Installation and Setup Guide for Cisco Secure ACS Solution Engine

Version 4.0
License and Warranty

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-7817249=
Text Part Number: 78-17249-02

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

Installation and Setup Guide for Cisco Secure ACS Solution Engine

INDEX

Preface

This guide describes how to install and initially configure the Cisco Secure ACS Solution Engine (ACS SE), and includes upgrade and migration information for both the HP and Quanta platforms. It also details administrative functions that you can perform from the command line interface. This guide covers two hardware platforms for the Cisco Secure ACS SE:

- the KD-1112 K9 platform—also referred to as the Quanta (1112) version
- the KD-1113 K9 platform—also referred to as the Quanta (1113) version

Audience

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

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

Organization

This guide contains the following chapters and appendixes:

- Preface
- Chapter 1, “Cisco Secure ACS Solution Engine Overview”
- Chapter 2, “Preparing for Installation”
- Chapter 3, “Installing and Configuring Cisco Secure ACS Solution Engine 4.0”
- Chapter 4, “Administering Cisco Secure ACS Solution Engine”
- Chapter 5, “Upgrading and Migrating to Cisco Secure ACS Solution Engine”
- Appendix A, “Technical Specifications for the Quanta (1112) Version”
- Appendix B, “Technical Specifications for the Quanta (1113) Version”
- Appendix C, “Windows Service Advisement”
- Appendix D, “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.

FONTOS BIZTONSÁGI ELOÍRÁSOK

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

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。

Documentation Updates

Table 1　Updates to Installation and Setup Guide for Cisco Secure ACS Solution Engine 4.0

Date	Description
12/16/2009	• Updated Solution Engine Specifications for the Quanta (1113) Version Platform • Updated the table ACS SE Technical Specifications for the Quanta (1113)

Product 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.

Table 2 describes the product documentation that is available.

Table 2 Product Documentation

Document Title	Available Formats
Documentation Guide for Cisco Secure ACS Solution Engine	• Printed document with the product. • PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-78-17336-01).[1]
Release Notes for Cisco Secure ACS Solution Engine	On Cisco.com.
Installation and Setup Guide for Cisco Secure ACS Solution Engine	• PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-78-17249-01).[1]
User Guide for Cisco Secure ACS Solution Engine	• PDF on the product CD-ROM. • On Cisco.com. • Printed document available by order (part number DOC-78-17345-01).[1]
Installation and User Guide for Cisco Secure ACS User-Changeable Passwords	• PDF on the product CD-ROM. • On Cisco.com.
Installation and Configuration Guide for Cisco Secure ACS Remote Agents	• PDF on the product CD-ROM. • On Cisco.com.
Regulatory Compliance and Safety Information for Cisco Secure ACS Solution Engine	• PDF on the product CD-ROM. • On Cisco.com.
Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine	On Cisco.com.
Recommended Resources for the Cisco Secure ACS User	On Cisco.com.

1. See Obtaining Documentation, page xix.

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.

A set of white papers about Cisco Secure ACS for Windows is available at the following URL:

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

Much of the information in these papers is applicable to Cisco Secure ACS Solution Engine.

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 at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

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

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation 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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

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

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tips We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request 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 list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing 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.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations 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.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—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.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *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 at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *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

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

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

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 78-5235-03B0 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	

Cisco Secure ACS Solution Engine Overview

System Description

Cisco Secure ACS Solution Engine (ACS SE) 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) and Terminal Access Controller Access Control System (TACACS+). ACS SE controls the authentication, authorization, and accounting (AAA) of users accessing corporate resources through the network.

You use ACS SE 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, you can use the same AAA framework, via TACACS+, to manage administrative roles and groups and to control how network administrators change, access, and configure the network internally.

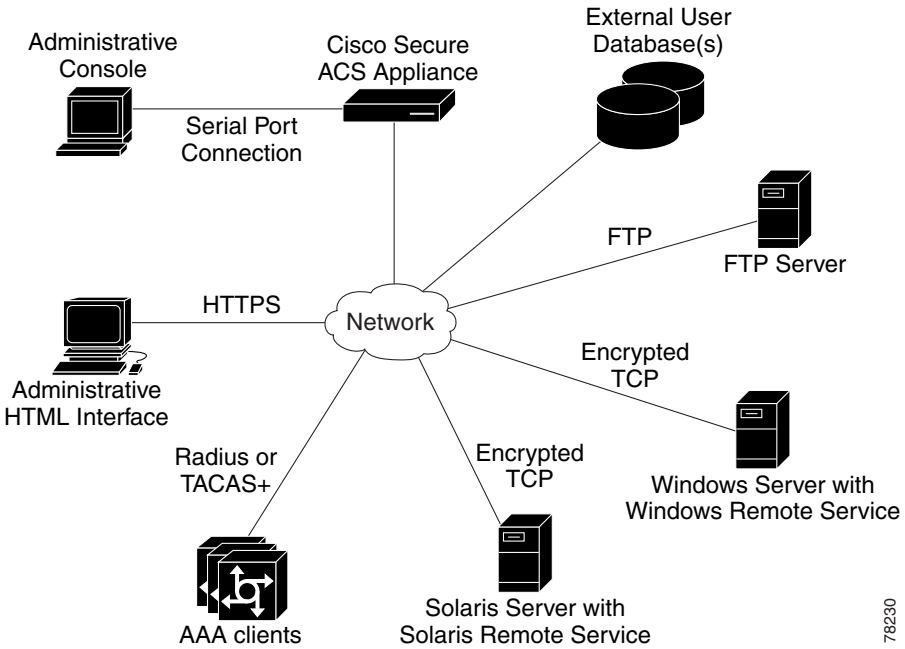
ACS SE provides almost the same set of features and functions as in the Cisco Secure ACS for Windows Server (the software product) in a dedicated, security hardened, application-specific, appliance packaging. ACS SE includes additional features specific to operating and managing the ACS appliance. See *Release Notes for Cisco Secure ACS Solution Engine* for the new features in this release.

To ensure a highly secure posture, ACS SE:

- Runs only the necessary services of the underlying hardened Windows operating system. (See Appendix C, "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 you to run arbitrary applications on it.
- Allows TCP/IP connections only via the ports necessary for its own operations.

Figure 1-1 shows the ACS SE operating context.

Figure 1-1 ACS SE Context Diagram



The administrative console 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 ACS SE features and capabilities, see the *User Guide for Cisco Secure ACS Solution Engine* and the *Release Notes for Cisco Secure ACS Solution Engine*.

ACS SE Hardware Description

ACS SE is a rack-mountable 1U box. The sections below describe the following hardware devices:

- Cisco Secure ACS 4.0.1 for Quanta (1112) version
- Cisco Secure ACS 4.0.1 for Quanta (1113) version

Solution Engine Specifications for the Quanta (1112) Version Platform

The ACS SE on the Quanta (1112) platform has the following specifications:

- 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.

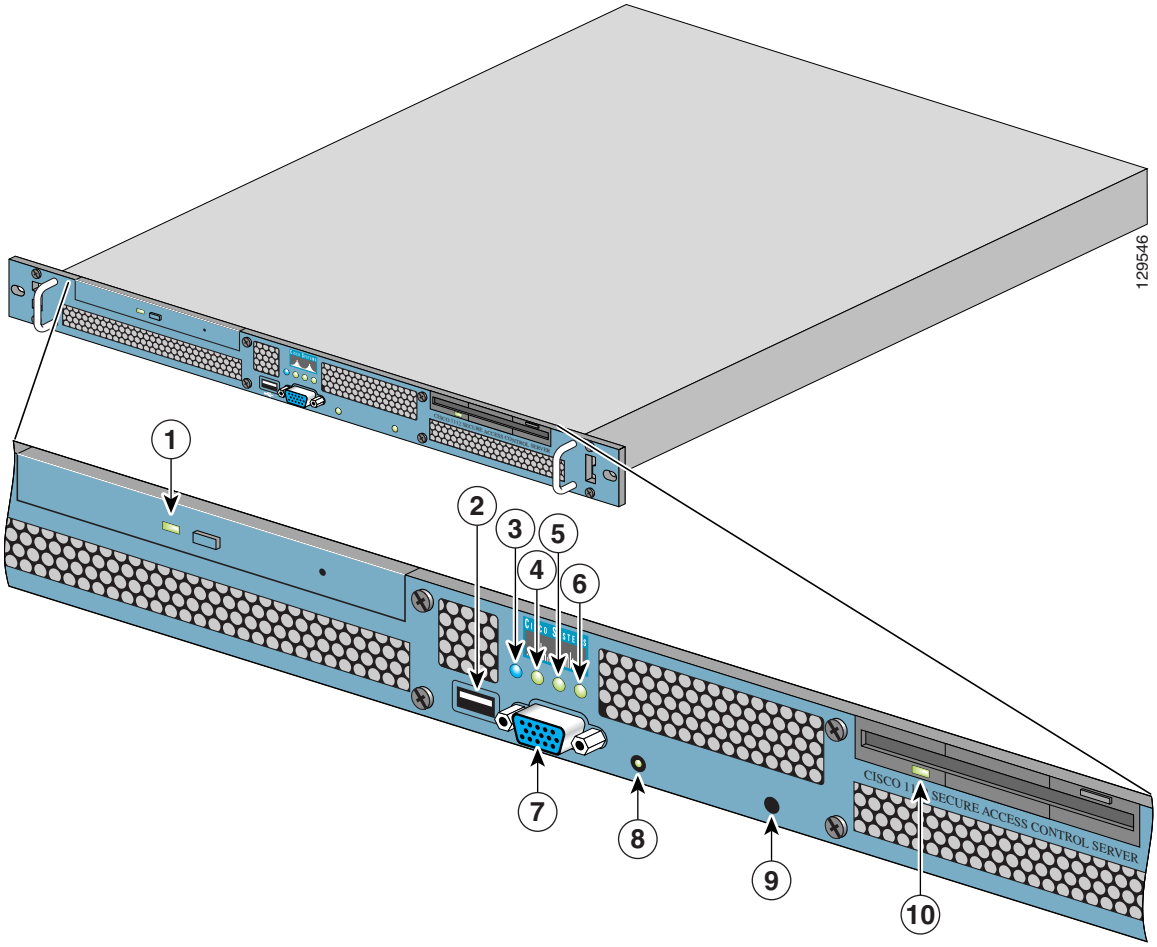
Technical specifications for the Quanta (1112) version are detailed in Appendix A, "Technical Specifications for the Quanta (1112) Version."

This section contains the following sections and subsections:

Front Panel Features for the Quanta (1112) Version

The ACS SE front panel on the Quanta (1112) version 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 the table below the illustration.

Figure 1-2 Front Panel Switches and Indicators



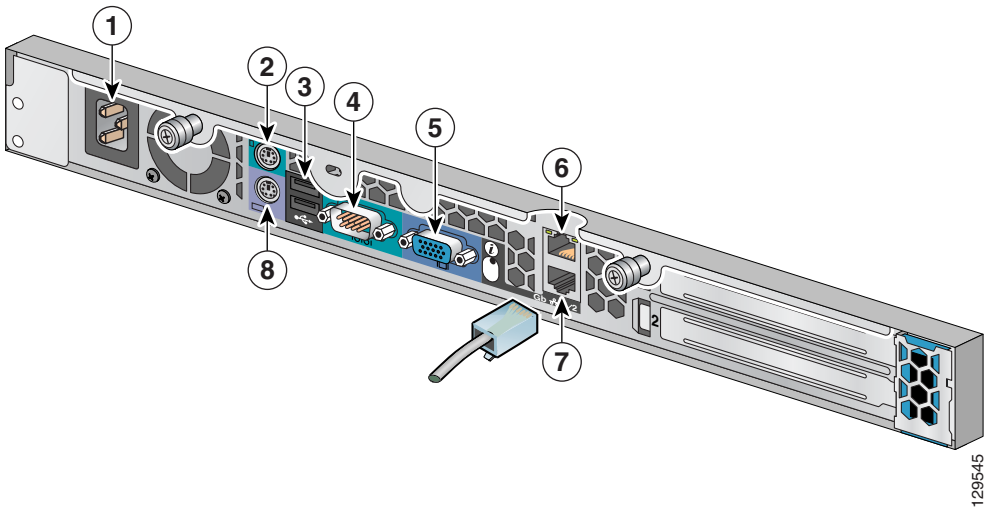
The following table describes the callouts in Figure 1-2.

No.	Switch or LED Indicator	Description
1	CD-ROM drive activity LED	On = Activity Off = No Activity
2	USB Connector (not supported)	Do not use.
3	Front unit identification LED	Glows blue after you switch on unit ID switch.
4	NIC 2 link/activity LED	On = Link Off = No Link Blinking = Activity
5	NIC 1 link/activity LED	On = Link Off = No Link Blinking = Activity
6	System health LED	Green = Good Amber = Degraded Red = Critical Error
7	Video connector (not supported)	Do not use.
8	Power On/Off LED	Blinking Green = Power is connected but not on Green = Power On Amber = Standby Mode Off = Power Off
9	Unit Identification Switch	When switched on, the Unit Identification LEDs on the front and back panels glow blue.
10	Floppy drive activity LED	On = Activity Off = No Activity

Back Panel Features for the Quanta (1112) Version

The back panel for the Quanta (1112) versions 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 for the Quanta (1112) Version



The following table describes the callouts in Figure 1-3.

No.	Description
1	AC power receptacle
2	Mouse connector (not supported). Do not use.
3	USB connector 1 (not supported). Do not use.
4	Serial connector (see Figure 1-4)
5	Video connector (not supported). Do not use.
6	RJ-45 Fast Ethernet connector with 10/100/1000-Mbit/s operation for NIC 2
7	RJ-45 Fast Ethernet connector with 10/100/1000-Mbit/s operation for NIC 1
8	Keyboard connector (not supported). Do not use.

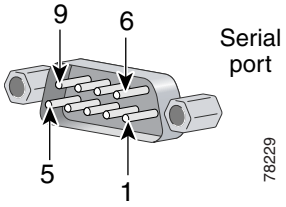
Serial Port

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
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. ACS SE 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 ACS SE 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).

Solution Engine Specifications for the Quanta (1113) Version Platform

The ACS SE on the Quanta (1113) platform has the following specifications:

- Intel Pentium 4 Prescott/Smithfield/Cedar Mill/Presler and Celeron D LGA775 CPU
- Broadcom 5721J Ethernet network interface card
- 80-GB or more ATA hard drive
- QSI DVD-ROM drive
- Serial port

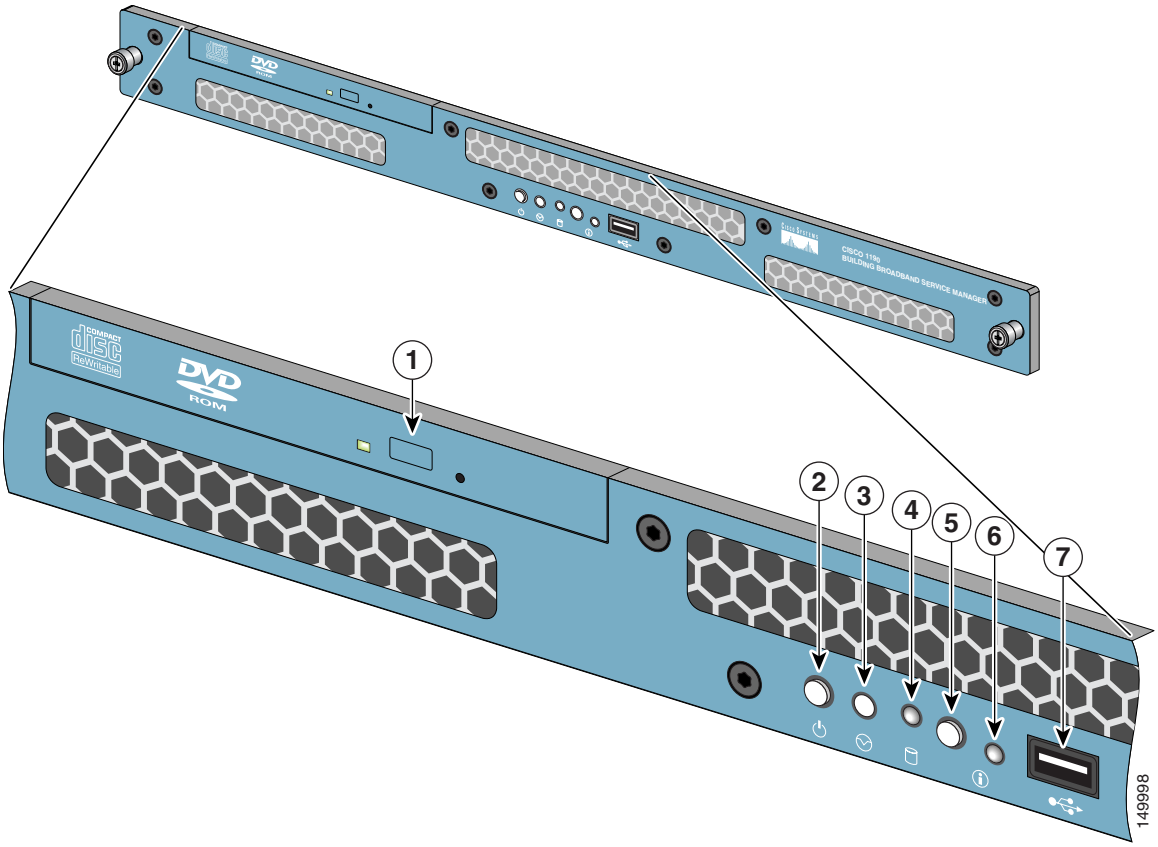
Technical specifications are detailed in Appendix B, “Technical Specifications for the Quanta (1113) Version.”

This section contains the following sections and subsections:

Front Panel Features for the Quanta (1113) Version

The ACS SE front panel on the Quanta (1113) version contains switches, indicators, and the CD-ROM drive. Figure 1-5 shows the front panel switches and LED indicators. The functions of the switches and LED indicators are described in the table below the illustration.

Figure 1-5 Front Panel Switches and Indicators for the Quanta (1113) Version



The following table describes the callouts in Figure 1-5.

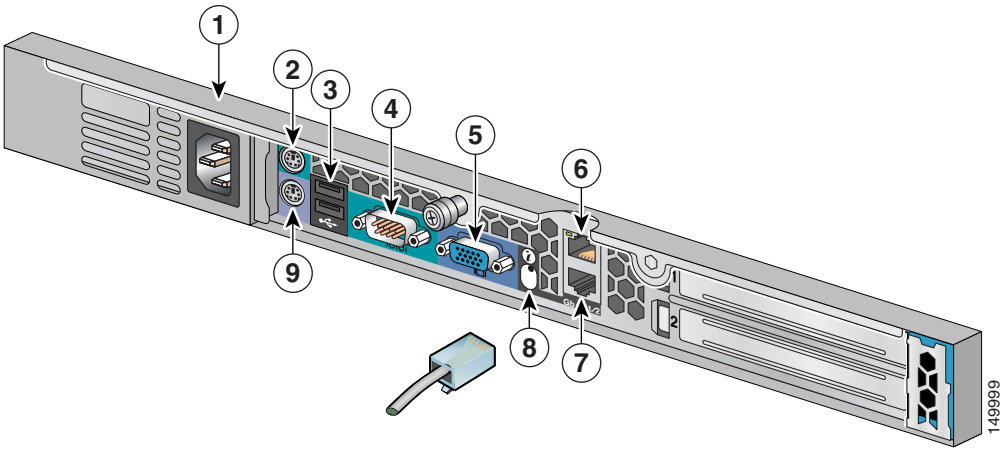
No.	Switch or LED Indicator	Description
1	DVD-ROM drive activity LED	On = Activity Off = No Activity
2	Power On/Off button and LED	Pushing the power button turns the unit on or off. The LED in the center of the power On/Off button has the following states: Blinking Green = Power is connected but not on Green = Power On Off = Power Off
3	Unused button	This button is not operational.
4	HDD LED	Indicates that there is activity on the hard drive.

No.	Switch or LED Indicator	Description
5	Unit Identification Button	To enable the Unit Identification LED, push the Unit Identification Button. When the Unit identification button is on, the Unit Identification LEDs on the front and back panels flash blue. This enables you to go behind the unit and look at the flashing blue light on the back You can turn off the flashing LED on the back of the unit off by pressing the Unit Identification button on the back panel. To turn off the Unit Identification LED, when the LED is on, push the Unit Identification Button.
6	Unit Identification LED	The Unit Identification LED has the following states: Off = System power is off, the system ID button has not been pushed, and there is no fault assertion condition (the system cover is on the device and there is no fault condition). Flashing Blue = When the system ID button is pushed, the Unit Identification LED flashes blue if the system is in either standby mode or system power is on. Solid Blue = System power is on, the system cover is on the device, and there is no fault assertion condition. The system ID button has not been pushed. Flashing Amber = The system is on standby power, there is a fault assertion condition (for example, the cover has been removed from the device), and the system ID button has not been pushed.
7	USB port (not supported)	Universal Serial Bus port. Do not use.

Back Panel Features for the Quanta (1113) Version

The back panel for the Quanta (1113) version contains the AC power receptacle, Ethernet connectors, indicator LEDs, and a serial port. Figure 1-6 shows the back-panel features.

Figure 1-6 Back Panel Features for the Quanta (1113) Version



The following table describes the callouts in Figure 1-6.

No.	Description
1	AC power receptacle
2	Mouse connector (not supported). Do not use.
3	USB connectors (not supported). Do not use.
4	Serial connector (see Figure 1-4)
5	Video connector (not supported). Do not use.
6	RJ-45 Fast Ethernet connector with 10/100/1000-Mbit/s operation for NIC 2
7	RJ-45 Fast Ethernet connector with 10/100/1000-Mbit/s operation for NIC 1
8	Unit Identification Button and LED. When the Unit Identification Button on the front panel is pressed, this causes the Unit Identification Button on the back panel to flash blue. To turn off the Unit Identification indicator on the back panel, push the Unit Identification button.
9	Keyboard connector

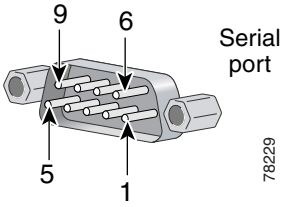
Serial Port

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 1-7 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 1-7 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
8	CTS	I	Clear to send
9	RI	I	Ring indicator
Shell	N/A	N/A	Chassis ground

Ethernet Connectors

Your Quanta (1113) system has two integrated 10/100/1000-megabit-per-second (Mbps) Ethernet connectors. ACS SE 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.

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 Solution Engine (ACS SE) 4.0, 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 ACS SE.

Note The English warnings in this document are followed by a statement number. To see the translations of a warning into other languages, look up its statement number in the *Regulatory Compliance and Safety Information for the Cisco Secure ACS Solution Engine*.

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. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Warning **Read the installation instructions before you connect the system to its power source.** Statement 10

Warning **The device is designed to work with TN power systems.** Statement 19

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units.** Statement 246

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 120 VAC, 15A (U.S./CAN); 240 VAC, 10A (INTERNATIONAL)** Statement 1005

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:**

- **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.** Statement 1006

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.** Statement 1015

Warning **This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security.** Statement 1017

Warning **The plug-socket combination must be accessible at all times, because it serves as the main disconnecting device.** Statement 1019

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.** Statement 1021

Warning **This equipment must be grounded. 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.** Statement 1024

Warning **This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.** Statement 1028

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.** Statement 1029

Warning **Only trained and qualified personnel should be allowed to install, replace, or service this equipment.** Statement 1030

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Warning **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

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 xxi, 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 no one will step on or trip over them. Be certain 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 and national wiring regulations.
- 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 occurs, 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 certain 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 ACS SE 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 ACS SE, 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.
- Observe power strip ratings. Ensure that the total ampere rating of all products plugged into the power strip does not exceed 80% of the rating.
- 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 regulations.

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 that 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, ensure that you 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 Bad plant wiring can result in radio frequency interference (RFI).

Note 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 that your site must meet for safe installation and operation of your ACS SE. Ensure that your site is properly prepared before beginning installation.

Environmental

When planning your site layout and equipment locations, remember 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 to isolate the cause of failures and prevent future problems.

Use the following precautions when planning the operating environment for your ACS SE:

- Always follow the ESD-prevention procedures described in Preventing EMI, page 2-5, to avoid damage to equipment. Damage from static discharge can cause immediate or intermittent equipment failure.
- Ensure 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. Ensure 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.**

For optimal installation, choose a site:

- With a dry, clean, well-ventilated and air-conditioned area.
- 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 ACS SE power requirements, see Appendix A, "Technical Specifications for the Quanta (1112) Version."

Warning **This product requires short-circuit (overcurrent) protection to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.**

Cabling

Use the cables in the accessory kit to connect the ACS SE 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 ACS SE to your network. For information detailing cable requirements, see Back Panel Features for the Quanta (1112) Version, page 1-4.

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.

Precautions for Products with Modems, Telecommunications, or Local Area Network Options

Observe the following guidelines when working with options:

- Do not connect or use a modem or telephone during a lighting storm. Electrical shock from lightning can result.
- Never connect or use a modem or telephone in a wet environment.
- Do not plug a modem or telephone cable into the Ethernet connector.
- Disconnect the modem cable before opening a product enclosure, touching or installing internal components, or touching an uninsulated modem cable or jack.
- Do not use a telephone line to report a gas leak while you are in the vicinity of the leak.

Required Tools and Equipment

You need the following tools and equipment to install the ACS SE:

- Number 2 Phillips-head screwdriver
- Tape measure and level
- Antistatic mat or antistatic foam
- ESD grounding strap

Installing and Configuring Cisco Secure ACS Solution Engine 4.0

This chapter describes how to install and initially configure Cisco Secure ACS Solution Engine (ACS SE) 4.0. It contains the following sections:

Note The details in this guide correspond to the KD-1112 K9 and the KD-1113 K9 platform only.

Installation Quick Reference

Table 3-1 provides a high-level overview of the installation and initial configuration process. Following installation and initial configuration, see the *User Guide for Cisco Secure ACS Solution Engine* for information on how to use a browser and the web interface to fully configure your ACS SE to provide the AAA services that you want from this installation.

Table 3-1 Quick Reference

Task	References
Use the rack mount kit to install the ACS SE in a rack.	Installing the Quanta (1112) ACS SE in a Rack, page 3-2 Installing the Quanta (1113) ACS SE in a Rack, page 3-13
Connect the ACS SE to an AC power source.	Connecting to the AC Power Source, page 3-21
Connect network and console cables.	Connecting Cables, page 3-22
Perform initial configuration of the ACS SE	Configuring ACS SE, page 3-23
Verify initial configuration	Verifying the Initial Configuration, page 3-27
Configure ACS SE to provide AAA services	Next Steps, page 3-27

Installing the Quanta (1112) ACS SE in a Rack

This section provides instructions for installing the ACS SE Quanta (1112) version in a rack. The rack must be properly secured to the floor, ceiling, or upper wall, and where applicable, to adjacent racks. The rack should be secured by using floor and wall fasteners, and bracing specified by industry standards.

Before installing the ACS SE in a rack, read Preparing Your Site for Installation, page 2-5, to familiarize yourself with the proper site and environmental conditions. Failure to read and follow these guidelines could lead to an unsuccessful installation and possible damage to the system and components.

When installing and servicing the ACS SE:

- 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, see 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 renders the equipment unsafe.

- Do not attempt to install the ACS SE in a rack that has not been securely anchored in place. Damage to the system and personal injury may result.
- Due to the size and weight of the computer system, never attempt to install the computer system by yourself.

See Precautions for Rack-Mounting, page 2-8, for additional safety information on rack installation.

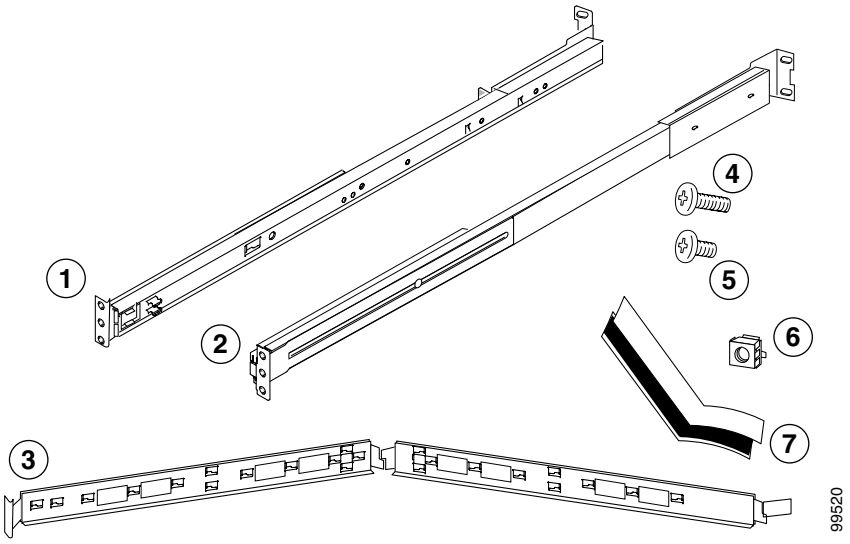
Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

- **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.** Statement 1006

The server can be installed in a system 1U rack. The rack rail components are (numbers in parentheses refer to Figure 3-1):

- 2 telescopic rails (1, 2)
- 1 cable management arm (3)
- Bag containing:
  - 9 Round head screws with washer (4)
  - 6 Round head screws (5)
  - 6 Cage nuts (6)
  - Velcro (7)

Figure 3-1 Rack Rail Components



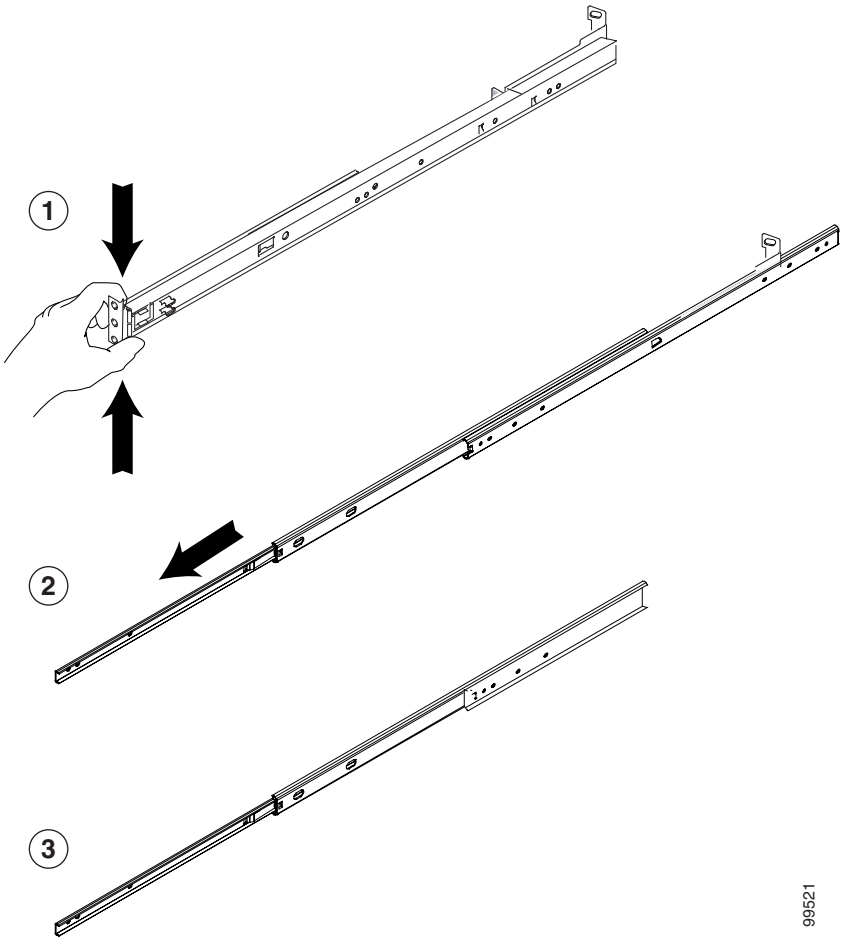
To install the Quanta (1112) ACS SE in a rack:

Step 1 Attach the telescopic rails to the rack assembly:

a. See Figure 3-2. Extend the server rail (1) as far as it will go.

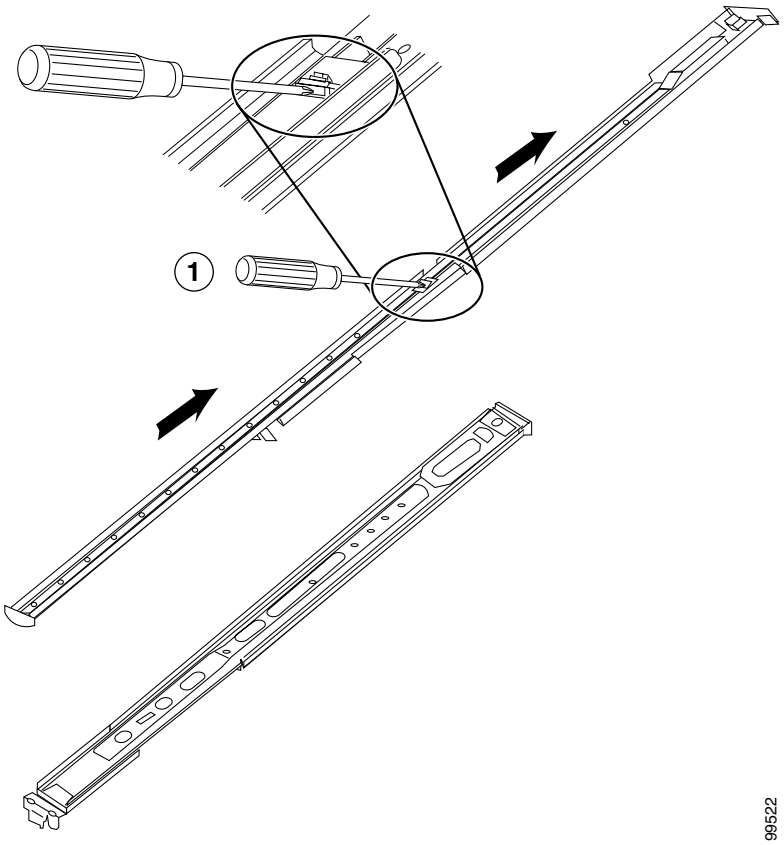
b. Press the green spring plate (2) and slide out that part of the server rail (1). (Set it aside for attaching to the chassis.)

Figure 3-2 Removing the Server Rail



c. See Figure 3-3. Using a screwdriver (1), push the middle rail to the end of the rail.

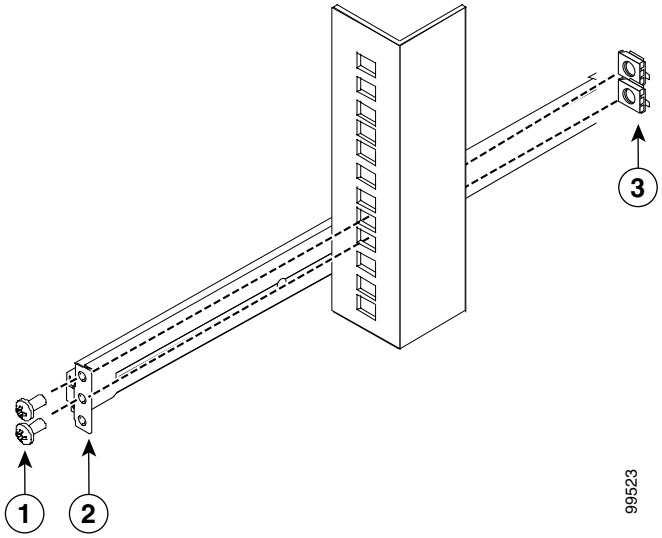
Figure 3-3 Telescoping the Rail



Note To allow for adjustment later in the installation, do not tighten any screws. The outer rail and bracket assembly with extended bracket (1) must be assembled to the left side.

d. See Figure 3-4. Attach the front end of the telescopic outside rail (1) to the rack.

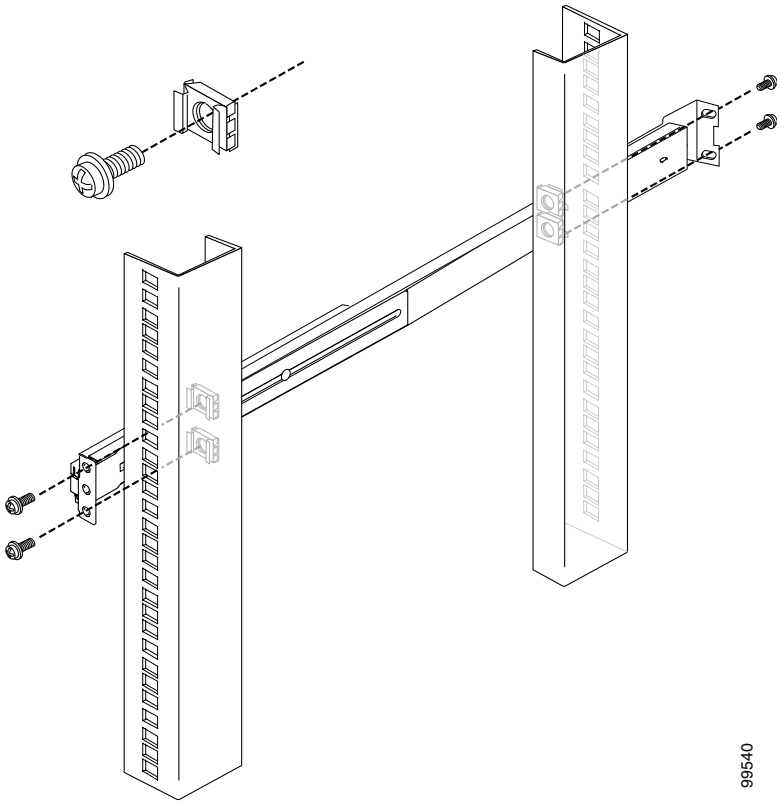
Figure 3-4 Attaching Front Rail to the Rack



Note The left side of the rail is for the cable arm.

e. See Figure 3-5. Attach the back end of the rail to the rack.

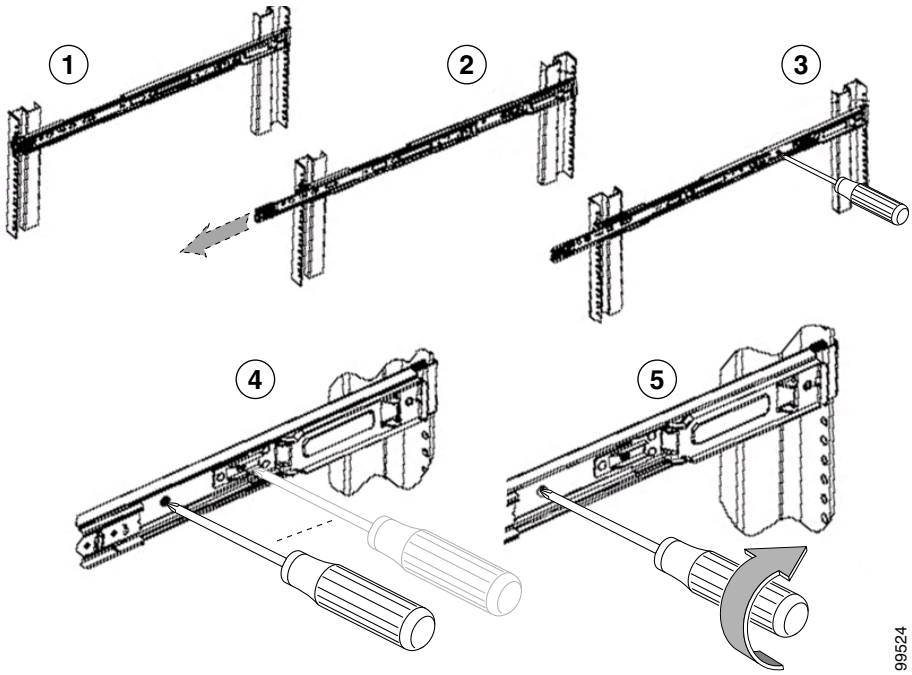
Figure 3-5 Attaching Back Rail to Rack



f. Repeat this process with the other rail and rack assembly.

g. Extend the middle rail about 30 cm (12 inches) and fasten with screws. See Figure 3-6. Then, push the middle rail back into its original position.

Figure 3-6 Attaching Screws to Telescopic Rail

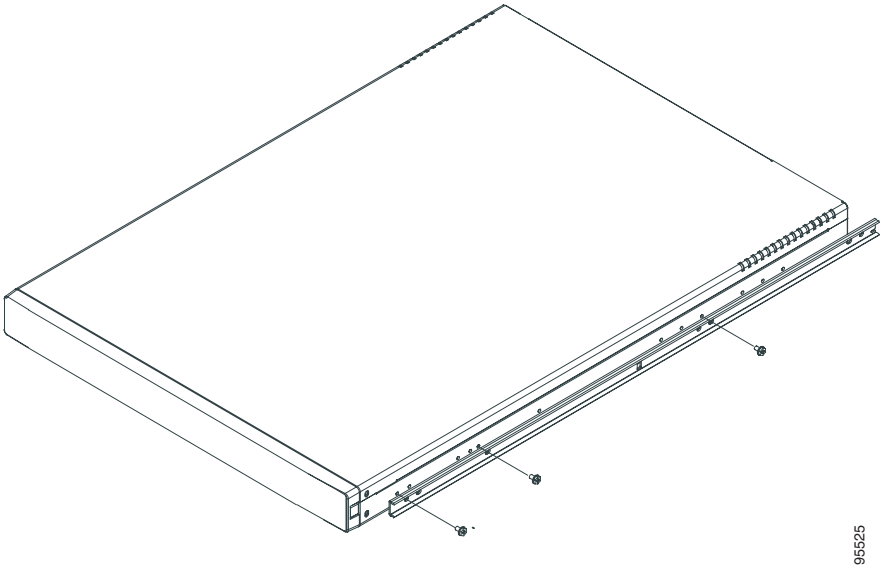


Note Leaving some play between the bracket and the rail until you install the rail into the rack will make affixing the rail to the rack easier. After the rail is attached to the rack, you can tighten the screws.

Step 2 Attach the chassis to the rack:

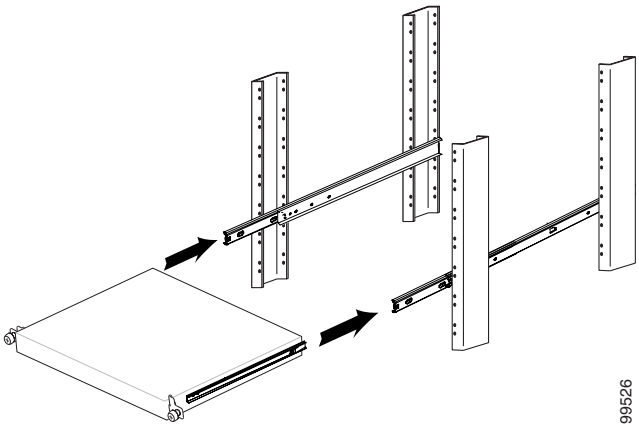
a. See Figure 3-7. Secure chassis to the inner rail using three screws. Repeat this process with the other server rail.

Figure 3-7 Attaching Chassis to Rail



b. See Figure 3-8. Insert the chassis in the rack.

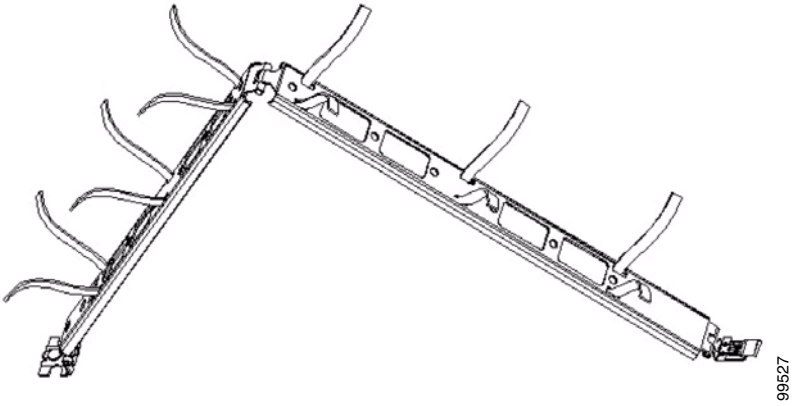
Figure 3-8 Sliding Chassis onto Rack



c. Slide the chassis backward and forward several times. Fasten with all the screws described in Step 1d.

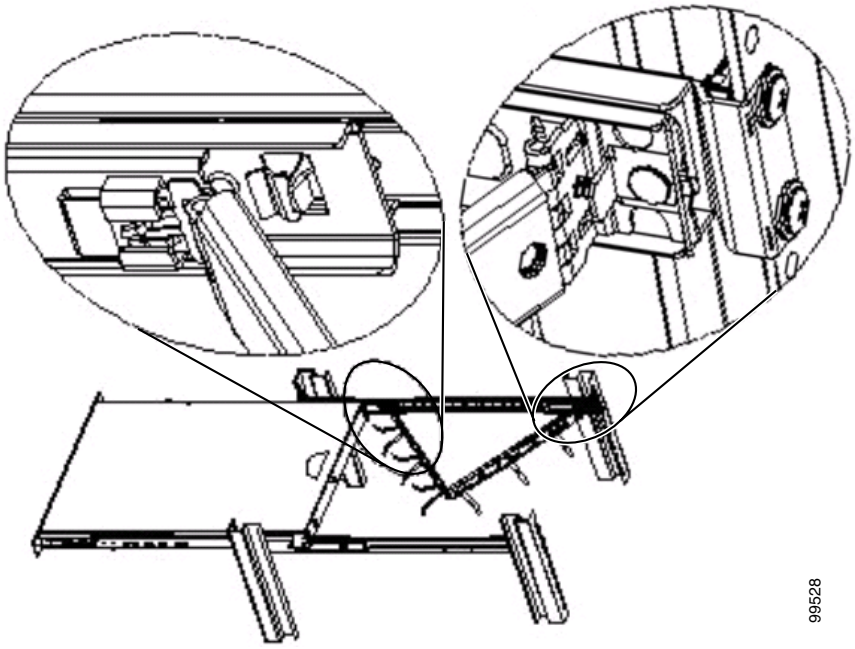
d. See Figure 3-9. Slide six Velcro strips into the holes of the management arm.

Figure 3-9 Attaching Velcro to Management Arm



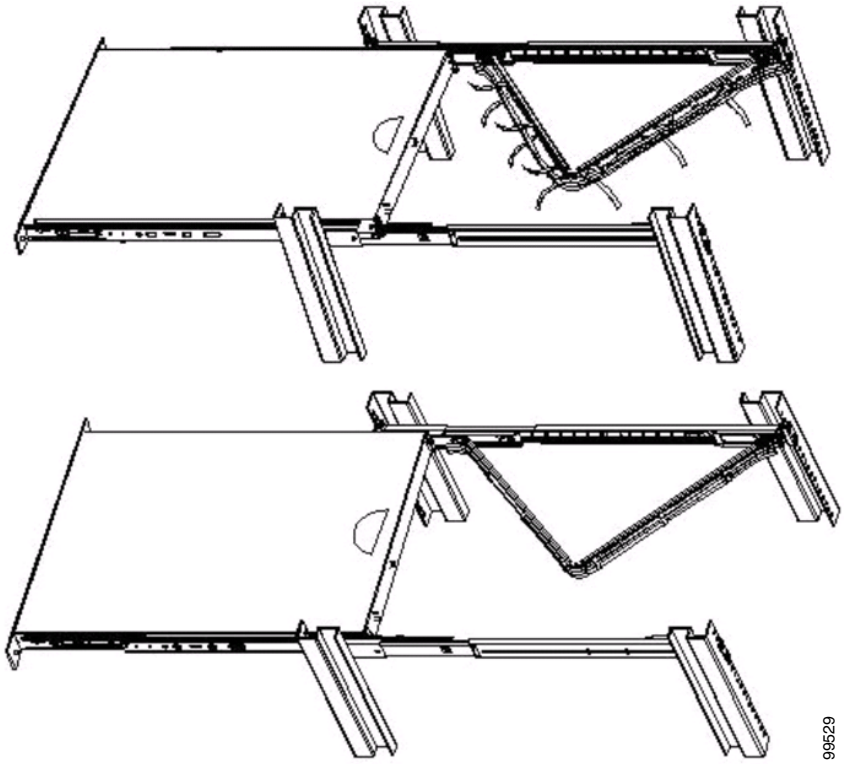
e. See Figure 3-10. Install the rear side of the cable management arm into the back rail until it snaps in the clip. Then install the front cable management arm into the inner rail until it snaps into the clip.

Figure 3-10 Attaching Management Arm



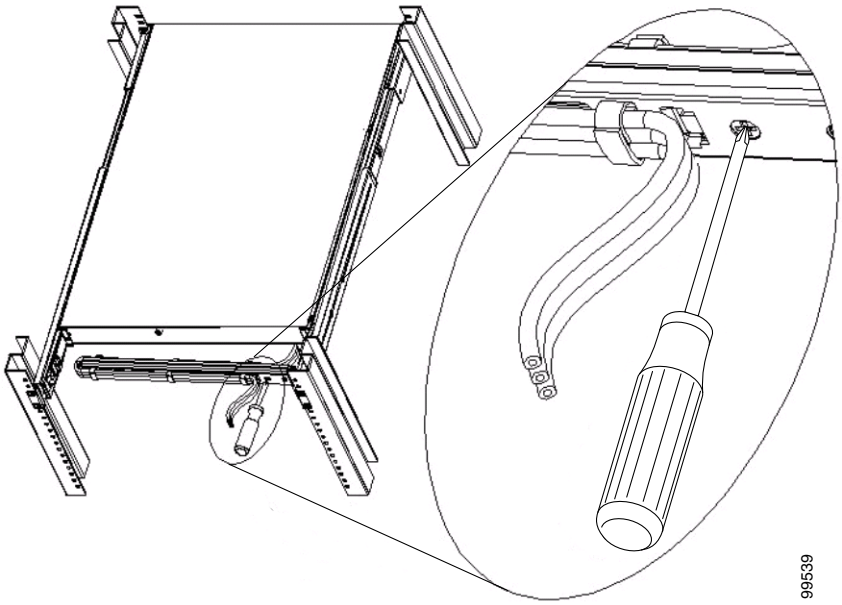
f. See Figure 3-11. Put cables into the cable management arm and use the Velcro to tighten the cable into the arm.

Figure 3-11 Installing Cable in Management Arm



g. See Figure 3-12. Push the server to the closed position. If the cable is too heavy to carry the server, use a screwdriver to adjust the cam so that the cable management arm is horizontal.

Figure 3-12 Fastening the Server into the Rack



Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 120 VAC, 15A (U.S./CAN); 240 VAC, 10A (INTERNATIONAL).** Statement 1005

Installing the Quanta (1113) ACS SE in a Rack

Before installing the Quanta (1113) ACS SE in a rack, read Preparing Your Site for Installation, page 2-5 to familiarize yourself with the proper site and environmental conditions. Failure to read and follow these guidelines could lead to an unsuccessful installation and possible damage to the system and components. Perform the steps below when installing and servicing the WLSE.

The rack must be properly secured to the floor, to the ceiling or 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.

When installing and servicing the ACS SE:

- 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, see 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 ACS SE in a rack that has not been securely anchored in place. Damage to the system and personal injury may result.
- Due to the size and weight of the computer system, never attempt to install the computer system by yourself.

See Precautions for Rack-Mounting, page 2-8 for additional safety information on rack installation.

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:**

- **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.**

The server can be installed in a system 1U rack. The rack rail components are as follows (numbers in parentheses refer to Figure 3-13):

- 2 telescopic rails (1, 2)
- Bag containing:
  - 8 Round head screws with washer (3)
  - 2 Round head screws (4)
  - 10 Cage nuts (5)

Figure 3-13 Rack Rail Components

To install the ACS SE 1113 (Quanta 1113) a rack, perform these steps as explained in the following sections:

1. Attach the chassis rail mount to the chassis (see Attaching the Chassis Rail Mount, page 3-15).
2. Attach the server rail to the rack assembly (see Attaching the Server Rail, page 3-18).
3. Slide the chassis on to the rack assembly (see Sliding Chassis On the Rack, page 3-20).

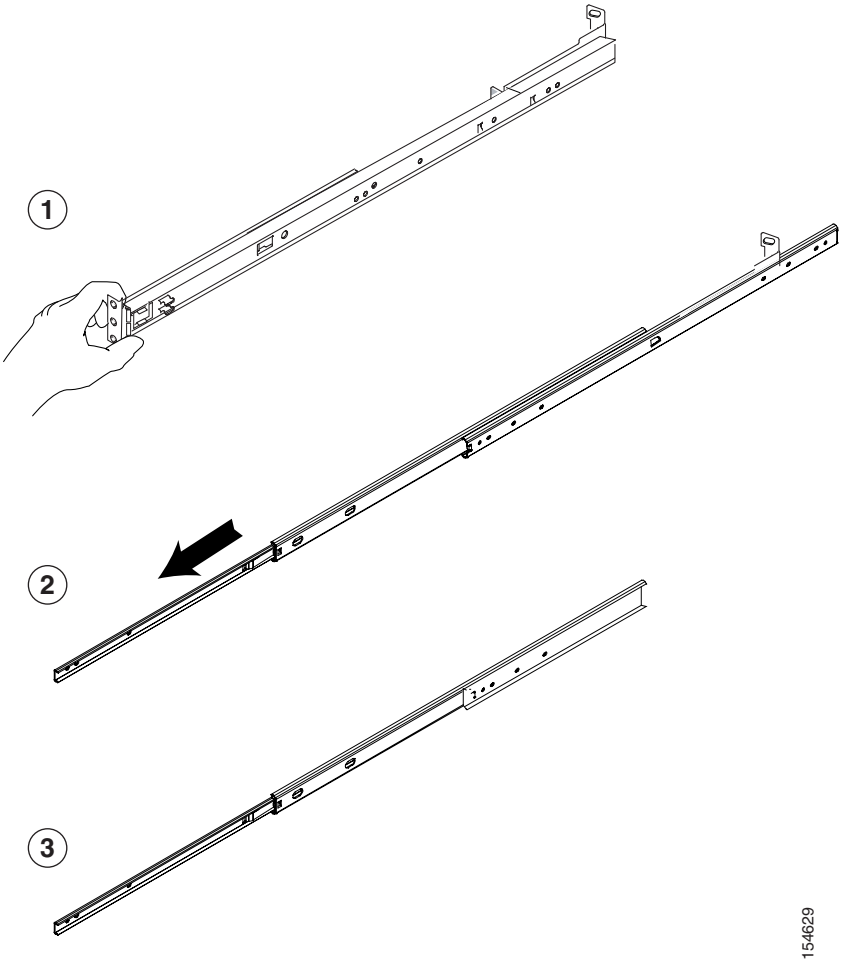
Attaching the Chassis Rail Mount

You must first remove the chassis rail mount section from the server rail and attach it to the chassis as shown in the following steps.

Procedure

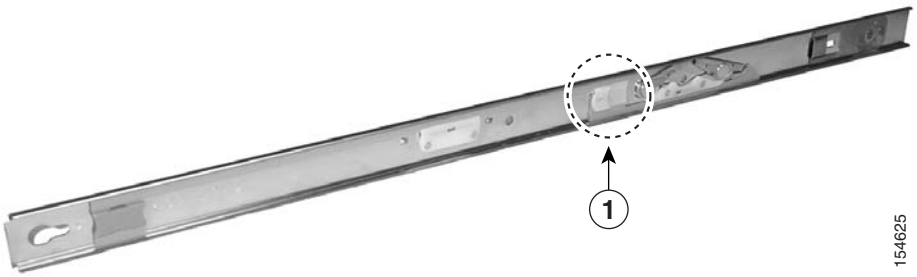
Step 1 See Figure 3-14. Extend the server rail as far as it will go. When fully extended, the server rail locks into the extended position.

Figure 3-14 Removing the Chassis Rail Mount



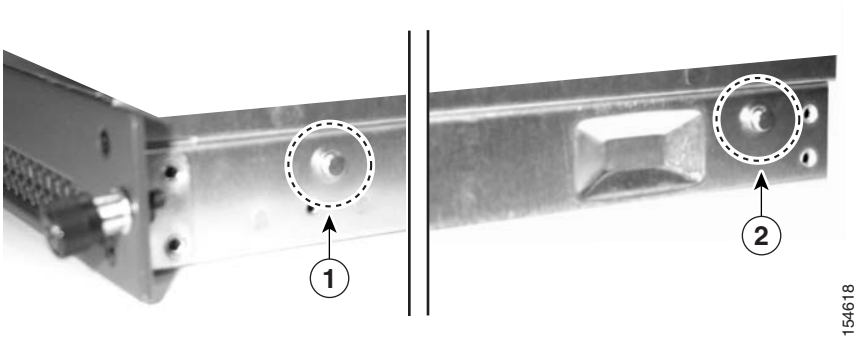
Step 2 See Figure 3-15. Slide the white tab (1) in the direction of its arrow and slide out the chassis rail mount part. (Set it aside for attaching to the chassis in the next step.)

Figure 3-15 Sliding the Chassis Rail Mount Release Tab



Step 3 Align the holes in the chassis rail mount to the pegs on the chassis (1 and 2 in Figure 3-16).

Figure 3-16 Positioning Chassis Rail Mount on Chassis



Step 4 See Figure 3-17. Align the holes (1) and then slide the rail until it locks into place (2).

Figure 3-17 Attaching Chassis Rail Mount to Chassis

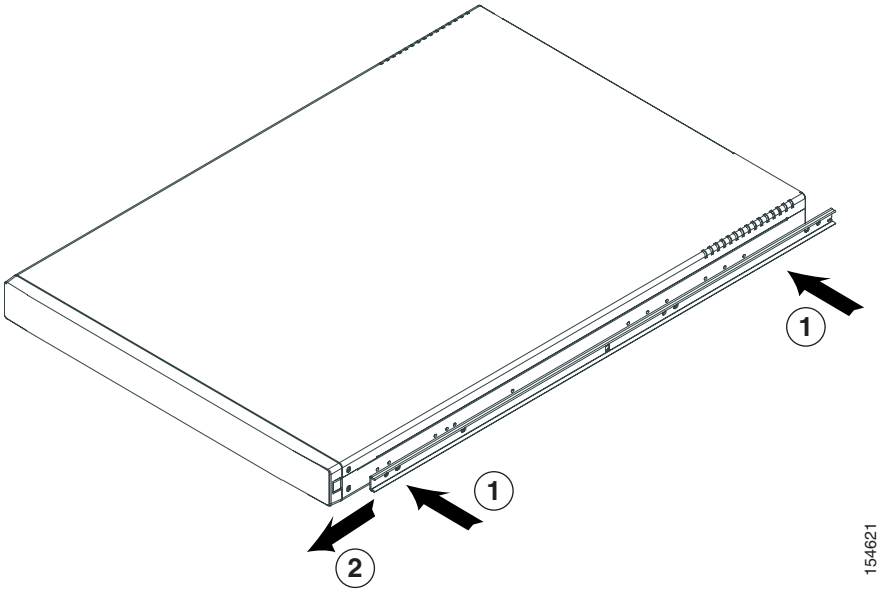
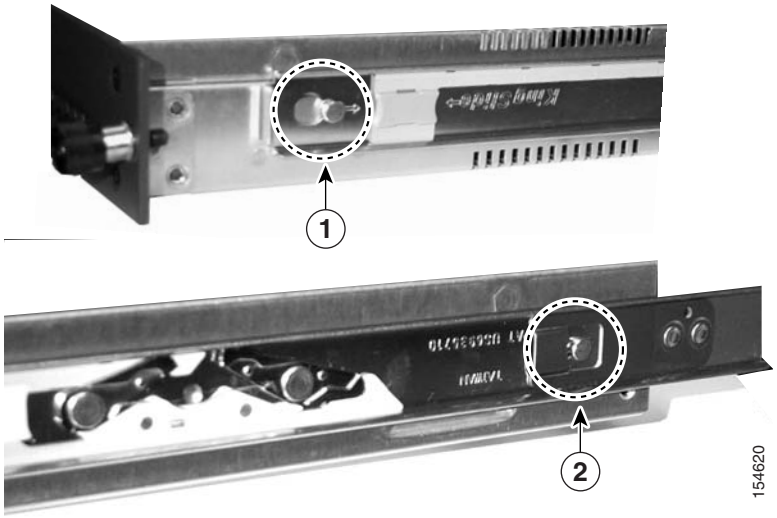


Figure 3-18 shows the chassis rail mount locked into place.

Figure 3-18 Chassis Rail Mount in Locked Position



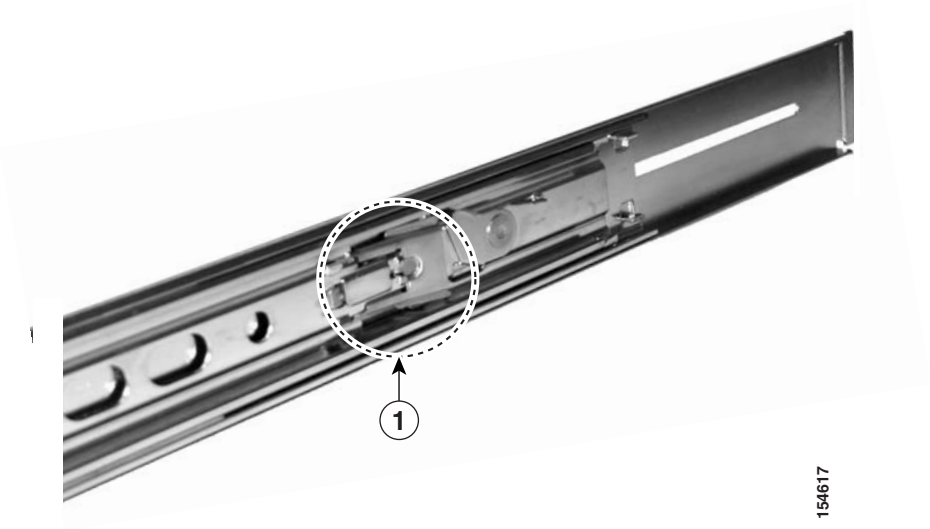
Attaching the Server Rail

Now that you have mounted the chassis rail mount, retract the server rail that you previously extended and then attach it to the rack. If you have already retracted the server rail, go to step 2.

Procedure

Step 1 To retract the arm of the server rail, push the tab shown in Figure 3-19. Then slide the arm back in.

Figure 3-19 Retracting the Server Rail



Step 2 Attach the server rail to the rack as shown in the figure that corresponds to your rack:

- For a square-peg rack, see Figure 3-20.
- For a circular-peg rack, see Figure 3-21.

Figure 3-20 Attaching Rail to a Square-Peg Rack

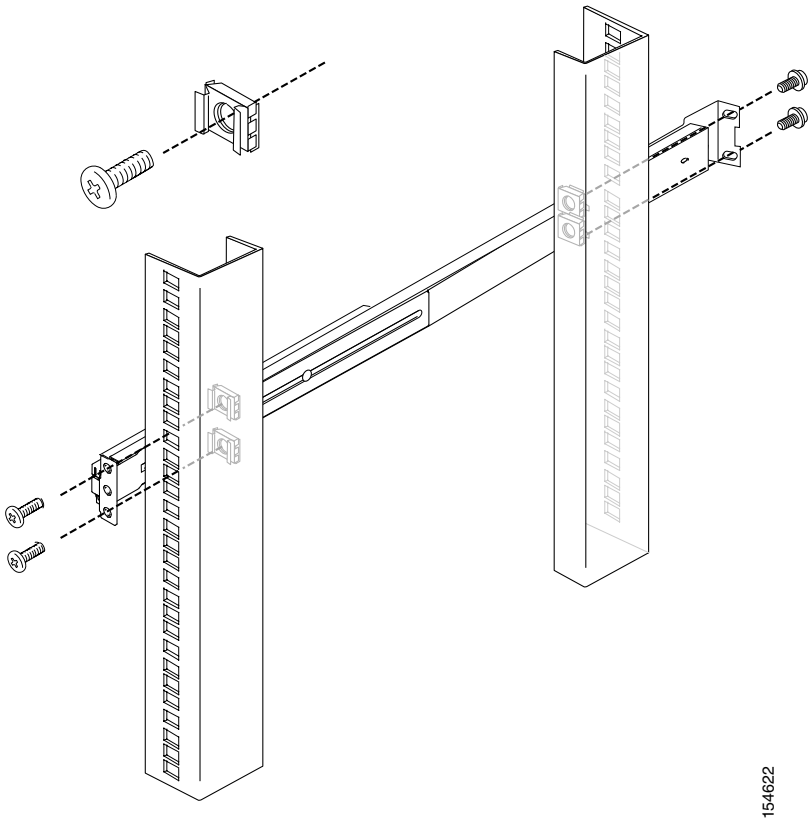
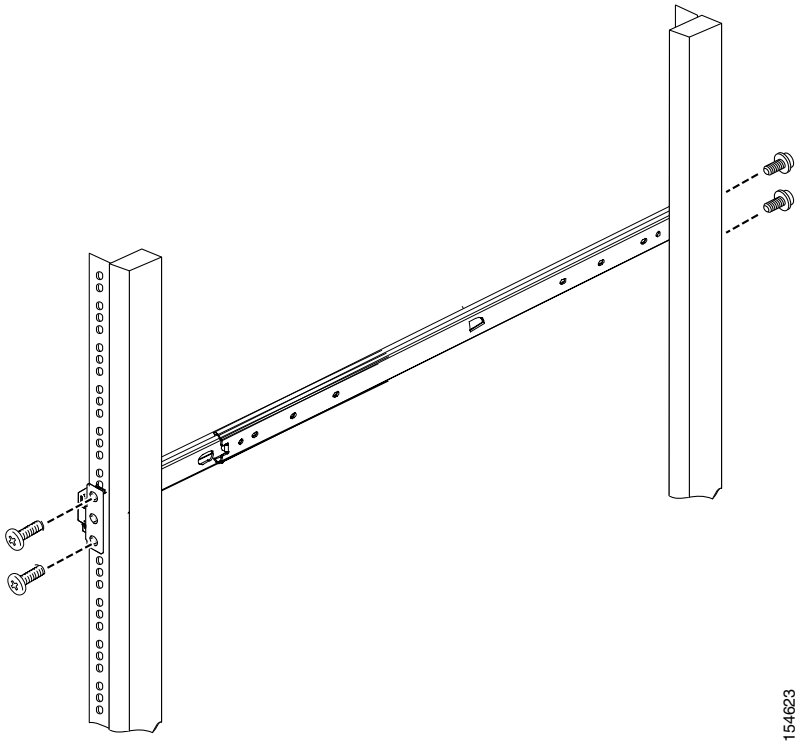


Figure 3-21 Attaching Rail to a Circular-Peg Rack



Step 3 Repeat this process with the other rail and rack assembly.

Note Leaving some play between the bracket and the rail until you install the rail into the rack will make affixing the rail to the rack easier. After the rail is attached to the rack, you can tighten the screws.

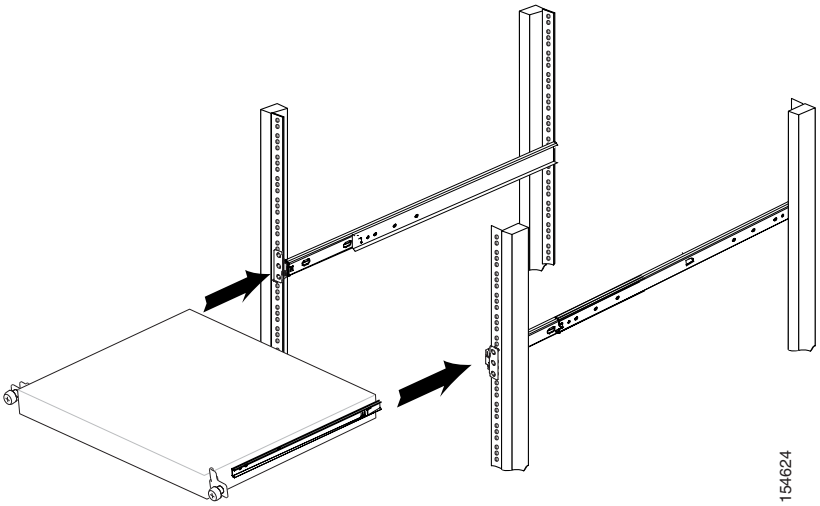
Sliding Chassis On the Rack

Step 1 See Figure 3-22. On the chassis rail mount, slide and hold the purple tab in the direction of the arrow. This allows the chassis rail mount to slide on to the rail.

Figure 3-22 Sliding the Chassis Rail Mount Extended Tab

Step 2 Insert the chassis in the rack. See Figure 3-23.

Figure 3-23 Sliding Chassis onto Rack



Slide the chassis back and forth several times. Fasten with all the screws.

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that you use a fuse or circuit breaker no larger than 120 VAC, 15A (U.S./CAN); 240 VAC, 10A (INTERNATIONAL).** Statement 1005

Connecting to the AC Power Source

Warning **This equipment must be grounded. 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.** Statement 1024

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

Connecting Cables

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

To connect the cables:

Step 1 Plug the network connection into the Ethernet 0 port (NIC 1). See Figure 1-3 on page 1-5 for the location of the Ethernet 0 port.

Step 2 Connect a console to the console or serial port using the supplied serial cable and, if necessary, the DB-9-to-RJ-45 console adapter. See Figure 1-3 on page 1-5 for the location of the serial port.

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

Initial Configuration

The first three steps of the four steps required to configure the ACS are documented in this manual:

- Establishing a Serial Console Connection, page 3-22
- Configuring ACS SE, page 3-23
- Verifying the Initial Configuration, page 3-27

Note You perform the fourth and final part of the configuration, which includes providing AAA services by establishing administrative and user accounts and configuring network connections, from the web interface. See *User Guide for Cisco Secure ACS Solution Engine* for more information.

Establishing a Serial Console Connection

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

To establish a serial console connection:

Note If you performed the procedure in Connecting Cables, page 3-22, 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 ACS SE. 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 ACS SE.

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

Step 2 Power on ACS SE and the console, and open your terminal emulation communication software on the console.

Tip See Figure 1-2 on page 1-3 for the location of the power switch on the ACS SE.

Step 3 Set your terminal emulation communication software to operate with the following settings:

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

Result: The `login:` prompt appears.

Configuring ACS SE

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

Before you begin to configure the solution engine, you should have the following information:

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

To configure the ACS SE:

Step 1 Establish a serial console connection to the ACS SE; for details see Establishing a Serial Console Connection, page 3-22.

Note If the ACS SE 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 appears above the `login:` prompt:

```
Cisco Secure ACS: [version number]
Appliance Management Software: [version number]
Appliance Base Image: [version number]
CSA build [version number]: (Patch: [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. You must log in as Administrator 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 that you intend to use for your ACS SE, 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 ACS SE administrator account name, and then press **Enter**.

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

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

Note The new password must contain a minimum of 6 characters, and 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 ACS SE 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 The following prompt appears for the new database password:

```
Please enter the Encryption Password for the Configuration Store.
Please note this is different from the administrator account,
it is used to encrypt the Database.
```

Type the new database 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*.

Step 11 At the `Enter new password again:` prompt, type the new database password, and then press **Enter**.

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

```
Password is set successfully.
```

Step 12 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 ACS SE, it must be connected to a working Ethernet connection.

Note A static IP address must be assigned to your ACS SE. You can set the IP address directly by answering **Y** to this step and performing the substeps detailed in Step 13. Alternatively, you may use a DHCP server if it assigns a single IP address that does not change.

Step 13 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 ACS SE 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 that 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 ACS SE at the `DNS Servers [xx.xx.xx.xx]:` prompt. If you do not configure the ACS SE 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 this 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 ACS SE.

g. At the prompt, `Enter hostname or IP address:`, type the IP address or hostname of a device connected to the ACS SE, 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 validated 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 means that you can correct network connections or retype the IP address.

Step 14 If the settings appear correctly, 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 15 To set the time and date of the ACS SE, 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 16 At the `Enter desired time zone index (0 for more choices):` prompt, type the index number of the time zone that you want, and then press **Enter**.

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

Step 17 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 that you want.

Tip Only if you select to use an NTP server can you subsequently use the `ntpsync` command.

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

Step 18 At the `Enter date [mm/dd/yyyy]:` prompt, type the date in the given format, and then press **Enter**.

Step 19 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 ACS SE initial configuration:

Before You Begin

Establish a serial console connection to the ACS SE. For details, see Establishing a Serial Console Connection, page 3-22.

Step 1 Reboot the ACS SE. For more information, see Rebooting the Solution Engine From a Serial Console, page 4-3.

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

Step 2 At the `login:` prompt, type the new administrator name, and press **Enter.**

Result: The password prompt appears.

Step 3 At the `password:` prompt, enter the password you created during initial configuration.

Result: The system prompt appears.

Step 4 At the system prompt, type **show**, and then press **Enter**.

Result: The system displays status information.

Step 5 Verify the displayed information.

Next Steps

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

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

Note Note regarding “Self” entry in AAA servers table to be added (in progress)

Administering Cisco Secure ACS Solution Engine

This section describes the major Cisco Secure ACS Solution Engine (ACS SE) system administration tasks that you can perform by using the command line interface (CLI) in the serial console connection. For all other ACS SE configuration and administration tasks, that is, those performed from the ACS web interface, see the *User Guide for Cisco Secure ACS Solution Engine*.

Serial console service starts automatically when the ACS SE 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 from a serial console connected to the ACS SE. This section contains the following procedures:

Logging In to the Solution Engine From a Serial Console

To log in to the ACS SE from a serial console:

Step 1 Establish a serial console connection to the ACS SE. For details, see Establishing a Serial Console Connection, page 3-22.

Step 2 At the `login:` prompt, enter the ACS SE administrator name.

Step 3 At the `password:` prompt, enter the ACS SE password.

Result: The system prompt appears:

ACS SE name

Note Only one set of ACS SE login credentials (administrator name and password) has the serial connection privilege.

Shutting Down the Solution Engine From a Serial Console

You use the serial console to shut down the ACS SE.

Caution Powering off the ACS SE by using only the power switch may cause the loss or corruption of data.

To use the serial console to shut down the ACS SE:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a 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 ACS SE displays the message:

```
It is now safe to turn off the computer
```

Step 4 Press the power switch and hold it down for 4 seconds to turn off the ACS SE. For the location of the power switch see Figure 1-2 on page 1-3.

Result: The ACS SE powers OFF.

Logging Off the Solution Engine From a Serial Console

To log off the ACS SE from the serial console:

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 Solution Engine From a Serial Console

To reboot the ACS SE from the serial console:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

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

Result: The ACS SE displays the message:

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

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

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

Determining the Status of Solution Engine System and Services From a Serial Console

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

Note You typically perform status determination in the ACS SE web interface. For more information, see "Determining the Status of Cisco Secure ACS Services" in the *User Guide for Cisco Secure ACS Solution Engine*.

To determine the status of the ACS SE and ACS Services:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a 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:

```
ACS SE Name
ACS SE Version
Appliance Management Software Version
Appliance Base Image Version
CSA build XXXX: (Patch: x_x_x_xxx)
```

```
Session Timeout (in minutes)
Last Reboot Time
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
    CSAgent
    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 D-17.

To trace the network route that the ACS SE takes to a given destination:

Step 1 At the system prompt, type **tracert**, followed by zero (0) 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 Solution Engine Services From a Serial Console

Note You typically stop solution engine services in the web interface.

You can stop any of the ACS SE services from the serial console. The ACS SE services include:

- CSAdmin
- CSAgent
- 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 Solution Engine System and Services From a Serial Console, page 4-3.

Note When you stop the CSAgent service, that service remains disabled until you explicitly start it again. That is, if you stop the CSAgent service it does not automatically restart when the system is rebooted.

To stop a service on the ACS SE:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

Step 2 Type **stop** followed by a single space and the name of the ACS service that 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 displays the message:

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

Followed by the message:

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

Starting Solution Engine Services From a Serial Console

Note You typically start solution engine services in the web interface.

You can start any of the ACS services from the serial console. The ACS SE services include:

- CSAdmin
- CSAgent
- 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 Solution Engine System and Services From a Serial Console, page 4-3.

To start an ACS service:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

Step 2 Type **start** followed by a single space and the name of the ACS service that 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 displays the message:

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

Followed by the message

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

Restarting Solution Engine Services From a Serial Console

Note You typically restart solution engine services in the web interface.

You can restart any ACS SE service from the serial console. ACS SE services include:

- CSAdmin
- CSAgent
- 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 Solution Engine System and Services From a Serial Console, page 4-3.

To restart an ACS service:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

Step 2 Type **restart** followed by a single space and the name of the ACS service that 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 displays 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 From the Serial Console

To obtain a list and description of commands on the ACS SE from the serial console:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a 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 ACS SE displays the list of commands and their descriptions shown in the following table:

Command	Description
?	List commands
backup	Backup Appliance
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
ntpsync	Perform Network Time Protocol synchronization
ping	Verify connections to remote computers

Command	Description
reboot	Soft reboot appliance
restart	Restart ACS services
restore	Restore Appliance
rollback	Rollback patched package
set admin	Set administrator's name
set dbpassword	Set database password
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 ACS SE commands, see Appendix D, “Command Reference.”

Working with System Data

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

Obtaining Support Logs From 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 ACS SE.

Note You typically perform this procedure in the ACS SE web interface.

This procedure uses the **support** command. For more information on this command, see support, page D-16. The arguments for the **support** command include:

Argument	Description
-d n	Collect the previous *n* days logs
-u	Collect user database information
server	Hostname for the FTP server to which the file is to be sent
filepath	Location under the FTP root for the server into which the package.cab is to be sent
username	Account used to authenticate the FTP session

To generate a *.cab* file of log and system registry information:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a 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 `Enter FTP Server directory` prompt, enter the pathname to the location on your FTP server to which you want to send the file and then press **Enter**.

Step 6 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 7 At the `Enter FTP Server Hostname or IP address` prompt, enter your FTP server hostname or IP address and 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 interrupt use of the ACS SE.

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

Result: The ACS SE 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 message indicates the ACS SE 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 ACS SE log files to an FTP server for further examination and processing. Using the **exportlogs** command, you can enter the name of the log or logs to export, or select log names from a list.

Before You Begin

You must have the FTP server address and pathname, 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 ACS SE.

To export log files to an FTP server:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

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

where *logname* is the name of log you want to export.

Tip You can enter more than one log name and separate 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 ACS SE.

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 pathname and press **Enter**.

Result: The ACS SE exports the specified files to the specified location.

Exporting a List of Groups

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

Before You Begin

You must have the FTP server address and pathname, 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 ACS SE.

To export a user group list to an FTP server:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

Step 2 Type **exportgroups**.

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

Step 3 Press **Enter**.

Result: The system displays the 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 ACS SE.

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

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

Step 6 At the `Directory:` prompt, enter the FTP server pathname and press **Enter**.

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

Step 8 At the `Password:` prompt, enter your FTP server password and press **Enter**.

Result: The ACS SE exports the group list file to the specified location. When done the system displays the message:

```
Transferring 'groups.txt' completed
```

The system prompt returns.

Exporting a List of Users

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

Before You Begin

You must have the FTP server address and pathname, 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 ACS SE.

To export a list of users to an FTP server:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

Step 2 Type **exportusers**.

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

Step 3 Press **Enter**.

Result: The system displays the 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 ACS SE.

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

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

Step 6 At the `Directory:` prompt, enter the FTP server pathname and press **Enter**.

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

Step 8 At the `Password:` prompt, enter your FTP server password and press **Enter**.

Result: ACS SE exports the file of the list of users to the specified location, and then displays the message:

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

The system prompt reappears.

Backing Up ACS Data From the Serial Console

This section details how to use the serial console to back up ACS SE data to an FTP server.

Note You typically perform this procedure in the web interface.

During backup, AAA services are interrupted, and ACS SE 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 From the Serial Console, page 4-14.

Before You Begin

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

Caution This procedure interrupts the use of the ACS SE for AAA services.

To export ACS SE data to an FTP server:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

Step 2 Type **backup**.

Tip You can enter the following parameters after 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 pathname 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 that 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 ACS SE 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 ACS SE displays the 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 ACS SE exports the backup file to the specified location and displays messages regarding the progress of the backup. The following message signifies the completion of the backup process:

```
Transferring xxx completed.
```

The system prompt reappears.

Restoring ACS Data From the Serial Console

This section details how to use the serial console to restore ACS SE data from an FTP server after you perform a backup. For more information on backing up ACS SE data, see Backing Up ACS Data From the Serial Console, page 4-12.

Note You typically perform this procedure in the web interface.

Before You Begin

You must have the FTP server address and pathname, 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 ACS SE for AAA services.

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

To restore ACS SE data from an FTP server:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

Step 2 Type **restore**.

Tip You can enter the following parameters after 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 pathname 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 If you previously chose to decrypt the backup file, 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 ACS SE 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 ACS SE has no shared profile components configured, you see a message about DCS (device command sets) not on the backup, which is normal.

When completed the system displays the message:

```
Done
```

Reconfiguring Solution Engine System Parameters

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

Resetting the Solution Engine Administrator Password

There is always a single set of ACS SE administrator credentials that consists of the 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 ACS web interface.

You can reset the ACS SE administrator name, the administrator password, or both. This procedure details how to reset the password after you log in with the existing credentials. To reset the administrator name see Resetting the Solution Engine Administrator Name, page 4-16.

If you do not have the existing ACS SE administrator login credentials, you must have the recovery CD ROM to reset these credentials. For information on resetting the administrator login and password without first logging in, see Recovering from Loss of Administrator Credentials, page 4-23.

To reset the ACS SE administrator login credentials:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

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

Result: The ACS SE displays the prompt:

```
Enter old password:
```

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

Result: The ACS SE displays the prompt:

```
Enter new account name:
```

Step 4 Type the new account name, and then press **Enter**.

Result: The ACS SE displays the prompt:

```
Enter new password
```

Step 5 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, uppercase letters, and lowercase letters). Each of the following examples is acceptable: *1PaSsWoRd, *password44, Pass*word*.

Result: The ACS SE displays the prompt:

```
Reenter new password
```

Step 6 Type the new password again, and then press **Enter**.

Result: The ACS SE displays the prompt:

```
Password is set successfully.
Administrator account name is set to _____
```

Resetting the Solution Engine Administrator Name

There is always a single set of ACS SE administrator credentials that consists of the 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 ACS web interface.

You can reset the ACS SE administrator name, the administrator password, or both. This procedure details how to reset the administrator name after you log in with the existing credentials. To reset the password, see Resetting the Solution Engine Administrator Password, page 4-15.

If you do not have the existing ACS SE administrator login credentials, 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 4-23.

To reset the ACS SE administrator name:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

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

Result: The ACS SE 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 message:

```
Administrator name is set successfully.
```

Resetting the Solution Engine Database Password

You should change the ACS SE database password from time to time, to ensure database security. This procedure details how to reset the password after you have logged on with the existing credentials.

To reset the ACS SE database password:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

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

Result: The ACS SE displays the prompt:

```
Enter old password:
```

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

Result: The ACS SE displays the prompt:

```
Enter new password
```

Step 4 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, uppercase letters, and lowercase letters). Each of the following examples is acceptable: *1PaSsWoRd, *password44, Pass*word*.

Result: The ACS SE displays the prompt:

```
Reenter new password
```

Step 5 Type the new password again, and then press **Enter**.

Result: The ACS SE displays the prompt:

```
Password is set successfully.
```

Reconfiguring the Solution Engine IP Address

Typically, you configure the IP address only once, during initial configuration. See Configuring ACS SE, page 3-23.

Caution Reconfiguring the IP address may cause other network devices to fail to recognize the ACS SE.

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 ACS SE, ACS SE must be connected to a working Ethernet connection.

To reconfigure the IP address:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a 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:

a. To specify the ACS SE 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 message:

```
IP Address is reconfigured.
```

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

Result*:* The ACS SE restarts. The system displays the 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 ACS SE.

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

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

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 **N**. This procedure gives you an opportunity, if required, to correct network connections or retype the IP address.

Result: The ACS SE restarts services, and displays the system prompt.

Setting the System Time and Date Manually

You can set and maintain the system date and time by using one 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 ACS SE system time and date by using an NTP, see Setting the System Time and Date with NTP, page 4-20.

To set the ACS SE system time and date manually:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

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

Result: The system displays the message:

```
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 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 by using one 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. (You can configure backup NTP servers if you desire.)

To set the ACS SE system time and date manually, see Setting the System Time and Date Manually, page 4-19.

To set the ACS SE system time and date with NTP:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

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

Result: The system displays the message:

```
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 displays indexed time zones and the 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(es):` prompt, enter the IP address of the NTP server that you want to use, and then press **Enter**.

Tip If you want to configure multiple NTP servers, at the `Enter NTP Server IP Address:` prompt, enter multiple IP addresses, each separated by a space.

Result: The system displays the message:

```
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 that can pass with no activity on the serial console before the console login times out.

To set the ACS SE system timeout:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a 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 Solution Engine System Domain

You can set the system DNS domain from the serial console. To set the ACS SE system domain:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a 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 confirmation message:

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

Setting the Solution Engine System Hostname

Caution Performing this procedure stops and restarts all services, and will interrupt use of the ACS SE.

You can set the system hostname. To set the ACS SE system hostname:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a 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. The system then displays the confirmation message:

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

(The hostname is then reset after system reboot.)

Patch Rollback

This section contains the following topics:

Removing Installed Patches

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

To roll back a ACS SE system patch:

Step 1 Connect a console to the ACS SE 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 the confirmation message:

```
Are you sure you want to rollback [patch name]?)(Y/N):
```

Step 3 Type **Y** to continue.

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 Solution Engine System and Services From a Serial Console, page 4-3.

Understanding the CSAgent Patch

In ACS SE the CSAgent service is implemented as a pre-installed patch. You must stop CSAgent before you can install any patch or upgrade. Although, as a patch, the CSAgent can be rolled back, the preferred method for disabling this service is simply to stop it. Once stopped, the CSAgent service does not restart when the system is restarted; you must explicitly restart the service for it to operate. For more information, see *User Guide for Cisco Secure ACS Solution Engine*.

Recovery Management

ACS SE functionality includes two procedures that the administrator can perform by using the ACS SE Recovery CD ROM:

- Recovering from Loss of Administrator Credentials, page 4-23
- Re-imaging the Solution Engine Hard Drive, page 4-25

Recovering from Loss of Administrator Credentials

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

You should understand the following regarding the ACS SE administrator login credentials:

- Only one set of administrator login credentials exists 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 Solution Engine Administrator Password, page 4-15.
- This recovery procedure entails replacing the administrator login credentials with a new account name and password.

To reset the administrator login credentials:

Step 1 Connect a console to the ACS SE 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 ACS SE Recovery CD ROM into the solution engine CD ROM drive.

Step 4 Power on the ACS SE. (Or if already running, reboot the solution engine. For more information, see Rebooting the Solution Engine From a Serial Console, page 4-3.)

Result*:* The system displays the message:

```
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 prompt:

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

Step 6 Type **Y**.

Result*:* The system displays the 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 ACS SE administrator, and then press **Enter**.

Step 11 At the `Enter new password:` prompt, type the new ACS SE 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, uppercase letters, and lowercase letters). Each of the following examples is acceptable: *1PaSsWoRd, *password44, Pass*word*.

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

Result*:* The system displays the message:

```
Password is set successfully.
```

Re-imaging the Solution Engine Hard Drive

Use the ACS SE Recovery CD ROM to re-image the ACS SE if necessary.

Caution Performing this procedure destroys all data stored on the ACS SE.

To re-image your ACS SE:

Step 1 Connect a console to the ACS SE 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 ACS SE CD-ROM drive. For the location of the CD-ROM drive, see Figure 1-2 on page 1-3.

Step 3 Power on the ACS SE. (Or, if the solution engine is already running, reboot it.) For more information, see Rebooting the Solution Engine From a Serial Console, page 4-3.

Result: The ACS SE displays the message:

```
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 ACS SE displays the message:

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

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

Step 5 Type **Y**.

Result: The ACS SE processes the new image (this may take more than 2 minutes) while displaying odd characters and then displays the message:

```
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 ACS SE.

Step 7 Press **Enter** to restart the ACS SE.

Result: The ACS SE 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, which is normal system behavior.

Note After re-imaging the solution engine hard drive, you must once again perform initial configuration of the ACS SE. For detailed instructions, see Configuring ACS SE, page 3-23.

Upgrading and Migrating to Cisco Secure ACS Solution Engine

This chapter describes how to upgrade to Cisco Secure ACS Solution Engine (ACS SE) 4.0, and how to migrate from an ACS Windows server to ACS SE. This chapter contains the following sections:

Upgrading to ACS SE 4.0.1 on the Quanta (1113) Platform

The ACS SE 4.0.1 release uses the ACS SE Quanta (1113) platform. ACS SE on the Quanta (1113) platform can only run the ACS 4.0.1 software release (ACS for Windows 4.0.1.27). You cannot upgrade the software directly on the ACS SE Quanta (1113) platform using the ACS upgrade or management upgrade packages. Instead, you must do the following:

1. Upgrade the software on a previous SE hardware platform (the Cisco 1111 or the Cisco 1112) to ACS version 4.0.1 (ACS for Windows 4.0.1.27) using one of the upgrade methods:
   - The full upgrade method. For information on this method, see Performing a Full Upgrade, page 5-4
   - The ACS management upgrade method. For information on this method, see Upgrading to ACS SE 4.0 on top of the Existing Base Image, page 5-6.
2. Back up the software on the previous SE hardware platform.
3. On the new hardware platform—the Quanta (1113) hardware version, first install the SE 1113 version, or use the existing installation, and then use the ACS restore feature to install the 4.0.1 software (ACS for Windows 4.0.1.27) on the SE device.

   For information on steps 2 and 3, see Migrating to ACS SE, page 5-11.

Upgrading to ACS SE 4.0

Note The information in this section applies only to upgrading the software on the Quanta (1112) version of the SE appliance hardware. If you are migrating the software release from an existing Cisco 1111 or Cisco 1112 device to a Cisco 1113 device—the Quanta (1113) version, you must first back up the existing software and then use the restore feature to install it on the Quanta (1113) hardware platform.

You can upgrade your existing ACS SE appliance with the latest ACS software, appliance management software, and appliance base image.

Table 5-1 describes the upgrade paths for ACS SE based on whether you want to perform a full upgrade, including the latest base image, and whether you want to restore existing data.

Note The ACS SE 4.0 base image includes additional Microsoft hotfixes. For details, see *Release Notes for Cisco Secure ACS Solution Engine 4.0*.

Table 5-1 Upgrade Paths to ACS SE 4.0

Upgrade Path	Description	Upgrade Procedure
Full upgrade with data restore	Upgrades appliance base image, appliance management software, and ACS software. Restores existing data.	Performing a Full Upgrade, page 5-4
Full upgrade without data restore	Upgrades appliance base image, appliance management software, and ACS software. All existing data is lost.	Performing a Full Upgrade, page 5-4
Appliance management software and ACS software upgrade.	Upgrades appliance management software, and ACS software on top of the existing base image. Existing data and configuration is automatically restored. The base image is not upgraded.	Upgrading to ACS SE 4.0 on top of the Existing Base Image, page 5-6

Note If you are upgrading from an ACS SE version before ACS SE 3.2.3, you must first upgrade to ACS SE 3.3.3. For information about upgrading to ACS SE 3.3.3, see *Release Notes for Cisco Secure ACS Solution Engine 3.3.3* on Cisco.com.

Table 5-2 describes various upgrade use cases that you can use to decide the appropriate upgrade path to follow.

Caution Backup and restore are supported and tested only when done on the same version. For example, backup on 4.0 and restore on 4.0 is supported; not backup on 3.3.3 and restore on 4.0.

Note Before you begin any upgrade procedure, we recommend that you back up your existing data and configuration.

Table 5-2 Upgrade Use Cases

From Version	Upgrade Path	Results
3.3.2, 3.3.1, or 3.2.3	**Full Upgrade with Data Restore** 1. Use the Upgrade Package Appliance Management Software for ACS 4.0.1. 2. Use the Upgrade Package ACS 4.0.1 Software for Appliance 3. Back up your data. 4. Use the ACS SE 4.0 Recovery CD[1] to upgrade the appliance. 5. Restore the data. See Performing a Full Upgrade, page 5-4.	• Base image upgraded including SNMP support, and installation of Cisco Security Agent (CSA). • Appliance management software upgraded. • ACS software upgraded. • Data restored.
3.3.3 (includes SNMP support and CSA)	**Full Upgrade with Data Restore** 1. Use the Upgrade Package Appliance Management Software for ACS 4.0.1. 2. Use the Upgrade Package ACS 4.0.1 Software for Appliance 3. Back up your data. 4. Use the ACS SE 4.0 Recovery CD[1] to upgrade the appliance. 5. Restore the data. See Performing a Full Upgrade, page 5-4.	• Base image upgraded including additional Microsoft hotfixes. • Appliance management software upgraded. • ACS software upgraded. • Data restored.
3.3.2, 3.3.1, or 3.2.3	**Full Upgrade without Data Restore** Use the ACS SE 4.0 Recovery CD[1] to upgrade the appliance. See Performing a Full Upgrade, page 5-4.	• Base image upgraded including SNMP support, and installation of Cisco Security Agent (CSA). • Appliance management software upgraded. • ACS software upgraded. • Blank database (data not restored).
3.3.3 (includes SNMP support and CSA)	**Full Upgrade without Data Restore** Use the ACS SE 4.0 Recovery CD[1] to upgrade the appliance. See Performing a Full Upgrade, page 5-4.	• Base image upgraded including additional Microsoft hotfixes. • Appliance management software upgraded. • ACS software upgraded. • Blank database.

Table 5-2 Upgrade Use Cases (continued)

From Version	Upgrade Path	Results
3.3.2, 3.3.1, or 3.2.3	**Appliance management software and ACS software upgrade.** 1. Use the Upgrade Package Appliance Management Software for ACS 4.0.1. 2. Use the Upgrade Package ACS 4.0.1 Software for Appliance See Upgrading to ACS SE 4.0 on top of the Existing Base Image, page 5-6.	• Base image not upgraded—no SNMP support and no installation of Cisco Security Agent (CSA). • Appliance management software upgraded. • ACS software upgraded. • Data restored.
3.3.3 (includes SNMP support and CSA)	**Appliance management software and ACS software upgrade.** 1. Use the Upgrade Package Appliance Management Software for ACS 4.0.1. 2. Use the Upgrade Package ACS 4.0.1 Software for Appliance See Upgrading to ACS SE 4.0 on top of the Existing Base Image, page 5-6.	• Base image not upgraded— no additional Microsoft hotfixes. • Appliance management software upgraded. • ACS software upgraded. • Data restored.

1. Ensure that you are using the correct recovery files for your specific hardware (Cisco 1111 or 1112).

Note If you use ACS Remote Agents, after any type of upgrade to ACS SE 4.0, you must uninstall your old version of ACS Remote Agents, and install Remote Agents for ACS SE 4.0.

Performing a Full Upgrade

This procedure upgrades ACS SE to version 4.0 on a Cisco 1111 or a Cisco 1112 device.

To restore data on the upgraded appliance, you must upgrade the software on the appliance so that you can back up the upgraded data and configuration. You then reinstall ACS 4.0, and restore your data and configuration.

If you do not want to restore data on the upgraded appliance, skip steps 2 and 5.

Before you begin:

Make a backup of your existing data and configuration

Note The backup procedure does not back up the cert7.db file. If you use this certificate file with an LDAP database, we recommend that you back it up on a remote machine for disaster recovery. When you migrate from an ACS server to ACS appliance, move the cert7.db file to a FTP server and download it according to the normal provisioning instructions. When you upgrade an ACS appliance, repeat the download procedure as originally used to provision the original appliance.

Step 1 If the ACS SE is running Cisco Security Agent, you must disable the CSAgent service before upgrading. You can do so at the console or in the web interface:

- Using the console, enter **show**. If the CSAgent service is running, enter **stop csagent**.
- Using the web interface, choose **System Configuration** > **Appliance Configuration** and verify that the CSA Enabled check box is not checked. If it is checked, uncheck the **CSA Enabled** check box and click **Submit**.

Step 2 Required for full upgrade with Restore. If you do not want to restore your data, skip to step 3.

a. Apply the Upgrade Package Appliance Management Software for ACS 4.0.1, which is available on the ACS SE 4.0 Upgrade CD.

b. Apply the Upgrade Package ACS 4.0.1 Software for Appliance, which is available on the ACS SE 4.0 Upgrade CD.

For details on using the web interface to upgrade, see the *User Guide for Cisco Secure ACS Solution Engine*. For details on using the command line to upgrade, see Loading and Installing an Upgrade Image, page 5-7.

Note When you use the upgrade package, dynamically mapped users are not kept.

c. Back up the upgraded ACS SE data and configuration by using one of the following features:

- ACS Backup, which is available in the System Configuration section of the web interface. For more information, see the *User Guide for Cisco Secure ACS Solution Engine*.
- The CLI **backup** command, which is available from the serial console. For more information, see Backing Up ACS Data From the Serial Console, page 4-12

Step 3 Use the ACS SE 4.0 Recovery CD to upgrade the appliance to 4.0. The upgrade destroys all data and installs a new image. Ensure that you have the correct version for your hardware.

For more information about reimaging the hard drive, see Re-imaging the Solution Engine Hard Drive, page 4-25.

Step 4 Perform an initial configuration of the ACS SE. For more information, see Configuring ACS SE, page 3-23.

Step 5 Required for full upgrade with Restore. If you do not want to restore your data, skip to step 6.

Restore the appliance data and configuration by using one of the following features:

- ACS Restore, which is available in the System Configuration section of the web interface. For more information, see the *User Guide for Cisco Secure ACS Solution Engine*.
- The **restore** command, which is available on the serial console. For more information, see Restoring ACS Data From the Serial Console, page 4-14.

Step 6 Verify that Cisco Security Agent is enabled by using one of the following features:

- At the console, enter **show**. If the CSAgent service is not running, enter **start csagent**.
- In the web interface, choose **System Configuration** > **Appliance Configuration** and verify that the CSA Enabled check box is checked. If not, select it and click **Submit**.

Upgrading to ACS SE 4.0 on top of the Existing Base Image

If you do not need the new features that are available with the upgraded base image, you can upgrade the Appliance Management Software and ACS software on top of the existing base image. The existing data and configuration are automatically upgraded and restored.

This procedure upgrades the ACS software to version 4.0 on a Cisco 1111 device or a Cisco 1112 device

Before you begin:

Make a backup of your existing data and configuration.

Note The backup procedure does not back up the cert7.db file. If you use this certificate file with an LDAP database, we recommend that you back it up on a remote machine for disaster recovery. When you migrate from an ACS server to ACS appliance, move the cert7.db file to a FTP server and download it according to the normal provisioning instructions. When you upgrade an ACS appliance, repeat the download procedure as originally used to provision the original appliance.

Step 1 If ACS SE is running Cisco Security Agent, disable the CSAgent service before upgrading by using one of the following features:

- At the console, enter **show**. If the CSAgent service is running, enter **stop csagent**.
- In the web interface, choose **System Configuration > Appliance Configuration** and verify that the CSA Enabled check box is not checked. If it is checked, uncheck the **CSA Enabled** check box and click **Submit**.

Step 2 Apply the Upgrade Package Appliance Management Software for ACS 4.0.1, which is available on the ACS SE 4.0 Upgrade CD.

For details on using the web interface to upgrade, see the *User Guide for Cisco Secure ACS Solution Engine*. For details on using the command line to upgrade, see Loading and Installing an Upgrade Image, page 5-7.

Step 3 Apply the Upgrade Package ACS 4.0.1 Software for Appliance, which is available on the ACS SE 4.0 Upgrade CD.

For details on using the web interface to upgrade, see the *User Guide for Cisco Secure ACS Solution Engine*. For details on using the command line to upgrade, see Loading and Installing an Upgrade Image, page 5-7.

Note When you use the upgrade package, dynamically mapped users are not kept.

Step 4 Verify that Cisco Security Agent is enabled by using one of the following features:

- At the console, enter **show**. If the CSAgent service is not running, enter **start csagent**.
- In the web interface, choose **System Configuration > Appliance Configuration** and verify that the CSA Enabled check box is checked. If not, select it and click **Submit**.

Step 5 To see the results of this upgrade procedure, view the Appliance Upgrade page. To do so, log in to the web interface and choose **System Configuration > Appliance Upgrade Status**.

The Application Versions table appears, displaying the upgraded application versions for the ACS software, appliance management software, and appliance base image.

Loading and Installing an Upgrade Image

This section describes how to load and install an ACS SE upgrade image from the command line interface of the serial console.

Upgrading the ACS SE typically involves the following steps:

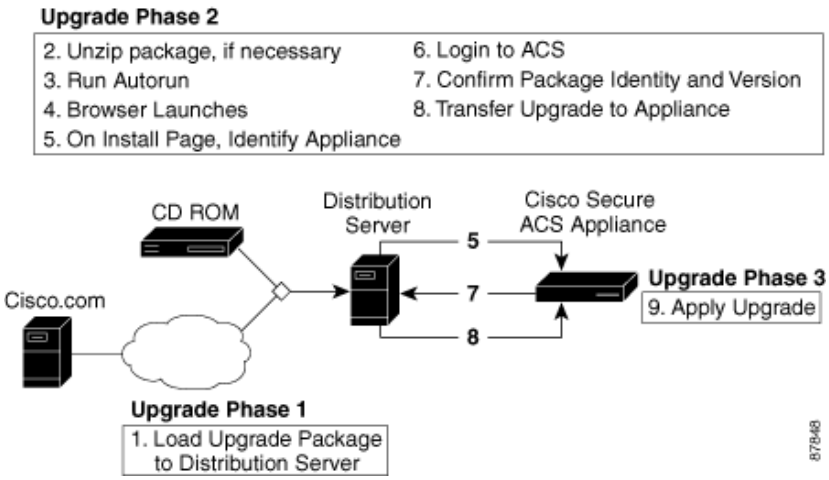
Step 1 Obtain the upgrade package from Cisco Systems and load it onto a distribution server in your network. You can use an upgrade CD or download the upgrade package from Cisco.com.

Step 2 Load the upgrade image onto the ACS SE from the distribution server on your network from within the web interface, or from the serial console. The ACS SE verifies the files that are transferred to ensure that they have not been corrupted. For more information on performing this step from the web interface, see the *User Guide for Cisco Secure ACS Solution Engine*. To load the upgrade image by using the command line interface, use the procedure described in Transferring an Upgrade Package to the Solution Engine via Serial Console, page 5-7.

Step 3 Finally, apply the ACS SE system upgrade from within the web interface, or from the serial console. For more information, see Applying a Solution Engine Upgrade, page 5-9.

This process is shown in Figure 5-1.

Figure 5-1 Solution Engine Upgrade Process



Transferring an Upgrade Package to the Solution Engine via Serial Console

Use this procedure to transfer an upgrade package from a distribution server to an ACS SE.

Before you begin

You must have acquired the upgrade package and selected a distribution server. For more information, see Loading and Installing an Upgrade Image, page 5-7.

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

To transfer an upgrade to your ACS SE:

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 that is included in the upgrade package runs on the other computer, not the distribution server.

b. If either of the following conditions is 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 from which you extracted the compressed upgrade package and run it.

Result: The HTTP server starts.

Step 2 If the distribution server uses Sun Solaris:

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.

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 solution engine 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 solution engines.

Step 3 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a 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 a Solution Engine Upgrade

Use this procedure to install upgrades on the ACS SE. 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 Solution Engine*. For information on how to load the upgrade package onto the ACS SE see, Transferring an Upgrade Package to the Solution Engine via Serial Console, page 5-7.

Also, if CSAgent is running, you must disable it before you issue the upgrade command. For information on stopping services see Stopping Solution Engine Services From a Serial Console, page 4-4.

Finally, because the ACS SE is nonoperational during the upgrade process, you should schedule the upgrade for a time when its absence online will have the least impact.

To apply a ACS SE system upgrade:

Step 1 Log in to the ACS SE. For more information, see Logging In to the Solution Engine From a Serial Console, page 4-2.

Caution The ACS SE will be nonoperational during the upgrade process.

Note If CSAgent is running, you must disable it before you issue the upgrade command.

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

Step 3 Press **Enter**.

Result: The system displays the following confirmation message:

```
Installing the patch could adversely affect the system. Do you still want to
continue?---y(yes), n(no)
```

Step 4 Type **Y** to continue.

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

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

Tip If no upgrade package is loaded on the ACS SE, a message requests that you download an upgrade package.

Step 5 Depending on your certification authority settings, you might 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 Solution Engine System and Services From a Serial Console, page 4-3.

Migrating to ACS SE

Migrating from Cisco Secure ACS for Windows Server (ACS for Windows) to ACS SE uses the backup and restore features of ACS. Backup files produced by ACS for Windows are compatible with ACS SE, provided that both are using the same version of ACS software.

Before You Begin

Before upgrading or transferring data, back up your original ACS database and configuration, and save the backup file in a location on a drive that is not local to the computer on which ACS is running.

Note The backup procedure does not back up the cert7.db file. If you use this certificate file with an LDAP database, we recommend that you back it up on a remote machine for disaster recovery. When you migrate from an ACS server to ACS appliance, move the cert7.db file to a FTP server and download it according to the normal provisioning instructions. When you upgrade an ACS appliance, repeat the download procedure as originally used to provision the original appliance.

Note If ACS runs on Windows NT 4.0, the following procedure will advise you when it is necessary to upgrade to Windows 2000 Server. Because the use of the backup and restore features is only supported between ACSs of the same version, you must use ACS for Windows 4.0, to transfer data from ACS for Windows to ACS SE. ACS for Windows 4.0 supports Windows 2000 Server and Windows Server 2003, not Windows NT 4.0. See the following procedure for more details.

To migrate from a Windows version of ACS to ACS SE:

Step 1 Set up the appliance, following the steps in Chapter 3, “Installing and Configuring Cisco Secure ACS Solution Engine 4.0.”

Step 2 On the ACS server, upgrade ACS for Windows to version 4.0. If you do not have a license for version 4.0, you can use the trial version, available at http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des.

If you run ACS on Windows NT 4.0, upgrade to ACS 3.0, and then migrate to Windows 2000 Server before upgrading to ACS 4.0. ACS 3.0 is the most recent version of ACS that supports Windows NT 4.0. For information about upgrading to ACS 3.0 or about migrating to Windows 2000 Server, see *Installing Cisco Secure ACS 3.0 for Windows 2000/NT Servers*. You can acquire the trial version of ACS 3.0 at http://www.cisco.com/cgi-bin/tablebuild.pl/acs-win-3des.

Step 3 In the web interface of ACS for Windows 4.0, use the ACS Backup feature to back up the database. For more information about the ACS Backup feature, see the *User Guide for Cisco Secure ACS for Windows Server*.

Step 4 Copy the backup file from the computer that is running ACS for Windows 4.0 to a directory on an FTP server. The directory must be accessible from the FTP root directory. ACS SE must be able to contact the FTP server. Any gateway devices must permit FTP communication between the appliance and the FTP server.

Step 5 In the web interface of ACS SE, use the ACS Restore feature to restore the database. For more information about restoring databases, see the *User Guide for Cisco Secure ACS Solution Engine*.

The ACS SE contains the original configuration of the ACS for Windows version from which you migrated.

Step 6 Continuing in the web interface of the ACS SE, verify that the settings for the *(Default)* entry in the Proxy Distribution Table are correct. To do so, choose **Network Configuration > (Default)** and ensure that the Forward To list contains the entry for the appliance.

Step 7 To replace the computer that is running ACS for Windows with ACS SE, you must change the IP address of the appliance to that used by the computer that is running ACS for Windows:

a. Record the IP address of the computer that is running ACS for Windows.

b. Change the IP address of the computer that is running ACS for Windows to a different IP address.

c. Change the IP address of the ACS SE to the IP address used previously by the computer that is running ACS for Windows. This is the IP address that you recorded in step a. For detailed steps, see Reconfiguring the Solution Engine IP Address, page 4-18.

Note If you do not change the IP address of the ACS SE to the address of the computer that is running ACS for Windows, you must reconfigure all AAA clients to use the IP address of the ACS SE.

Technical Specifications for the Quanta (1112) Version

Table A-1 provides the technical specifications of the Cisco Secure ACS Solution Engine (ACS SE) on the KD-1112 K9 platform.

Table A-1 ACS SE Technical Specifications for the Quanta (1112) Version

Component	Specifications
Height	4.3 cm
Width	48.2 cm
Depth	59 cm
Weight	18.2 Kg (full system including packaging and accessory kits)
Rated input voltage	100 VAC to 240 VAC
Rated input frequency	50 Hz to 60 Hz
Rated input current	3.5 A (110 V) to 2.0 A (220 V)
Rated input power	385 W
Power supply output: steady state	280 W
Operating temperature range	0°C to 40°C
Shipping temperature range	-40° to 65°C
Operating relative humidity	90% (noncondensing) at 35°C
Nonoperating relative humidity	90% (noncondensing) at 35°C
Processor	3.2 GHz
Cache Memory	1M FSB 800
Memory	1024 M
Network Controller (NIC)	Integrated two 10/100/1000 Gb ethernet support
Hard Drive	Seagate SATA 80G, ST380023AS
System battery	Maxell or Varta CR2032 210mAh lithium 3V

Table A-1 ACS SE Technical Specifications for the Quanta (1112) Version (continued)

Component	Specifications
Chipset	Intel Canterwood ES MCH + hanceRapids ICH chipset
CD-ROM	24x Slim CD-ROM

Technical Specifications for the Quanta (1113) Version

Table B-1 provides the technical specifications of the Cisco Secure ACS Solution Engine (ACS SE) on the CSACSE-1113 K9 platform.

Table B-1 ACS SE Technical Specifications for the Quanta (1113)

Component	Specifications
Height	4.24 cm
Width	42.4 cm
Depth	51 cm
Weight	18.2 Kg (full system including packaging and accessory kits)
Rated input voltage	100–240 Vac
Rated AC input current (maximum)	6.5 A
Rated frequency	47–63 Hz
Rated input power	345 W
Power supply output: steady state	345 W
AC input current (maximum)	6.5 A
Apparent power rating (kVA)	0.507
Mean time before failure (MTBF)	44,000 hours
Operating temperature range	0°C to 40°C
Shipping temperature range	-40° to 65°C
Operating relative humidity	80% (noncondensing) at 40°C
Nonoperating relative humidity	80% (noncondensing) at 40°C
Network Controller (NIC)	Integrated two 10/100/1000 Gb ethernet support
Hard Drive	80-GB or more ATA hard drive[1]

Table B-1 ACS SE Technical Specifications for the Quanta (1113)

Component	Specifications
Chipset	Intel E7230 Mukilteo MCH
DVD-ROM	QSI DVD-ROM Combo

1. The latest Cisco ACS 1113 appliances contain a 160-GB or 250-GB hard disk drive (the older Cisco ACS 1113 appliances contain a 80-GB hard disk drive). These appliances support high-availability (HA) deployments. You can deploy any combination of 80-GB, 160-GB, or 250-GB appliances in your HA deployments.

Windows Service Advisement

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

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

- Services That are Run, page C-1
- Services That are not Run, page C-2

Services That are Run

Table C-1 lists the services that are run on the ACS SE.

Table C-1 Operating System Services Automatically Run by ACS SE

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.
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 local area network and remote connections.
Plug and Play	Manages device installation and configuration and notifies programs of device changes.

Table C-1 Operating System Services Automatically Run by ACS SE (continued)

Service Name	Description
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.
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 by 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 C-2 lists the operating system services that are not run on the ACS SE.

Table C-2 Disabled Operating System Services in ACS SE

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

Table C-2 Disabled Operating System Services in ACS SE (continued)

Service Name	Description
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.
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 by 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
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 Quality of Service (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.

Table C-2 Disabled Operating System Services in ACS SE (continued)

Service Name	Description
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.
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 multisession 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 Solution Engine (ACS SE).

This appendix contains the following sections:

CLI Conventions

The 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 ACS SE CLI with the IOS CLI. Though they are similar, they are not identical.

Command Privileges

Access to CLI commands on the ACS SE 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 3-22.

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`.
- Valid command but omit required options, the system displays `Incomplete command`.
- 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 by 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 D-1 summarizes all commands available on the ACS SE. Refer to the full description of commands that you are not familiar with before using them.

Table D-1 Command Summary

Command	Summary Description	Location of Full Description
backup	Back up ACS data to an FTP serve.	backup, page D-4
download	Download ACS Install Package.	download, page D-5
exit	Logout the session.	exit, page D-5
exportgroups	Send a list of groups to an FTP server.	exportgroups, page D-5
exportlogs	List and send selected logs to an FTP server.	exportlogs, page D-6
exportusers	Send a list of users, by group, to an FTP server.	exportusers, page D-6
help	List description of commands.	help, page D-7
ntpsync	NTP synch with predefined NTP servers	ntpsync, page D-7
ping	Sends Internet Control Message Protocol (ICMP) echo_request packets for diagnosing basic network connectivity.	ping, page D-8
reboot	Soft reboot appliance.	reboot, page D-9
restart	Restart ACS services.	restart, page D-9
restore	Restore Appliance.	restore, page D-10
rollback	Rollback patched appliance.	rollback, page D-11

Table D-1 Command Summary (continued)

Command	Summary Description	Location of Full Description
set admin	Set administrator's name.	set admin, page D-11
set dbpassword	Set database password.	set dbpassword, page D-12
set domain	Set appliance's DNS domain.	set domain, page D-12
set hostname	Set appliance's hostname.	set hostname, page D-12
set ip	Set appliance's IP configuration.	set ip, page D-13
set password	Set administrator's password.	set password, page D-13
set time	Set the time zone, date, and time information, or configure one or more NTP addresses.	set time, page D-13
set timeout	Set the timeout for serial console with no activity.	set timeout, page D-14
show	Show version of appliance and ACS, system load status, ACS service status, IP configuration, appliance's hostname and DNS domain.	show, page D-14
shutdown	Shut down appliance.	shutdown, page D-15
start	Start ACS services.	start, page D-15
stop	Stop ACS services.	stop, page D-15
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 D-16
tracert	Display the network route to a specified host and identify faulty gateways.	tracert, page D-17
upgrade	Perform the second stage of upgrade.	upgrade, page D-17

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 ACS SE commands. Command names are case insensitive.

backup

To back up 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 that you want to encrypt the data, you are prompted for an encryption password. For more information, see Backing Up ACS Data From the Serial Console, page 4-12.

Example

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

backup onyx joeadmin backupdata

download

To download an upgrade image to the ACS SE 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 ACS SE. The syntax is:

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 web interface. After loading an upgrade image by executing the **download** command, install the image by using the **upgrade** command. For more information see Loading and Installing an Upgrade Image, page 5-7.

Example

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

download 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 process 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

ntpsync

To perform Network Time Protocol (NTP) synchronization with a predefined NTP server, use the **ntpsync** command. For information on setting the NTP server see set time, page D-13.

ntpsync

Syntax Description

This command has no arguments or keywords.

Example

The following command uses the predefined NTP synchronization server to synchronize ACS SE time to the NTP server time:

ntpsync

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

Table D-2 Syntax for the Ping Command

Argument	Description
-t	Ping the specified host until stopped.To see statistics and continue, type Control-BreakTo 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 ACS SE, 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 ACS SE:

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 Solution Engine Services From a Serial Console, page 4-6.

Example

The following command syntax 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

Argument	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 or group database, and the 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 ACS to its original condition after installing 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 ACS SE 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 ACS SE administrator. For more information, see Resetting the Solution Engine Administrator Password, page 4-15.

Example

This command sets the administrator name to john:

set admin john

set dbpassword

To set the ACS SE database password, use the **set dbpassword** command. Subsequent prompts take you through the process.

set dbpassword

Syntax Description

This command has no arguments or keywords.

Usage Guidelines

Use the **set dbpassword** command to begin resetting the database password. Subsequent prompts take you through the process. For more information, see Resetting the Solution Engine Database Password, page 4-17.

Example

The following command initiates the database password setting procedure:

set dbpassword

set domain

To set the DNS domain of the ACS SE, 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 ACS SE, use the **set hostname** command.

set hostname [*hostname*]

Syntax Description

hostname	Name of the ACS SE.

Example

This command sets the ACS SE name to *acs1*:

set hostname acs1

set ip

To set the ACS SE 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 Solution Engine IP Address, page 4-18.

Example

The following command begins the system IP address configuration.

set ip

set password

To set the ACS SE 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 Solution Engine Administrator Password, page 4-15.

Example

The following command initiates the password setting procedure:

set password

set time

To set the ACS SE 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 4-19.

You can also use the **set time** command to enable an NTP server to synchronize the ACS SE. You can configure one or more NTP servers by separating each NTP IP address entry with a space. For more information, see Setting the System Time and Date with NTP, page 4-20 and the command reference ntpsync, page D-7.

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 ACS SE, system load status, ACS service status, IP configuration, system time and NTP settings, ACS SE 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 ACS SE 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 Solution Engine Services From a Serial Console, page 4-5.

Example

The following command starts the CSAuth and CSAgent services:

restart csauth csagent

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, which may interfere with AAA services.

Note When you stop the CSAgent service, not only does the ACS SE stop CSAgent, but it also changes the startup type to manual. This action has the effect of keeping it stopped; even after reboot. Likewise, starting CSAgent resets the startup type to automatic.

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 Solution Engine Services From a Serial Console, page 4-4.

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

Argument	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 web interface, this command restarts the ACS services, which 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

Argument	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 ACS services, which 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 ACS SE. Ensure that you have stopped CSAgent prior to employing the **upgrade** command. For more information, see Loading and Installing an Upgrade Image, page 5-7.

Example

The following initiates the second stage of an upgrade:

upgrade

A

B

C

D

E

F

H

I

L

M

N

O

P

R

S

T

U

W