them.

Table C-1 Command Summary

Command	Summary Description	Location of Full Description
backup	Backup ACS data to an FTP serve.	backup, page C-5
dbcompact	Compact database by dumping, initializing database, and loading database from dump file.	dbcompact, page C-6
download	Download ACS Install Package.	download, page C-6
exit	Logout the session.	exit, page C-7
exportgroups	Send a list of groups to an FTP server.	exportgroups, page C-7
exportlogs	List and send selected logs to an FTP server.	exportlogs, page C-8
exportusers	Send a list of users, by group, to an FTP server.	exportusers, page C-9
help	List description of commands.	help, page C-10
ping	Sends Internet Control Message Protocol (ICMP) echo_request packets for diagnosing basic network connectivity.	ping, page C-10
reboot	Soft reboot appliance.	reboot, page C-11
restart	Restart ACS services.	restart, page C-12
restore	Restore Appliance.	restore, page C-13
rollback	Rollback patched appliance.	rollback, page C-13
set admin	Set administrator's name.	set admin, page C-14
set domain	Set appliance’s DNS domain.	set domain, page C-15
set hostname	Set appliance’s hostname.	set hostname, page C-15
set ip	Set appliance’s IP configuration.	set ip, page C-16
set password	Set administrator’s password.	set password, page C-16

Table C-1 Command Summary (continued)

Command	Summary Description	Location of Full Description
set time	Set the time zone, date, and time information.	set time, page C-17
set timeout	Set the timeout for serial console with no activity.	set timeout, page C-17
show	Show version of appliance and ACS, system load status, ACS service status, IP configuration, appliance's hostname and DNS domain.	show, page C-18
shutdown	Shut down appliance.	shutdown, page C-18
start	Start ACS services.	start, page C-19
stop	Stop ACS services.	stop, page C-19
support	This command runs CSSupportCL.exe program. The CSSupportCL.exe performs almost exactly the same functionality as the GUI-based Support page. That is, it will collect a set of logs and Registry and other useful information, and compress this into a single cab file that can then be analyzed for support purposes.	support, page C-20
tracert	Display the network route to a specified host and identify faulty gateways.	tracert, page C-21
upgrade	Perform the second stage of upgrade.	upgrade, page C-22

Command Description Conventions

Command descriptions in this document and in the CLI help system use the following conventions:

- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate optional elements.

- Braces ({ }) indicate a required choice. Braces within square brackets ([{ }]) indicate a required choice within an optional element.
- Bold indicates commands and keywords that are entered literally as shown.
- Italics indicate arguments for which you supply values.

Commands

This section describes the Cisco Secure ACS Appliance commands. Command names are case insensitive.

backup

To backup ACS data to an FTP server, use the **backup** command.

backup [*server*] [*username*] [*filepath*]

Syntax Description

server	Hostname for the FTP server to which the file will be sent.
username	User account name used to authenticate the FTP session.
filepath	Location under the FTP root for the server into which the backup will be sent.

Usage Guidelines

If you do not enter the parameters, the system prompts you for the information. Also you are prompted to encrypt the backup. If you indicate you want to encrypt the data, you are prompted for an encryption password. For more information, see Backing Up ACS Data via the Serial Console, page 4-18.

Example

The following command employs the user account *joeadmin* to backup the ACS data to the *backupdata* folder on the *onyx* FTP server:

```
backup onyx joeadmin backupdata
```

dbcompact

To compact the database by dumping, initializing the database, and loading the database from the dump file, use the **dbcompact** command.

Note The CSAuth service is temporarily halted while this command executes. This interrupts any user authentication.

dbcompact

Syntax Description

This command has no arguments or keywords.

Example

The following command compacts the database by dumping, initializing the database, and loading the database from the dump:

```
dbcompact
```

download

To download an upgrade image to the Cisco Secure ACS Appliance use the **download** command. Executing the **download** command establishes contact with the system specified, retrieves the manifest file from that system, and automatically downloads the upgrade image to the Cisco Secure ACS Appliance.

download [*hostAddress*]

Syntax Description

hostAddress	The IP address from which the image will be sent

Usage Guidelines

This command is generally executed from within the HTML interface. After loading an upgrade image by executing the download command, you need to install the image by using the upgrade command. For more information see Upgrading the Appliance, page 4-32.

Example

The following command downloads an upgrade image from the system with the address 10.51.256.256

```
dbcompact 10.51.256.256
```

exit

To log out of the system, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Example

The following command logs you out of the system:

```
exit
```

exportgroups

To export a list of user groups, use the **exportgroups** command.

exportgroups [*server*] [*username*] [*filepath*]

Note The CSAuth service is temporarily halted while this command executes. This interrupts any user authentication.

Syntax Description

server	Hostname for the FTP server to which the file will be sent.
username	User account name used to authenticate the FTP session.
filepath	Location under the FTP root for the server into which the group list will be sent.

Usage Guidelines

If you do not enter the parameters, the system prompts you for the information.

Example

The following command employs the user account *joeadmin* to send a list of user groups to the *groupdata* folder on the *diamond* FTP server:

```
exportgroups diamond joeadmin groupdata
```

exportlogs

To list and send selected logs to an FTP server, use the **exportlog** command.

exportlogs [*filename*] [*filename*]

Syntax Description

filename	Name of the file to be exported.

Usage Guidelines

This command lists all the log files that can be downloaded to an FTP server if no filenames are supplied. Otherwise, you can enter each filename with a space separating each filename. You are then prompted for the FTP server address, user login name, password, and the filepath for the file or files to be uploaded.

Example

The following command exports the log files mylog2002-01-31.csv and mylog2002-02-01.csv:

```
exportlog mylog2002-01-31.csv mylog2002-02-01.csv
```

exportusers

To export a list of users, use the **exportusers** command.

exportusers [*server*] [*username*] [*filepath*]

Note The CSAuth service is temporarily halted while this command executes. This interrupts any user authentication.

Syntax Description

server	Hostname for the FTP server to which the file will be sent.
username	User account name used to authenticate the FTP session.
filepath	Location under the FTP root for the server into which the users list will be sent.

Usage Guidelines

If you do not enter the parameters, the system prompts you for the information.

Example

The following command employs the user account *joeadmin* to send a list of users to the *userdata* folder on the *emerald* FTP server:

```
exportusers emerald joeadmin userdata
```

help

To list descriptions of commands, use the **help** command.

help

Syntax Description

This command has no arguments or keywords.

Example

The following command lists descriptions of commands:

```
help
```

ping

To send ICMP echo_request packets for diagnosing basic network connectivity, use the **ping** command.

ping [**-t**] [**-a**] [**-n** *count*] [**-l** *size*] [**-f**] [**-i** *TTL*] [**-v** *TOS*] [**-r** *count*] [**-s** *count*] [{**-j** *host-list*}|{**-k** *host-list*}] [**-w** *timeout*] *destination-list*

Syntax Description

-t	Ping the specified host until stopped. To see statistics and continue - type Control-Break. To stop - type Control-C.
-a	Resolve addresses to hostnames.
-n count	Number of echo requests to send.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet.
-i TTL	Time To Live.
-v TOS	Type Of Service.
-r count	Record route for count hops.

-s count	Timestamp for count hops.
-j host-list	Loose source route along host-list.
-k host-list	Strict source route along host-list.
-w timeout	Timeout in milliseconds to wait for each reply.

Examples

```
acsappl1> ping 10.19.253.228

Pinging 10.19.253.228 with 32 bytes of data:

Reply from 10.19.253.228: bytes=32 time=140ms TTL=120
Reply from 10.19.253.228: bytes=32 time=160ms TTL=120
Reply from 10.19.253.228: bytes=32 time=150ms TTL=120
Reply from 10.19.253.228: bytes=32 time=140ms TTL=120

Ping statistics for 10.19.253.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 140ms, Maximum =  160ms, Average =  147ms

acsappl1> ping -n 6 10.19.253.228

Pinging 10.19.253.228 with 32 bytes of data:

Reply from 10.19.253.228: bytes=32 time=130ms TTL=120
Reply from 10.19.253.228: bytes=32 time=140ms TTL=120
Reply from 10.19.253.228: bytes=32 time=140ms TTL=120
Reply from 10.19.253.228: bytes=32 time=140ms TTL=120
Reply from 10.19.253.228: bytes=32 time=130ms TTL=120
Reply from 10.19.253.228: bytes=32 time=130ms TTL=120

Ping statistics for 10.19.253.228:
    Packets: Sent = 6, Received = 6, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 130ms, Maximum =  140ms, Average =  135ms
```

reboot

To restart the Cisco Secure ACS Appliance, use the **reboot** command.

reboot

Note AAA services are temporarily halted while this command executes.

Syntax Description

This command has no arguments or keywords.

Example

The following command causes a soft reboot of the Cisco Secure ACS Appliance:

```
reboot
```

restart

To restart one or more of the ACS services, use the **restart** command.

restart [*service name(s)*]

Note AAA services are temporarily halted while this command executes.

Syntax Description

This command uses as an argument the name of the service or services to be restarted.

Usage Guidelines

Use the **restart** command to stop and restart any of the ACS services. You can determine the status of each service by using the show command. For more information, see Restarting Appliance Services via Serial Console, page 4-9.

Example

The following command restarts the CSAuth and CSAdmin services:

```
restart csauth csadmin
```

restore

To restore ACS data from an FTP server, use the **restore** command.

restore [*server*] [*username*] [*filepath*] [*filename*]

Syntax Description

server	Hostname for the FTP server from which the file will be sent.
username	User account name used to authenticate the FTP session.
filepath	Location under the FTP server root in which the restore file is located.
filename	Name of the restore file to be used.

Usage Guidelines

If you do not enter the parameters, the system prompts you for the information. Also, you will be prompted to enter a decrypt password; and you will be prompted to restore the user/group database and or the Cisco Secure ACS system configuration.

Example

The following command employs the user account *joeadmin* to retrieve a restore file, *allofit*, from the *restoredata* folder on the *topaz* FTP server:

```
restore topaz joeadmin restoredata allofit
```

rollback

To remove any patches and roll back to the originally installed version, use the **rollback** command.

rollback [*appName*]

Syntax Description

appName	Name of the program (provided as part of patch distribution) to remove a specific patch and roll back to original installed version.

Usage Guidelines

Use this command to return a Cisco Secure ACS to its original condition after having installed a patch program. The rollback command has the effect of stopping all ACS services, copying all files in the backup directory to the originally installed directories, restoring a specified list of Registry entries, and starting all ACS services once again.

Example

The following command executes the program *remvptch4* and returns the system to the state that existed before the patch program was applied:

```
rollback remvptch4
```

set admin

To set the name of the Cisco Secure ACS Appliance administrator, use the set admin command.

set admin [*administratorname*]

Syntax Description

administratorname	Name of system administrator.

Usage Guidelines

Use the **set admin** command to reset the name of the Cisco Secure ACS Appliance administrator. For more information, see Resetting the Appliance Administrator Password, page 4-24.

Example

This command sets the administrator name to john:

```
set admin john
```

set domain

To set the DNS domain of the Cisco Secure ACS Appliance, use the set domain command.

set domain [*domain-name*]

Syntax Description

domain-name	Name of DNS domain.

Example

This command sets the domain name to xyz.com:

```
set domain xyz.com
```

set hostname

To set the hostname of the Cisco Secure ACS Appliance, use the set hostname command.

set hostname [*hostname*]

Syntax Description

hostname	Name of the Cisco Secure ACS Appliance.

Example

This command sets the Cisco Secure ACS Appliance name to acs1:

```
set hostname acs1
```

set ip

To set the Cisco Secure ACS Appliance IP configuration, use the set ip command.

set ip

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use the **set ip** command to reset the system IP address in response to subsequent prompts. For more information, see Reconfiguring the Appliance IP Address, page 4-26.

Example

The following command begins the system IP address configuration.

```
set ip
```

set password

To set the Cisco Secure ACS Appliance administrator's password, use the **set password** command. Subsequent prompts take you through the process.

set password

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use the **set password** command to begin resetting the administrator's password. Subsequent prompts take you through the process. For more information, see Resetting the Appliance Administrator Password, page 4-24.

Example

The following command initiates the system ip setting procedure:

```
set password
```

set time

To set the Cisco Secure ACS Appliance time zone, NTP server, date, or time, use the **set time** command:

set time

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use the **set time** command to begin the setting of the timezone, current date, and current time. Subsequent prompts take you through the process. For more information, see Setting the System Time and Date Manually, page 4-28.

You can also use the **set time** command to enable an NTP server to synchronize the Cisco Secure ACS Appliance. For more information, see Setting the System Time and Date with NTP, page 4-29.

Example

The following command initiates the system time setting procedure:

```
set time
```

set timeout

To set the period, in minutes, after which the serial console will time out, use the **set timeout** command.

set timeout [*minutes*]

Syntax Description

This command has a single argument: the number of minutes before timing out. If you enter the command with no argument, the system prompts you for a value in minutes.

Example

The following command establishes a serial console timeout after10 minutes:

```
set timeout 10
```

show

To show the version of the Cisco Secure ACS Appliance, system load status, ACS service status, IP configuration, system time and NTP settings, Cisco Secure ACS Appliance hostname, DNS domain, and timeout value use the **show** command.

show

Syntax Description

This command has no arguments or keywords.

Example

The following command lists Cisco Secure ACS Appliance information:

```
show
```

shutdown

To shut down the appliance from the serial console, use the **shutdown** command.

shutdown

Syntax Description

This command has no arguments or keywords.

Example

The following command shuts down the appliance:

```
shutdown
```

start

To start one or more of the ACS services, use the start command.

start [*service name(s)*]

Syntax Description

This command uses as an argument the name of the service or services to be started.

Usage Guidelines

Use the **start** command to start any ACS service. You can determine the status of each service by using the show command. For more information, see Starting Appliance Services via Serial Console, page 4-7.

Example

The following command starts the CSAuth and CSadmin services:

```
restart csauth csadmin
```

stop

To stop one or more of the ACS services, use the **stop** command.

stop [*service name(s)*]

Note Services subject to this command are halted until restarted. This may interfere with AAA services.

Syntax Description

This command uses as an argument the name of the service or services to be stopped.

Usage Guidelines

Use the **stop** command to stop any ACS service. You can determine the status of each service by using the show command. For more information, see Stopping Appliance Services via Serial Console, page 4-6.

Example

The following command stops the CSAuth and CSAdmin services:

```
stop csauth csadmin
```

support

The **support** command collects a set of logs, Registry information, and other useful information that details activity. Executing the command compresses this set of logs into a single cab file, which can then be analyzed by support personnel.

To initiate the support program, use the **support** command.

support [**-d n**] **server filepath** [**username**]

Syntax Description

-d n	Collect the previous n days logs (up to 9999).
-u	Collect user database information.
server	The hostname for the FTP server to which the file is to be sent.
filepath	The location under the FTP root for the server into which the package.cab is to be sent.
username	The account used to authenticate the FTP session.

Note Unlike its counterpart in the HTML interface, this command restarts the Cisco Secure ACS services. This means that AAA services are interrupted.

Example

The following command packages logs from the past *3* days, together with user database information, and sends it to the FTP server on the machine *host*, as *diagdir/diag.cab* where the user will be prompted for the password to the *sammy* account on the FTP server:

```
support -d3 -u ftp://host/diagdir/diag.cab sammy
```

tracert

To display the network route to a specified host and identify faulty gateways, use the **tracert** command.

tracert [**-d**] [**-h** *maximum_hops*] [**-j** *host-list*] [**-w** *timeout*] *target_name*

Syntax Description

-d	Do not resolve addresses to hostnames.
-h *maximum_hops*	Maximum number of hops to search for target.
-j *host-list*	Loose source route along host-list.
-w *timeout*	Wait timeout milliseconds for each reply.

Example

```
acsappl1> tracert 10.19.253.228

Tracing route to 10.19.253.228 over a maximum of 30 hops

  1   <10 ms   <10 ms   <10 ms  champaign-gw1.cisco.com [171.69.180.1]
  2    40 ms    50 ms    60 ms  sjce-wan-gw1.cisco.com [171.69.8.17]
  3    40 ms    70 ms    70 ms  sjce-wbb-gw1.cisco.com [10.18.255.1]
  4    60 ms    70 ms    60 ms  sjce-rbb-gw1.cisco.com [171.69.7.233]
  5    71 ms    70 ms    60 ms  sjce-sbb1-gw1.cisco.com [171.69.14.34]
  6    80 ms    51 ms    70 ms  sjck-as-gw2.cisco.com [171.69.14.246]
  7    60 ms    90 ms    80 ms  sj-frame-1.cisco.com [171.70.192.54]
  8   150 ms   180 ms   161 ms  10.19.253.225
  9   141 ms   160 ms   170 ms  10.19.253.228
Trace complete.
```

upgrade

To perform the second stage of an upgrade, use the upgrade command.

upgrade

Note This command typically reboots the Cisco Secure ACS services. This means that AAA services are interrupted.

Syntax Description

This command has no arguments or keywords.

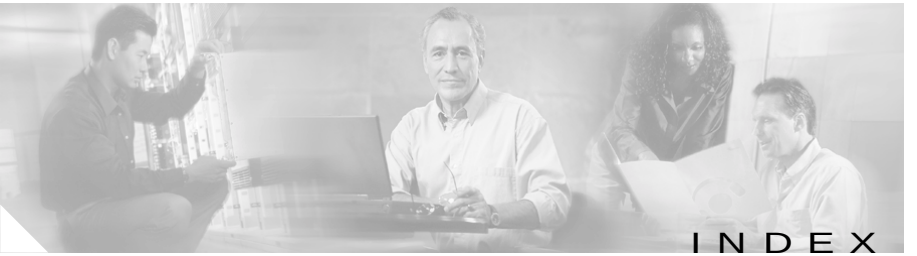
Usage Guidelines

Use the **upgrade** command to install an upgrade package that you have already loaded to the Cisco Secure ACS Appliance. For more information, see Upgrading the Appliance, page 4-32.

Example

The following initiates the second stage of an upgrade:

```
upgrade
```



A

B

C

D

E

F

H

I

L

O

P

R

S

T

U

W